~~TOP SECRET CREAM~~

ARMY SECURITY AGENCY

Washington, D. C.

EUROPEAN AXIS SIGNAL INTELLIGENCE IN WORLD WAR II AS REVEALED BY "TICOM" INVESTIGATIONS AND BY OTHER PRISONER OF WAR INTERROGATIONS AND CAPTURED MATERIAL, PRINCIPALLY GERMAN

In Nine Volumes

VOL. I

Prepared under the direction of the

CHIEF, ARMY SECURITY AGENCY

1 May 1946

WDGAS-14

~~TOP SECRET CREAM~~

VOLUME 1--SYNOPSIS

VOLUME 1 SYNOPSIS

1. Origin of "TICOM".-- The word "TICOM" served as a cover name for a special project and for an organization, the "Target Intelligence Committee." The project, which was originally conceived by Colonel George A. Bicher, Director of the Signal Intelligence Division, ETOUSA, in the summer of 1944, aimed at the investigation and possible exploitation of German cryptologic organizations, operations, installations, and personnel, as soon as possible after the impending collapse of the German armed forces. Colonel Bicher elicited and secured the support of the U. S. Navy and of the British, and accordingly a joint and combined "Target Intelligence Committee" was established in England in October 1944, by the authority of the Chief of Staff, United States Army; the Commander-in-Chief, United States Fleet; and the Chairman, London Sigint Board.

The Target Intelligence Committee originally planned airborne operations, even before the German collapse, to seize important German signal intelligence targets, known from Ultra material and prisoner of war interrogations. There were four objectives:

a. To learn the extent of the German cryptanalytic effort against England and America;

b. To prevent the results of such German cryptanalysis against England and America from falling into unauthorized hands as the German Armies retreated;

c. To exploit German cryptologic techniques and inventions before they could be destroyed by the Germans; and

d. To uncover items of signal intelligence value in prosecuting the war against Japan.

The TICOM mission was of highest importance. American cryptographers did not then know with certainty the extent to which United States communications were secure or ~~unsecure~~ insecure, nor did they know the extent of the enemy's cryptanalytic abilities, strength, and materiel, except by conjecture, by inference from Anglo-American cryptanalysis of German systems and from prisoner of war interrogations. German cryptanalytic successes were obviously unpublicized. They were reflected instead in higher casualty lists and lessened success on the part of Allied tactics and strategy.

In the Spring of 1945, however, conditions for the proposed operations became rapidly unsatisfactory. The known German signal intelligence agencies were dispersing or retreating to other localities in greatest disorder. Pinpoint locations could not be established. The possibility was remote that Anglo-American parachute units could seize worthwhile personnel and material and hold them through the confusion of major battles. Therefore, in March, 1945, TICOM decided instead to alert six United States-British target exploitation teams in England, these teams to be sent into enemy territory as either United States or British troops overran it, where they were to take over and exploit known or newly discovered targets of signal intelligence interest and to search for other signal intelligence targets and personnel.

The first exploitation team was dispatched in April 1945 to the Neumuenster-Flensburg area, and other teams were quickly dispatched to other areas as soon as overrun. The odyssies of the TICOM teams striving to locate and exploit signal intelligence targets during the confused days before and after the German capitulation, make~~s~~ entertaining as well as instructive reading. They are fully recorded in the TICOM publication~~s~~.[1] A short summary of these operations is given in Volume 8, Chapter X, of this report.

The results obtained from these TICOM efforts were impressive. Approximately 4000 separate German documents were captured.[2] This material weighed 5 tons. Many cryptographic devices and machines were captured. One hundred and ninety six reports, based on interrogation of German signal intelligence personnel, together with other miscellaneous reports and translations were issued by TICOM.

The true value of the TICOM effort is not measurable in such statistics. Its importance lies rather in what the TICOM effort revealed to American cryptologists concerning German signal intelligence, with particular reference to American systems. The TICOM prisoner of war interrogations and captured documents, with the interrogations conducted by other Anglo-American agencies (notably the Combined Services Detailed Interrogation Centre, or "CSDIC") have given Anglo-American investigators a reasonably complete picture of German signal intelligence. The United States Army Security Agency has obtained from these interrogations and documents information useful in assessing its own cryptanalytic and cryptographic achievements, especially its own development of rapid analytic machinery, the state of its research in cryptography, and the cryptographic security of American systems.

[1] See IF 15, IF 40, IF 51, IF 101, IF 165, IF 166, IF 167, and I-1.

[2] By "document" is meant either one or a collection of papers, books, files of correspondence, messages, films, worksheets or other items of intelligence value, to which a TICOM document number was assigned for convenience in classification and handling.

2. The European Axis cryptanalytic effort against United States communications.--From TICOM sources it is learned that European cryptanalysts were unable to read any U. S. Army or Navy high-level cryptographic systems. The Army Converter M134C (SIGABA), the Army Teletypewriter Cipher Attachment known as the Converter M-228 (SIGCUM), the Army Teletypewriter Privacy Set (SIGIBS), the Army High Security Teletypewriter Cipher System (SIGTOT), the Army Speech Equipment RC-220-T1 (SIGSALY), the Combined Cipher Machine (CCM), the Navy Electric Cipher Machine Mark III (ECM, identical with SIGABA), and the Navy Teletypewriter Cryptographic Attachment (C. S. P. 1515, identical with the Army Converter M-228) were completely secure. One Army Strip system (System No. 47 or 67) and one Navy strip system (probably C. S. P. 1404) were read for short intervals until the principle of strip elimination was introduced. The low-grade ciphony device (Speech Equipment AN/GSQ-1, or SIGJIP) was not read, although theoretical solutions were worked out.

Both of the unenciphered War Department Telegraph Codes (SIGRIM and SIGARM) were read by the Germans. Hungary received photostatic copies of War Department Confidential Code Number 2, probably from the Bulgarians, together with at least one set of cipher tables, and the Italians reconstructed subsequent editions of the enciphering tables. The compromise appears to have been shared with other Axis powers, notably Germany, Finland and Japan. Military Intelligence Code No. 11 (physically compromised), used by the Military Attache in Cairo, was read throughout the summer of 1942. The Germans read messages in several versions of the Division Field Codes.

German cryptanalysts solved from 10 per cent to 30 per cent of intercepted U. S. Army M-209 messages. Save where keys were captured, it was usually read too late to be of tactical value. Messages sent by the U. S. Army in Slidex, Codex, Bomber Code, Assault Code, Aircraft Movement Code, Map Coordinate Codes, and Cipher Device M-94 where employed, were read regularly and almost 100 per cent.

Combined Naval Cypher No. 3, used by the U. S. Navy and the Royal Navy for Atlantic Convoy operations, was read almost 100 per cent by the Germans from the end of 1941 through the middle of 1943. The solution of this system was perhaps for the allies the most disastrous signal intelligence success achieved by the Germans. Allied convoy shipping losses suffered during this period were six times as great as during any other comparable period.

The Germans engaged in intensive and successful traffic analysis activities against United States Army and Army Air Force radio communications. This included direction-finding, analysis of call sign and frequency allocation systems, analysis of plain text and operator's chat, as well as more complex operations, such as air-borne radar route tracking, and monitoring of transmitter zero beat tuning.

The U. S. Army Converter M-134A (SIGMYC), and the U. S. Navy Cipher Machine (HCM), furnished by the Navy to the State Department, were not read by the Germans. The State Department Strip systems O-1 and O-2 were solved, the former probably through a compromise, and the latter through cryptanalysis. Several State Department codes, including the Brown Code (unenciphered) and Code A-1 (enciphered), were compromised and read, probably from 1938 and 1939, respectively.

From an intelligence standpoint the results obtained by the German cryptanalytic successes were important, but not decisive. American Army and Navy strategy was secure as long as high level systems were employed. Tactical operations, however, did suffer. The Anglo-American convoy shipping losses during 1942 and early 1943 were huge, largely because of German successes with Combined Naval Cypher No. 3. German traffic analysis and cryptanalysis provided a comprehensive order of battle for the U. S. Army and Army Air Forces in the United Kingdom, in the Mediterranean, and on the continent. According to a German air force officer, "no attack of the Eighth Air Force came as a surprise." The value of the intelligence which the Germans got from State Department codes and strip ciphers is not accurately known. The strip systems were probably read too late to be of any great value. The compromise of Military Intelligence Code No. 11 did provide intelligence of unquestioned tactical value, particularly in the summer of 1942 during Rommel's advance to Egypt.

The German cryptanalytic effort against Russian military communications was even greater than that made against the United States. The German successes in solution of medium and low grade English military and naval communications systems were considerable. The cryptanalysis of the diplomatic communications of Italy, Japan, France, Turkey, Bulgaria, Greece, Portugal, Spain, Switzerland, and other smaller nations also achieved important results.

A tabulation of the results of German and other European Axis cryptanalysis, country by country, is given in Chart 1-2, at the end of this Volume. These results will be discussed also in the subsequent volumes on the separate German agencies.

3. <u>Organization of German Signal Intelligence Agencies</u>.-- Germany possessed six main cryptologic organizations during World War II, with a total strength, including field units and overhead, of approximately 30,000 persons. Italy possessed two main signal intelligence organizations; Finland, Austria, and Hungary each had one. The grand total of European Axis personnel engaged in signal intelligence in World War II is estimated as 36,000.

This number is small when compared with the numbers engaged in the Anglo-American effort. The grand total of Anglo-American signal intelligence personnel at the end of the War, including all services and including field and overhead personnel, was in excess of 60,000 persons. Out of this total, the United States Army employed approximately 28,000 persons.

Of the six main German cryptologic organizations, four were military, and two were civilian.

The four military organizations were:

a. The Signal Intelligence Agency of the Army High Command (OKH/GdNA), which dealt with enemy Army traffic.

b. The Signal Intelligence Agency of the Navy High Command (OKM/4SKL III), which dealt with enemy naval traffic.

c. The Signal Intelligence Agency of the Air Force High Command OKL/LN Abt 350), which dealt with enemy Air Force traffic.

d. The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), which dealt with enemy, neutral or friendly diplomatic traffic, commercial traffic and news broadcast

The two civilian organizations were:

a. The Foreign Office Cryptanalytic Section (Pers Z S) which also dealt with diplomatic traffic, enemy, neutral, or friendly.

b. Goering's "Research" Bureau (FA), a Nazi party agency which also dealt with diplomatic traffic, news releases, broadcast monitoring, telephone monitoring, and other types of communications intelligence, enemy, neutral, or friendly.

Chart number 1-1 at the end of this volume shows how the above six agencies were related. Brief descriptions of these agencies and their work follow.

4. The Signal Intelligence Agency of the Army High Command.-- The Signal Intelligence Agency of the Army High Command (Oberkommando des Heeres, General der Nachrichten Aufklaerung, abbreviated OKH/GdNA) was located at Jueterbog, about 60 miles southwest of Berlin. Its mission included cryptanalysis and evaluation of Allied army traffic, at any level, whether strategic or operational. It also did a small amount of radio broadcast monitoring.

This Agency was the main unit of the German Army signal intelligence service in 1945. Other units were:

a. Two intercept stations operating directly under the Signal Intelligence Agency, and supplying it with intercepts of Allied high-level traffic.

b. Nine field Signal Intelligence Regiments assigned to various Army Groups for the purpose of interception, traffic analysis, cryptanalysis, and evaluation of Allied Army low-level tactical traffic in the Army Group areas. These Regiments were independent of the Central Signal Intelligence Agency, but supplied the latter with intercepts and reports.

c. A small Signal Intelligence Section, assigned to the Army Commander in Chief, West, which acted as a coordinating section for the two Signal Intelligence Regiments on the Western front.

An estimated total of 12,000 persons was employed in the Army signal intelligence effort described above.

The main successes of the German Army signal intelligence organization from its formation to the end of the war included the following:

a. Before 1939 it was able to establish French, Dutch, and British order of battle. This was dome by cryptanalysis of French codes and Dutch Army double-transposition ciphers, and through direction-finding and traffic-analysis directed against British Army communications systems.[3]

b. During the 1940 French campaign it established French mobile order of battle. This was done by cryptanalysis of French codes(unnamed).[4]

c. It established Russian army order of battle and location of strategic reserves, from early in the war through 1943. This was accomplished through traffic analysis and cryptanalysis of Russian 2, 3, 4, and 5-figure codes (both Army and Peoples Commissariat (NKVD)).[5]

d. It gave Rommel intelligence of great operational value during the fighting around Tobruk. This was done by solving the super-encipherment of a compromised British code (unidentified).[6]

e. Information on operations undertaken by the American Army in North Africa, and thereafter through the war, was obtained through solution of Converter M-209 traffic.[7] During the fighting in Sicily the Germans captured two weeks after it went into effect, a key list valid for one month[8] and were enabled thereby to read the system completely for the remaining two weeks.[9] On other nets when sufficient depth

[3] I 78

[4] I 78

[5] I 78; I 26; I 21; I 19

[6] IF 107; I 113. Germans called this "the British War Office Code."

[7] I 154; IF 107; I 60; I 113

[8] IF 107

[9] I 60

was available, from 10%[10] to 30%[11] of M-209 traffic was readable, though most of the traffic was read too late to be of tactical value.[12]

f. Information concerning U. S. Army activities in Iceland, England, Central America, and North Africa, was obtained by reading the U. S. Army Division Field Codes (DFC 15, 16, 17, 21, 25, and 28, and possibly others).[13]

g. Tactical information concerning Allied bombing and artillery targets,[14] weather reports,[15] and reports on the size and location of Allied units passing Military Police control points in France,[16] were obtained from solutions of "Slidex," a British device for protecting operational low-level traffic. This device was used by both British and American forces and various versions of it were solved, usually in from one to three hours.[17]

h. Solution of traffic passed on Hungarian internal networks in 1941 gave evidence that transportation of German troops over Hungarian railroads could be safely undertaken.[18]

i. Successful cryptanalysis was carried out against the traffic of Yugoslav partisans, Greek partisans, Czech agents, Russian agents, and the Polish resistance movement.[19]

The Signal Intelligence Agency of the Army High Command issued three daily reports. These were sent to the Army High Command, Navy High Command, Air Force High Command, and to the Supreme Command, Armed Forces; to Himmler as chief of the Elite guard; and probably to the Reich Security Office (RSHA).

[10] I 60

[11] I 113

[12] I 142

[13] IF 120 and IF 107

[14] IF 107 p 8

[15] I 74

[16] I 80

[17] I 74, I 76, I 80, I 109, IF 107

[18] IF 126 p 10

[19] I 115, I 76, D 60, I 170, I 58, and others.

Each of the nine Signal Intelligence Regiments in the field supplied intelligence directly to commanders at Army Group, Army, and Corps levels, looking to them for primary directives on missions and priorities. They cooperated closely with the local Air Force Signals Regiments.

The Signal Security Agency of the Army High Command (Inspektion 7/IV, abbreviated In 7/IV) issued Army Codes and Ciphers until 1944, when this function was taken over by the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi).

Volume 4 is a detailed account of the German Army Signal Intelligence Agency, its field units, and their activities.

5. The Signal Intelligence Agency of the Air Force High Command-- The Signal Intelligence Agency of the Air Force High Command (Oberkommando der Luftwaffe, Luftnachrichten Abteilung 350, abbreviated OKL/LN Abt 350, previously Chi Stelle, O B d L), was the principal unit of the German Air Force Signal Intelligence Service in 1945. Field units were:

a. Three autonomous Signal Intelligence Regiments with a total of eight battalions.

b. Five autonomous Signal Intelligence Battalions. Thirteen thousand people, including overhead, were employed in all the above units.

The German Air Force Signal Intelligence Service successes against the Royal Air Force and the United States Army Air Forces were outstanding.

a. The Service furnished a comprehensive and continuous picture of the battle order and deployment of United States Army Air Force and Royal Air Force units in the United Kingdom, in the Mediterranean Theater, and, after D-day, on the continent. This information came mainly from traffic analysis, radio-telephone monitoring, and monitoring of air-borne radar devices. The solution of Royal Air Force 4-figure codes (from March 1940 until 1 November 1942) gave basic data which was enlarged upon and used until the end of the war.[20]

[20] I 70, IF 182, IF 175 p 19

b. It gave prompt and accurate warning of United States Army Air Force and Royal Air Force heavy bomber missions. This resulted from advanced methods of traffic analysis, from radiotelephone monitoring, and from radar monitoring.[21]

c. It gave immediate warning to German ground forces and fighter squadrons of tactical operations by Allied ground support aircraft.[22]

d. In connection with its western front activities, the solution of the Bomber code, Slidex, Syko, and Rekoh (used by the Royal Air Force and, for a short time, by the United States Army Air Force), both by capture and cryptanalysis, was important throughout the war.[23]

The German Air Force Signal Intelligence Service successes against the Russian Air Force were also great.

a. Its cryptanalysis of Russian Air Force ground-to-ground 2-figure, 3-figure, and 4-figure administrative and operational codes, and some 5-figure codes, provided a complete order of battle for the Russian Air Forces from 1937 until the end of the war. A large amount of intelligence on Russian Army battle order was also obtained from a study of air networks.[24]

b. From partial decipherment of air-ground traffic, from plane-to-ground radio-telephone monitoring, and from radio-direction finding of bombers when airborne, it was able to give accurate warnings of all Russian long-range strategic bombing raids.[25]

c. From cryptanalysis of each Russian Air Army's 2-figure, 3-figure, and 4-figure traffic, from traffic analysis, from plane-to-plane radio-telephone monitoring, and from radio direction-finding of planes in flight, it was able to warn German ground forces and fighter squadrons of impending operations by Russian fighters and fighter bombers.[26]

[21] I 70

[22] IF 182

[23] IF 175

[24] I 120

[25] IF 187

[26] IF 187

Intelligence from both Western and Russian fronts, in the form of daily, weekly, or monthly reports, was furnished by the Signal Intelligence Agency (OKL/LN Abt 350) to the Air Force High Command and to the local Air Forces (Luftflotten). Daily and monthly reports were also sent to the local Army Signal Intelligence Regiments. Monthly reports were sent to the Army Commander in Chief West, to the Signal Intelligence Agency of the Army High Command (OKH/GdNA), to the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III), to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and also to the Air Force Signal Intelligence units in the field.[27]

Field units, charged with the responsibility for warnings on allied air raids, telephoned their warnings and reports directly to fighter squadrons, anti-aircraft batteries, and the local Gauleiters in charge of civilian air raid warnings.[28]

Group IV of Division II in the Office of the Chief Air Force Signal Officer (Oberkommando der Luftwaffe/Generalnachrichtenfuehrer II, Gruppe IV, abbreviated OKL/Gen Nafue II/IV) issued codes and ciphers for the Air Force. Group IV of Division III (OKL/Gen Nafue III/IV) checked them for cryptographic security.

A detailed description of the Signal Intelligence Service of the Air Force is given in Volume 5 of this report.

6. <u>The Signal Intelligence Agency of the Navy High Command</u>--The Signal Intelligence Agency of the Navy High Command (Oberkommando der Kriegsmarine, 4 Seekriegsleitung III, abbreviated OKM/4 SKL/III) was responsible for traffic analysis, cryptanalysis, and evaluation of British, American, Russian, French, and Swedish naval traffic. It had a strength of approximately 1,000 persons. It also had operational control over a field organization of approximately 2,500 persons. The field units were as follows:

a. Four detachments in Flanders, Brittany, Wilhemshaven and Pomerania engaged in cryptanalysis on low-level systems, interception and direction-finding. Each detachment had a total complement of 200 men, including 100 intercept operators and 10 cryptanalysts.

[27] IF 180 p 31 a

[28] IF 181

b. Eighteen "primary direction-finding stations", whose main duties were interception rather than direction finding. Each station had a strength of 100, including 60 intercept operators, and 5 cryptanalysts.

c. Twenty five "secondary direction-finding stations", whose duties were direction finding and traffic analysis. Each station had a strength of 26 persons.

d. Small detachments were occasionally set up for special missions.

The main successes of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) included the following:

a. In 1939 it was able to establish the war-time organization and disposition of the British Fleet, through solution of British Naval Code No. 2.

b. In the spring of 1940 it obtained complete information concerning the proposed British and French Norway expedition ("Operation Stratford"). This was done by solution of British Naval Cypher No. 4.[29] The German invasion of Norway followed immediately. During the subsequent Norwegian campaign, solution of traffic sent in British Naval Cypher No. 4. gave detailed information on Allied counter-measures, such as proposed British landing fields, transport arrival schedules, and the disposition of British and French surface forces.[30]

c. Throughout 1942 and part of 1943 it provided important intelligence on Atlantic convoys by a current (and nearly 100%) solution of Combined Cypher No. 3 used by British and U. S. North Atlantic Convoys.[31] The average monthly allied shipping losses in the Atlantic during this period were approximately six times the average monthly losses in later periods.

Minor successes of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) included the solution of the British Interdepartmental Cypher;[32] solution in 1943 of a Royal Air Force torpedo-bomber transposition cipher used for practice exercises in the English Channel;[33] and solution of various minor Navy and Merchant Navy codes and ciphers.

[29] T-517

[30] T-517

[31] I 12

[32] Performed jointly with Goering's "Research" Bureau (FA), the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and with the Signal Intelligence Agency of the Commander in Chief German Air Force (Chi Stelle, OBdL) I 147.

[33] D 6 D 15 D 41

The Naval Signal Intelligence field units described above carried out direction-finding activities against Allied naval and merchant ships, plotted their positions and movements, and passed the information to local commanders. Detachment Flanders, at Bruges, assisted in the 1942 "escape" of the pocket battleships Scharnhorst and Gneisenau when they made their dash from Brest through the English Channel to Kiel. This same detachment read British naval traffic to advantage during the Dieppe raid.

The Signal Security Agency of the Navy High Command (OKM/4 SKL/II), as opposed to the Signal Intelligence Agency(OKM/4 SKL/III), issued German naval codes and ciphers, and made cryptographic security studies of these systems. Its exact strength is unknown.

The detailed organization and history of the two signal agencies of the Naval High Command (OKM/4 SKL/III and OKM/4 SKL/II) are not discussed further in this report. Their use of punch-card book-keeping machinery ("I. B. M."), their security studies, and their chief cryptanalytic methods, however, are discussed in Volume 2.

7. The Signal Intelligence Agency of the Supreme Command Armed Forces.- The Signal Intelligence Agency of the Supreme Command Armed Forces (Oberkommando der Wehrmacht, Chiffrierabteilung, abbreviated OKW/Chi) had three main functions:

a. It intercepted, studied, and evaluated diplomatic, military attache, and "agent" traffic.

b. It monitored, and evaluated commercial radio traffic and news broadcasts.

c. It made security studies of the codes and ciphers used by the Supreme Command, Armed Forces, the Army, the Air Force and the Navy, and many government departments, vetoing (after 1944) the use of those it deemed insecure.

The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) operated at least thirteen radio intercept stations of its own, and received radio traffic from other agencies as well (notably Goering's "Research" Bureau (FA)). It also received land-line traffic from sources not stated.[34]

[34] DF 9, p 3

With the exception of military attache systems, it did not work on enemy Army, Navy or Air Force traffic. Documentary evidence as to its cryptanalytic successes is limited. The following summary covers its most important known cryptanalytic achievements:

a. The most extensive 1939-1944 successes seem to have been achieved with French systems. The electrical Hagelin Cipher Machine B-211 (adopted by the French - now obsolete) was solved, and limited success was also achieved in the solution of the French Hagelin Machine BC-38.[35] An important military attache code (ASA trigraph FVD) was solved at the beginning of the war.[36] After 1940 all Vichy-French systems were automatically compromised when filed with the German Armistice Commission in Wiesbaden.

b. At least four Japanese diplomatic codes (including those designated by ASA trigraphs JAE, JAH and JBA) were solved. In 1938 and 1939 the Agency collaborated with the Cryptanalytic Section of the Foreign Office (Pers Z S) in a current solution of daily keys for the Japanese "Red" Machine.[37]

c. Precise details on solution of U.S. systems are not available. The agency had compromised copies of at least two U.S. State Department codes, namely "Brown" and "Al". Work was also done on the U.S. State Department Strip Ciphers 0-1 and 0-2, the lead in 0-2 solution being taken by the Foreign Office Cryptanalytic Section.[38]

d. Croatian Enigma traffic was solved through compromised machine wirings.[39]

[35] I 45 p 7; I 160 p 6

[36] I 31 p 8

[37] I 31 p 11

[38] I 89

[39] I 58 p 3; I 92 p 2

e. Little information is available on successes in solution of English systems. Polish, Turkish, Greek and Latin American systems were solved extensively. Prior to 1943, appreciable success was achieved in the solution of Italian diplomatic codes.

During the first half of the year 1944 important decodes designated as "VN's" (Verlaessliche Nachrichten) totaled 3,000 per month.[40] Selected decodes were sent to Field Marshal Keitel, Chief of Armed Forces; to Hitler; and by Keitel to General Jodl, Chief of the Armed Forces Operations Staff. They were also sent to the Army, Navy and Air Force High Commands,[41] and probably to the Signal Intelligence Agencies of these commands.[42] In addition, approximately 45 special reports were sent each day to special recipients, such as the Field Economic Office, the Department of Armed Forces Propaganda, the Western Armies Branch and Joint Intelligence.[43]

After 1944 the Signal Intelligence Agency of the Supreme Command Armed Forces issued cryptographic systems for the Army and interservice communications. One of its most important responsibilities by the end of the war was the evaluating of the cryptographic systems of other services. A file belonging to Dr. Erich Huettenhain, its chief cryptanalyst, indicated that cryptographic studies were made on cipher teleprinters, Enigma machines, specially designed Hagelin machines, small cipher devices and hand systems.[44]

[40] DF 9

[41] I 143, p 9

[42] I 13, p 3

[43] DF 9 p 2

[44] D 59

In connection with its security commitments, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was responsible for the two most serious German cryptographic mistakes of the war: the continued use in high level German military communications of the plugboard Enigma machine and the teleprinter cipher attachment SZ 42 in their insecure forms. OKW/Chi rejected the 1943 proposals of the Army Signal Security Agency (IN 7/IV) that the (insecure) SZ 42 be replaced by the cipher teleprinter T52d, a secure device.[45] It also frowned on suggestions that the insecure plugboard Enigma be used with pluggable reflector wheels, a change which would have made it secure.[46]

Approximately 800 persons were employed in all duties except intercept.

Volume 3 of this Report gives a more detailed account of this agency.

8. The German Foreign Office Cryptanalytic Section.-- The German Foreign Office had two cryptologic sections, the Cryptanalytic Section (Personal Z Sonderdienst des Auswaertigen Amtes, abbreviated Pers Z S) and the Cryptographic Section (Personal Z Chiffrierdienst des Auswaertigen Amtes, abbreviated Pers Z Chi).

The Cryptanalytic Section of the Foreign Office (Pers Z S) was the senior German cryptanalytic agency. It was organized in 1919 or before. At its greatest strength it employed approximately 200 persons. Its mission was the solution of foreign diplomatic codes and ciphers. The Section had one small intercept station at Dahlem.[47] For the rest of its intercept it was dependent upon the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), Goering's "Research" Bureau (FA) and the German Postoffice.

[45] D59, p 17

[46] D 59, p 10; see also I 31

[47] I 22, para 103

[48] I 22, para 103

The Cryptanalytic Section achieved its greatest successes with diplomatic codes, both one-part and two-part, enciphered and unenciphered.

a. From 1935 until 1942 it achieved practically 100 per cent success in the solution of Italian diplomatic codes.[49]

b. It read the United States State Department Grey, Brown and A-1 Codes.[50] It also succeeded in solving the American Diplomatic Strip Ciphers 0-1 and 0-2, the former in partial fashion based upon a compromise.[51]

c. The Section solved two British Foreign Office "R" Codes and the British Government Telegraph Codes.[52]

d. In 1940 success in solution of French diplomatic codes was estimated at seventy five per cent.[53]

e. A number of major Japanese diplomatic codes were read, and there is some evidence that at least one major Chinese system was solved.[54]

f. The Section also solved two machine ciphers. The Japanese Red Machine was solved in 1938 and read currently until February, 1939.[55] The Section collaborated with the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) in this solution, and it is not known which agency deserves credit for the original solution.[56] In 1941, after a partial solution by Goering's "Research" Bureau (FA), the Swiss diplomatic Enigma traffic was solved.[57]

Little information is available on the Section's achievements in terms of intelligence. The distribution it gave its decodes is unknown. The Section's personnel seem to have thought primarily in terms of cryptanalysis as a science, rather than in terms of what their intelligence contribution meant to a successful German diplomacy.[58] The Section seems to have been badly neglected by higher Foreign Office authorities, both with respect to needed personnel, and with regard to interest in its work.

[49] I 22, para 25

[50] I 22

[51] I 22, para 54; DF 15, p 4, 5; I 89

[52] D 16, Reports 2, 3, 4

[53] D 54, p 13

[54] I 22, para. 176

[55] I 22, para 19

[56] I 22, para. 19

[57] D 54, p 18

[58] See Vol. VI. Ch. 5

Some of the Section's senior personnel acted in an advisory capacity to the Foreign Office Cryptographic Section (Pers Z Chi).[59] The latter section was responsible for the preparation, compilation,distribution and security of Foreign Office codes and ciphers. Few details are available concerning its security studies or its personnel. It was presumably responsible for the use in German diplomatic correspondence of the code systems known as the "Deutsches Satzbuch", the Deutsches Satzbuch enciphered by"Floradora" (Army Security Agency trigraph GEC), and the "one-time pad"(Army Security Agency trigraph GEE),all of which were read by Anglo-American cryptanalysts.Volume 6 of this paper gives an account of the cryptologic Sections of the German Foreign Office.

9. Goering's "Research" Bureau. -- Goering's "Research" Bureau (Reichsluftfahrtministerium Forschungsamt,abbreviated as FA) was formed in 1933. According to Goering,it supplied the new Nazi government with a signal intelligence organization of its own which had "no political axe to grind nor ideology to follow".[60]

In addition to non-military cryptanalysis,the "Research" Bureau had the following functions:

a. As a Nazi censorship organization in peace-time it monitored telephone conversations in all large German cities at first only in the Reich but later extending into Austria, Denmark,and"German" Poland.[61]. It had access to messages sent over all German commercial teletype and telegraph facilities,[62] and maintained investigators in all main postal censorship offices.[63]

b. In war-time it liaised closely in the censorship of all communications as directed first by the Abwehr and later by Himmler's Reich Main Security Office. It is known to have served the latter agency as a cryptanalytic agency for Russian Agent messages.(As no cryptanalytic organization within the Reich Main Security Office is known to TICOM it is probable that the"Research" Bureau filled this function).[64]

[59] I 172; I 22

[60] I 143

[61] TF 29; T 240

[62] I 143; IF 15

[63] IF 132

[64] TF 29; T 240

c. It monitored world-wide radio news broadcasts, in particular the British Broadcasting Company (London) broadcasts.[65]

d. It operated six wireless intercept stations of its own, for intercepting foreign diplomatic and commercial traffic. In addition, it exchanged copies of wireless intercepts with the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III), and probably with the Signal Intelligence Agency of the Commander in Chief German Air Force (Chi Stelle OBdL).

As can be seen from the functions outlined above, the "Research" Bureau was not primarily concerned with cryptanalysis. No documentary evidence bearing on its cryptanalytic successes was found by TICOM. Based upon secondary evidence and scattered TICOM interrogations, the bureau's chief cryptanalytic achievements seem to have been as follows:

a. In 1941 the agency collaborated with the Cryptanalytic Section of the German Foreign Office (Pers Z S) in solving the Swiss Enigma.[66] Personnel from the Bureau claimed to have broken Finnish (or Swedish) Hagelin traffic.[67]

b. According to newspaper reports, 1938 decodes of French traffic revealed that, lacking English support, the French Government did not intend to oppose the Austrian Anschluss with force.[68]

c. In 1938, during the Munich Conference, the "Research" Bureau is said to have solved the British system which carried Chamberlain's messages to London. Hitler once delayed a conference with Chamberlain for several hours in order to get such decodes.[69]

d. Solution of Russian internal wireless messages revealed bottlenecks in the Russian military supply system. The dates of this solution are unknown.[70]

[65] IF 132

[66] I 25; I 54; D 54 Report 8

[67] I 25 p 6

[68] IF 188

[69] IF 132

[70] I 25

The "Research" Bureau circulated its intelligence in the following forms:

a. Decode bulletins were sent regularly to Hitler, Goering, Field Marshal Keitel and General Jodl of the Supreme Command Armed Forces (OKW), Foreign Minister Ribbentrop, and Admiral Doenitz of tho Navy High Command.

b. Individual items of current interest, collected items on single subjec:, and consolidated special reports were sent to interested ministries.

c. Special liaison officers were assigned to the Foreign Office, the Supreme Command of the Armed Forces, the Reich Security Office, the Economic Ministry and Ministry for War Production, and the Propaganda Ministry.[71]

Goering's "Research" Bureau had over 2,000 personnel. Less than one per cent of these were apprehended by TICOM for interrogation.

Volume 7 of this report is a detailed account of this agency.

10. Collaboration between German Signal Intelligence Agencies in Cryptographic Matters-- It seems probable that, prior to 1943, there was some sort of collaboration between the various branches of the German Armed Forces in cryptographic matters. The widespread usage of the Enigma machine, the universality of the teleprinter systems used, the allocation of similiar hand cipher systems to army, air force and police units, all point either to an excellent cooperation in the cryptographic field, or to the existence of some shadowy interservice agency or higher authority whose responsibility it was to study, test and recommend the introduction of such devices and systems. There is no reference in the TICOM material to such an agency, other than a passing 1942 reference to "the big executive committee," a group which apparently had some responsibility for cryptographic changes and improvements in a cipher type teleprinter.[72] From the headings

[71] IF 135

[72] D 59, p 6

on various memos belonging to Dr. Huettenhain (chief cryptanalyst for the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi)), it could be assumed that the Chief Armed Forces Signal Communications Group (OKW/Chef Ag WNV) acted as a senior military cryptographic authority, approving or disapproving the introduction of various systems, and using the facilities of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) and the army agencies (Inspectorate 7/VI (In 7/VI) and the Army Ordnance Development and Testing Group Signal Branch (Wa Pruef 7)) as its staff or advisory agencies.[73]

An order from Field Marshal Keitel, Chief of Staff of the Supreme Command Armed Forces (OKW), dated October 1943, made the introduction of new ciphers for branches of the Armed Forces contingent upon the agreement of the Supreme Command Armed Forces (OKW), and probably upon the agreement of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[74]

In 1944 General Praun, who was both Chief Signal Officer of the Supreme Command Armed Forces (OKW/WFSt/Chef WNV) and the Chief Signal Officer of the Army (OKH/Chef HNW), made the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) a central clearing house for all German cipher development and security scrutiny work. This was easily done with reference to the Army. On September 5, 1944, General Praun signed an order directing that the cryptographic development and testing functions of the Army be turned over to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). Personnel from the Army Security Agency (In 7/IV),

[73] D 39, various letters and memos. From the headings of cryptographic manuals, it could be assumed that Ag WNV/Fu I, as issuing authority, was responsible until 1944, when OKW/Chi apparently replaced it. See OKW/Ag WNV/Fu I "Schluesselanleitung zum RS 44" dated March 27, 1944 and OKW/Chef WFSt/Ag WNV/Chi "Rasterersatzverfahren" of Dec. 7, 1944, TF 31 and TF 32 respectively.

[74] D 68, p 11; D 57 p 14

including Technician Dr. Fricke, and the personnel of Inspectorate 7/VI (In 7/VI) who were engaged in cryptographic work, were transferred into the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[75] Thereafter, while the actual production of keys was left as an Army responsibility, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) devised the cipher systems and provided the material for Army key production.[76]

With the Navy and the Air Force the picture was somewhat different. They were permitted to continue their cryptographic development work, and retained the right to say which of their systems was to be used in what place--so long as the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) concurred from a security standpoint in the original introduction of the systems. As Admiral Krause of the Signal Intelligence Agency of the Naval High Command (OKM/4 SKL/III) pointed out, "OKW/Chi recommendations could only lay down the (security) limits within which it was possible to use a system." The responsibility for whether and where a Navy system was to be used lay with the Navy.[77]

With regard to ciphers used by the Waffen SS, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) had consultative powers only. While General Gimmler, successor to General Praun as Chief Signal Officer, publicly characterized the cooperation between the two services as "perfect",[78] Col Mettig, chief of the cryptographic division in OKW/Chi, indicated that an effective supervision was never introduced.[79]

[75] D 68 p 3

[76] D 55, p 43 ?

[77] D 68, p 14

[78] D 68, p 13

[79] I 96, p 19

The preeminence of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) in cryptographic matters and security was apparently official only with the military services. In his speech of 29 NOVEMBER ~~December 20~~, 1944, General Gimmler pointed out that primacy in the civilian field was dependent upon voluntary concurrence from the agencies affected. He could only plead that "OKW was prepared to take the lead in this matter, providing that the Party and State concurred" and requested that "the Party and Reichs authorities" cooperate.[80] Goering's "Research" Bureau (FA) developed its own codes and ciphers,[81] although the Bureau did use cipher teleprinters adopted by the military services.[82] Evidence is available that in 1945 administrative hand ciphers (Behoerdenhandschluessel) were issued to Senior Specialist Wenzel of the "Research" Bureau (FA).[83] A similiar situation prevailed with the German Foreign Office. The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was never allowed to know the details of the ciphers used by the Foreign Office.[84] The Foreign Office, however, did use cipher teleprinters and Enigma machines.[85]

11. Collaboration between German Signal Intelligence Agencies in Cryptanalytic Matters.-- The collaboration between Agencies in cryptanalytic matters varied. In general relationship between Goering's "Research" Bureau (FA) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) were not overly cordial. The Signal Intelligence Agency of the Naval High Command (OKM/4 SKL/III) maintained a traditional

[80] D 68 p 14

[81] IF 132

[82] I 25, page 9

[83] T 240

[84] I 31, page 15

[85] I 22, para 115

navy reserve in dealing with other agencies. There was no high-level signal intelligence coordination, and there was frequent overlapping and duplication of effort between the agencies dealing with diplomatic cryptanalysis. But, with the exceptions noted above, there seems to have been as much liaison and as much cooperation as were necessary. This was especially true in the case of the military field organizations, the Army Signal Intelligence Regiments ("KONAs") and their Air Force equivalents, the Air Signal Regiments (LN Rgts).

a. Relationships between Foreign Office Cryptanalytic Section, Goering's "Research" Bureau, and the Signal Intelligence Agency of the Supreme Command Armed Forces.-- The Cryptanalytic Section of the Foreign Office (Pers Z S) enjoyed reasonably good working relationships with both Goering's "Research" Bureau (FA) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). As stated, however, the relationships between the latter two agencies do not appear to have been cordial.

The Foreign Office (Pers Z S) received the bulk of its intercept from Goering's "Research" Bureau (FA) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[86] It received numerous compromised codebooks and keys from both agencies.[87] Cooperative attacks on difficult problems were not uncommon. In the case of an unspecified U. S. Strip System, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) worked on the point-to-point traffic, while the Foreign Office (Pers Z S) worked on the circular traffic,[88] with a complete exchange of results. In the case of the Japanese Red machine, the Foreign Office (Pers Z S) attempted to solve messages sent on even days, while the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) attempted to solve messages sent on odd days, a "practical arrangement" reached also between the U. S. Army and the U. S. Navy prior to the Pearl Harbor disaster. Results

[86] I 22, para 103

[87] T2038; D16, pages 3, 5; DF 15, pages 4, 5

[88] I 31, page 10

were exchanged.[89] Goering's "Research" Bureau (FA) and the Foreign Office Cryptanalytic Section (Pers Z S) cooperated on the solution of the Swiss Enigma.[90] Exchange of code group identifications, additives and enciphering keys between these two agencies were frequent, especially on English, Italian and Vatican systems.[91] Personnel were exchanged between the Foreign Office Cryptanalytic Section (Pers Z S) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[92]

Goering's "Research" Bureau (FA) was formed by a small group of cryptanalysts who left the Cipher Department of the Reich Defense Ministry (Reichswehrministerium), the predecessor agency of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). This defection may account for the bad feeling between the two agencies.[93] There are no known examples of direct cryptanalytic exchanges between the two agencies, nor were there subsequent exchanges of personnel. Goering's "Research" Bureau (FA) was not given access to the special cryptanalytic machinery developed by the Signal Intelligence Agency of the Supreme Armed Forces (OKW/Chi),[94] although this machinery was made available to other agencies. Relationships could probably have been improved had not Goering's "Research" Bureau (FA) sought to take over the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[95]

[89] I 31, para 53

[90] D 54, page 18

[91] D16, pages 1, 2; I 172, paras. 11, 13, 14; T2252, various report

[92] I 22, paras. 20, 84

[93] I 21, p 1; I 131, p 3

[94] DF 9 p 3

[95] I 131, p 3; I 78 p 4

With reference to the exchange of traffic, however, collaboration was apparently complete. It is known that in early 1944 approximately one third of the intercept received by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) came from Goering's "Research" Bureau (FA).[96] The latter always received copies of all the traffic intercepted by Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) stations.[97]

b. Military Agency Relationships-- exchanges of cryptanalytic information.-- Collaboration between the Army Signal Intelligence agencies (OKH/GdNA and its predecessors, In 7/VI and HLS Ost) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was excellent. The Chief Signal Officer of the Supreme Command Armed Forces (OKW/Chef WNV) was also the Chief Signal Officer of the Army (OKH/Chef HNW)[98] However, since the Supreme Command agency's commitment was diplomatic and military attache traffic, no broad basis for cryptanalytic liaison existed.

The Army and Air Force Signal Intelligence Agencies maintained permanent liaison on English Naval and Air systems (SYKO, M209).[99] In 1943 the Army Agency (OKH/In 7/VI) had discovered how to recover true M-209 settings from relative settings, and they had passed the technique on to the Navy and Air Force agencies.[100] According to Senior Specialist Tranow of the Naval Agency, however, the Army-Navy cooperation was given up in early 1944 since "no results of value were obtained."[101] In 1943 the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), the Cryptanalytic Section of the German Foreign Office (Pers Z S), and the Signal Intelligence Agency of the Commander in Chief German Air Forces (Chi-Stelle OBdL) collaborated on solution of an unidentified US strip system.[102]

[96] DF 9, p 3

[97] I 85 , p 3

[98] IF 108

[99] I 93, p 3, 4

[100] I 144, p 2

[101] I 93, p 3

[102] D60, p 5

The Army-Navy- Air Force field collaboration was usually excellent.[103] It embraced on occasion exchange of personnel and equipment, a complete exchange of reports, and a close cryptanalytic liaison on operative systems.[104] Eastern front reports show a detailed operational collaboration between Air Force Signal Regiment 353 (LN Regt 353), the Army Signal Intelligence Regiment 1, (KONA 1), and the Naval units dealing with Russian Black Sea Fleet traffic.[105] Army Signal Intelligence Regiment 5 (KONA 5) worked closely with the Air Force Signal Intelligence organizations in the West (at Paris and Noisy).[106]

During the period 1940-1942 the Signal Intelligence Agencies of the Navy (OKM/4 SKL III) and the Air Forces (Chi-Stelle OBdL), and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and also Goering's "Research" Bureau (FA), all collaborated on solution of the English Interdepartmental Cipher.[107] There was "Research" Bureau (FA)-Naval (OKM/4 SKL/III) cooperation on the solution of the British Government Telegraph Code (South Africa) and Bentley's Code.[108] The Army Agency, Inspectorate 7/VI (In 7/VI) actually worked on Turkish diplomatic traffic, by agreement with Goering's "Research" Bureau[109] and had Army Signal Intelligence Regiment 4 (KONA 4) intercept this traffic for them. This work probably duplicated efforts of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) however.

[103] I 26, p 2

[104] US M-94, M-209, Slidex, Russian codes, etc.

[105] I 130, p 15

[106] I 113, p 8

[107] I 93, p 4; I 147, p 11, 12

[108] I 93, p 3

[109] IF 126, p 8

c. Military Agency Relationships--exchange of personnel.--In 1942 Prof. Novopaschenny of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) and a group of his cryptanalysts were transferred to Intercept Control Station East (HLS), one of the predecessors of the Signal Intelligence Agency of the Army High Command (OKH/GdNA) for work on the main Russian army five-figure code.[110] At one time the Naval commander in the Aegean area placed his radar intercept personnel and equipment under the command of Air Signal Regiment (LN Rgt) 352.[111] On one occasion personnel from Air Signal Regiment (LN Rgt) 353 went aboard the cruiser "Prinz Eugen" to monitor traffic from the Air Arm of the Russian Baltic Fleet.[112] In the spring of 1942 the Signal Intelligence Agency of the Naval High Command (OKM/4 SKL III) exchanged personnel with the Army and Air Force in order to get trained Hollerith operators.[113] In 1939 Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was detailed to the Army agency to work on solution of French military systems.[114]

d. Military Agency Relationships--Cooperation with regard to IBM and Rapid Analytic Machinery.-- The Army Signal Security Agency (Inspektion 7/IV abbreviated In 7/IV) pioneered in the use of IBM (Hollerith) equipment. Its installations were set up in the winter of 1939 and 1940, and later transferred to Army Inspectorate 7/VI (In 7/VI),one of the predecessors of the Signal Intelligence Agency of the Army High Command (OKH/GdNA).[115]

[110] IF 123 p 3

[111] I 126 p 14

[112] I 163 p 3

[113] I 146 p 17

[114] D 60 p 4, 5

[115] I 67 p 2

In March, 1942, representatives of Goering's "Research" Bureau (FA), and of the Signal Intelligence Agencies of the Commander in Chief Air Forces (Chi Stelle OBdL) and the Navy High Command (OKM/4 SKL/III) visited the Army installations and obtained valuable information as to the possibilities of IBM in cryptanalysis.[116] The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) never owned its own Hollerith machinery and used the Army installations.[117]

In 1944 the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) developed a number of "decoding devices," some of which were handed over to the Army, Navy and Foreign Office agencies.[118] The Digraph Weight Recorder (Bigrammsuchgeraet) was made available to the German Weather Service (WENUEB).[119]

e. Military Agency Relationships--cooperation with regard to interception.-- Goering's "Research" Bureau (FA) occasionally furnished the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi Stelle, OBdL) with traffic.[120] The amount of this traffic is not known. Goering's "Research" Bureau (FA) also passed some intercepted commercial traffic of naval interest to the Signal Intelligence Agency of the Naval High Command (OKM/4 SKL/III).[121] The German Navy passed its weather intercept to the Air Force, who had some interservice responsibility for the solution of weather traffic.[122] On operational fronts, when army search receivers found air force frequen ies, information concerning these frequencies was supplied to the appropriate air force field intercept units.[123] The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) controlled a naval direction finding station in Spain.[124]

[116] I 146, p 17

[117] I 67, p 2, 3

[118] DF 9, p 3

[119] I 31, p 4

[120] I 29, p 3

[121] I 93, p 12, 18

[122] I 93, p 4

[123] I 130, p 15

[124] I 96, p 7

f. Cooperation between Military and Civilian Agencies on solution of Agents' systems.-- The extensive German effort against agent-partisan systems warrants separate discussion. This effort was shared by at least three organizations, and perhaps a fourth. The organizations were: the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), Army Inspectorate 7/VI (OKH/In 7/VI), perhaps Goering's "Research" Bureau (FA), and a small organization which did little or no cryptanalysis, the Radio Defense Corps of the Supreme Command Armed Forces (OKW/WNV/FU III). The relationship between these agencies illustrates collaboration in both intercept and cryptanalysis, and an allocation of primary responsibility which varied from problem to problem.

At the beginning of the war, responsibility for monitoring clandestine transmissions in Germany and the occupied territories was borne by the Radio Defense Corps (OKW/WNV/FU III).[125] In the spring of 1942 the Radio Defense Corps pressed for the establishment of its own cryptanalytic section. Neither the Army nor the Supreme Command signal intelligence agencies were anxious to see the establishment of a new cryptanalytic agency for agent traffic. Accordingly, a section for cryptanalysis on agent transmissions was established in the Army Inspectorate 7/VI (In 7/VI).[126] This section was known (from its chief) as "Referat Vauck".

Originally located in Berlin, Referat Vauck moved in the fall of 1943 with the Radio Defense Corps (FU III) to Dorf Zinna, near Jueterbog. It was transferred in the fall of 1944 from Inspectorate 7/VI (In 7/VI) to the newly formed Signal Intelligence Agency of the Army High Command (OKH/GdNA) and was transferred again in early 1945 to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi/Gr. IV). Both these latter changes were administrative only, since the section remained with the Radio Defense Corps at Jueterbog.[127]

[125] I 115, p 2

[126] I 115, para 15

[127] I 115, paras 12, 31

Referat Vauck did not enjoy a monopoly on agent cryptanalysis. Most of its and the Radio Defense Corps' (FU III) effort was concentrated on western agent networks (France, Belgium). In the eastern and Balkan theaters, other agencies handled the bulk of agent intercept and cryptanalysis, as follows:

(1) Russian Partisan Traffic-- The work done by Referat Vauck on this problem covered only the period mid-1942 to mid-1943. Its work was then taken over by a section under Lt. Schubert of Army Signal Intelligence Regiment (KONA) 6.[128] Schubert was ultimately transferred to the Signal Intelligence Agency of the Army High Command (OKH/GdNA), where he took over "eastern" cryptanalysis on the NKVD-partisan networks.[129]

(2) Yugoslav systems-- Most of the interception and cryptanalysis on Yugoslav systems was done, not by the Radio Defense Corps (FU III), but by a special detachment of Army Signal Intelligence Regiment (KONA) 4, stationed in Belgrade.[130] Cryptanalytic work on the more difficult Balkan systems was done in Berlin by Balkan Section (Referat Bailovic) of Army Inspectorate 7/VI (In 7/VI), who thus complemented the activities of Referat Vauck.[131]

(3) Polish Resistance Movement Systems-- In 1943 Referat Vauck solved the principal system used by the Polish Government in Exile (London) for communication with the Polish Resistance Movement (Warsaw). So important was this traffic that, in the fall of 1943, eight members of Vauck's Section were transferred to the Polish Section in the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi, Gr. V). The intercept work done by the Radio Defense Corps (FU III) was augmented by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) intercept station at Lauf,[132] and I.B.M. assistance was given by Army Inspectorate 7/VI (In 7/VI).

[128] I 115, p 7

[129] I 26, p 1

[130] I 115, p 8

[131] I 115, p 8

[132] I 115, p 9

There is one reference (by Lt. Schubert) to "Research" Bureau (FA) participation in this work. In Janauary, 1945, Senior Specialist (ORR) Wenzel of Goering's "Research" Bureau (FA) was sent by the Radio Defense Corps (OKW/WNV/FU III) to the Signal Intelligence Agency of the Army High Command (OKH/GdNA) to work on resistance movement systems.[133]

(4) Other Agent Traffic-- Duplicates of all Radio Defense Corps intercept were forwarded to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), who, on occasion, helped Referat Vauck with more difficult problems.[134]

12. Other European Axis Cryptanalytic Agencies--

a. Italian Cryptanalytic Agencies-- Until the September, 1943, armistice, there were four Italian cryptologic agencies, the two most important being the Cryptanalytic Section of the Army Intelligence Service (Servizio Informazioni Militari, abbreviated SIM) and the Cryptanalytic Section of the Navy Intelligence Service (Servizio Informazioni Speciali, abbreviated SIS). These two agencies had both cryptanalytic and cryptographic functions. The Ministry of Foreign Affairs maintained a small cryptographic office (Ufficio Crittografico) to compile Italian diplomatic codes and ciphers.[135] The Inspector General of Political Police in the Ministry of the Interior (Publica Sicurezza) also maintained a cryptanalytic section to deal with "Communist" and "foreign agent" codes and ciphers.[136] The Italian Air Force Intelligence Service (Servizio Informazioni Aeronautica, abbreviated SIA) maintained its own intercept organization, but no cryptanalytic personnel. The Cryptanalytic Section of the Navy Intelligence Service (SIS) acted for the Air Force in this matter.[137]

[133] I.26 p 27

[134] For example, their work on the Russian agent traffic called "Rote 3" - D60, page 16.

[135] IF 1500

[136] IF 1502

[137] IF 209

After September, 1943, the functions of the Cryptanalytic Section of the Army Intelligence Service (SIM) were taken over by a neo-Fascist organization, the Defense Intelligence Service (Servizio Informazioni Difesa, abbreviated SID), which confined its activities to commercial and broadcast monitoring and solution of systems read by its predecessor agency.[138] No TICOM information is available concerning the post-1943 activities of the other agencies mentioned above.

The Cryptanalytic Section of the Army Intelligence Service (SIM) maintained four fixed intercept stations in Italy, and a field organization whose precise strength is unknown.[139] After June, 1943, each field army probably disposed of both a cryptanalytic party (Nucleo) and intercept facilities.[140] The Cryptanalytic Section of the Naval Intelligence Service (SIS) maintained seven fixed intercept stations in Italy and its possessions. It also controlled intercept groups located on the flagships of all naval commands.[141]

Italian cryptanalytic successes seem to have been limited. The Army Cryptanalytic Section worked on diplomatic, military attache, commercial and army systems.[142] The Naval Section concentrated its efforts on British Naval and Air operational codes.[143] Both sections were small,[144] trained cryptanalysts were at a premium,[145] and IBM equipment was difficult to procure. The Army Cryptanalytic Section read the U. S. State Department "Brown" Code (through compromise) and solved (or purchased) several other U. S. systems including the Military Intelligence Code No. 11.[146] According to General Gamba, head

[138] IF 1517, 1524, 1526

[139] IF 1517

[140] IF 1520, IF 1523

[141] IF 209

[142] IF 1517

[143] IF 209

[144] IF 209

[145] IF 1518

[146] IF 1517, IF 1524

of the Section, they also read a British diplomatic five-figure code, and an unenciphered four-figure, two-part British diplomatic code (Foreign Office "R" Code ?), as well as French, Turkish and Rumanian systems.[147] The Naval Section read British naval tactical codes, the daily-changing air code enciphering tables, and an unidentified four-figure "Anglo-American Naval code".[148] A four-figure British Naval code was read from 1941 until the North African landings in November, 1942.[149]

The Germans held a low opinion of Italian cryptanalytic capabilities, and considered their cryptographic procedures to be highly insecure. As a result, good cooperation was never achieved. What formal liaison existed, ended with the 1943 Armistice. The Germans then took over the remnants of the Italian organization (SID), dissolving it in February, 1944.[150]

For a more detailed discussion of the Italian cryptanalytic organization see Volume 8.

b. The Hungarian Cryptanalytic Agency-- The Hungarian Cryptanalytic Bureau (Section X of the General Staff-Hungarian name unknown) was subordinated to the Ministry of Defense. It had a strength of approximately fifty persons.[151] Its principal cryptanalytic work was done on Turkish codes and ciphers, as well as Italian, Polish and Russian systems. TICOM recovered approximately 90 code books from the agency, covering work on codes from 16 countries.[152] The organization was evacuated in 1945 to German territory, and later dispersed into Hungarian collecting camps.

[147] IF 1518

[148] IF 209, IF 1527

[149] IF 1527

[150] IF 1527

[151] I 193 p 3

[152] A 27

The Hungarian Bureau was said to have had an excellent relationship with the German Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and the Finnish cryptanalytic organization.

For further discussion on the Hungarian Cryptanalytic Agency, see Volume 8.

c. The Austrian Cryptanalytic Agency-- A small Austrian Cipher Bureau (subordination and Austrian name unknown) had been in existence for some years prior to 1934. It had a staff of at least five key cryptanalysts, who worked principally on Italian, French, Swiss, Yugoslav, Spanish, U. S. and English systems. Before 1934, and during the critical period prior to the annexation its personnel made a regular "black market" exchange of cryptanalytic results with the Signal Intelligence Agency of the German War Ministry (Reichskriegsministerium) dealing with Senior Specialist (ORR) Fenner and Captain (later Major and Colonel) Boetzel. After annexation, its principle cryptanalysts went to work for various German Signal Intelligence agencies including the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and Goering's "Research" Bureau (FA).

d. The Finnish Cryptanalytic Agency-- The Finnish Signal Intelligence Agency (Finnish name unknown) was subordinated to the military intelligence organization of the Finnish General Staff. Of approximately battalion strength, it was subdivided into intercept, cryptanalytic and evaluation units.[153]

Highly regarded by German cryptanalysts, with whom excellent liaison existed, it worked on military, naval and diplomatic traffic. First priority was given to Russian traffic, followed by Polish, Swedish and U. S. traffic.[154] They succeeded in solving the five-figure Russian military code used at the time of the first Russo-Finnish war. In 1943 they also solved an unspecified U. S. Strip cipher.[155]

See Volume 8 for a further discussion of the Finnish Cryptanalytic Agency.

[153] I 106 p 3

[154] I 111 p 4

[155] I 31 p 9

e. The Bulgarian Cryptanalytic Agency-- TICOM sources make only one reference to Bulgarian cryptanalytic work. In 1944 the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) gave a training course to certain Bulgarian cryptanalytic personnel.[156]

13. Liaison between German Signal Intelligence Agencies and other Axis cryptanalytic Agencies.-- The four German military cryptanalytic agencies appear to have engaged in active liaison with allied (Axis) cryptanalytic agencies. There is no evidence (from TICOM sources) that any foreign liaison was undertaken by Goering's "Research" Bureau (FA) or the Cryptanalytic Section of the German Foreign Office (Pers Z S). The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) appears to have had some primacy, especially in the field of relationships with Japan.[157]

a. Liaison with Japan.-- The Signal Intelligence Agency of the Naval High Command (OKM/4 SKL III) attempted to give the Japanese data on the British Naval Cipher No. 3, receiving in return some strips and settings for the U. S. Strip Cipher "DUPYH!" [158] There was a formal liaison between the Signal Intelligence Agency of the Supreme Command Forces (OKW/Chi) and the Japanese military attache in Berlin. Some data on American systems was given to the Japanese, but no intelligence was exchanged.[159] In January, 1945, a German interservice cryptanalytic delegation was to be sent to Japan by submarine, but the plan never materialized.[160]

[156] I 96, p 5

[157] I 119, p 6; I 29, p 6

[158] I 93, pages 8, 9; I 12, p 19

[159] I 21, p 3

[160] I 105, p 5; I 48, p 3

b. Liaison with Italy.--There was little practical cryptanalytic collaboration with the Italians. Code book groups were exchanged.[161] The Germans had no confidence in the security of Italian cryptographic systems.[162] Liaison was terminated at the end of 1943.[163]

c. Liaison with Hungary.--According to Colonel Kettler of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), liaison with the Hungarians had existed since the 1920's.[164] In the spring of 1944 one-eighth of the intercept used by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) came from Hungarian sources.[165] From April, 1944, until January, 1945, a Hungarian intercept company was attached to III/Air Signals Regiment 353.[166] The Hungarian agency also sent Italian, Rumanian and Polish traffic to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), who returned solution methods on this traffic to the Hungarian agency.[167]

d. Liaison with Finland.--The liaison with the Finns on Russian traffic seems to have been the most satisfactory cooperation undertaken by the Germans. Detachments of Airforce Signal Intelligengg personnel worked with the Finns at Mikkeli and Sortavala.[168] There were permanently assigned liaison officers, both Finnish and German, at the Finnish agency and the Army Signal Intelligence Agency East (HLS/Ost).[169]

[161] I 21, p 1

[162] I 78, p 11

[163] I 21, p 3

[164] I 21, p 2

[165] DF 9, p 3

[166] I 130, p 15

[167] I 21, p 2

[168] I 120, p 3

[169] I 21, p [illegible]; I 116, p 10

The cooperation embraced exchange of intercepted traffic, work on keys and systems (including non-Russian systems, such as an unspecified U. S. Strip System[170]) and exchanges of equipment. There is, however, some evidence that the Finns did not provide the Germans with all the cryptanalytic material available.[171]

e. Liaison with Spain and Bulgaria-- Cryptanalytic liaison between these two countries and the Germans appeared to be unimportant.

14. Chart summarizing results of European Axis cryptanalysis-- Chart 1-2 summarizes the results of the European Axis cryptanalytic effort against the cryptographic systems of other nations, as learned from TICOM sources, and as annotated with Army Security Agency material.

For purposes of brevity, the following abbreviations have been used in this chart:

FA- represents Goering's "Research" Bureau (FA).

OKH- represents the Signal Intelligence Agency of the Army High Command (OKH/GdNA), its predecessors and/or field units.

OKL- represents the Signal Intelligence Agency of the Air Force High Command (OKL/LN Abt 350), its predecessors and/or field units.

OKM- represents the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III and/or its field units.

OKW- represents the Signal Intelligence Agency of the Supreme Command Armed Forces.

Pers Z S- represents the Foreign Office Cryptanalytic Section (Pers Z S).

SID- represents Italian Defense Intelligence Service (SID). (see Volume 8, Page 15).

SIM- represents Italian Army Intelligence Service (SIM) and/or its field units.

In many cases, positive system identifications could not be made. Where doubt existed, the systems were therefore entered separately. Thus, many systems may have been entered more than once in the chart.

[170] I 31, p 9

[171] I 84, p 5

Volume 1

Tab A

A 27. "List of Documents Received from Hungarian Crypt. Unit Eggenfelden." A TICOM Publication.

Abwehr.-- Military Intelligence.

Agents Section of In 7/VI.-- Referat Vauck (Vauck's Section, named for its chief, First Lt. Vauck).

Ag WNV/Fu (Amtsgruppe Wehrmachtnachrichtenverbindungen/Funkueberwachung).-- Armed Forces Radio Monitoring Service.

Air Signal Regiment.-- Luftnachrichtenregiment (LN Regt).

Amtsgruppe Wehrmachtnachrichtenverbindungen/Funkueberwachung (Ag WNV/Fu).-- Armed Forces Radio Monitoring Service.

Armed Forces Radio Monitoring Service.-- Amtsgruppe Wehrmachtnachrichtenverbindungen/Funkueberwachung (Ag WNV/Fu).

Army Ordnance, Development and Testing Group, Signal Branch.-- Chef der Heeresruestung und Befehlshaber des Ersatzheeres, Amtsgruppe fuer Entwicklung und Pruefung des Heereswaffenamts, Waffenpruefung, Abteilung 7 (Wa Pruef 7).

Army Signal Intelligence Regiment.-- Kommandeur der Nachrichtenaufklaerung (KONA).

Boetzel, _____, Col. Chief of Code and Cipher Section of German War Ministry, 1934 - 1939. Chief of the Signal Intelligence Agency of the Army High Command. (OKH/GdNA).

Chief Armed Forces Signal Communications Group.--Oberkommando der Wehrmacht/Chef Amtsgruppe Wehrmachtnachrichtenverbindungen (OKW/Chef Ag WNV).

Chief Signal Officer of the Army.--Oberkommando des Heeres/Chef des Heeresnachrichtenwesens (OKH/Chef HNW).

Chief Signal Officer of the Supreme Command Armed Forces.--Oberkommando der Wehrmacht/Waffenfuehrungsstab/Chef der Wehrmachtnachrichtenverbindungen (OKW/WFst/Chef WNV).

Chiffrierdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes (Pers Z Chi).--Foreign Office Cryptographic Section.

Chiffrierstelle, Oberkommando der Luftwaffe (Chi-Stelle Ob d L).-- Signal Intelligence Agency of the Air Force High Command.

Chi-Stelle Ob d L (Chiffrierstelle, Oberbefehlshaber der Luftwaffe).--Signal Intelligence Agency of the Commander in Chief of the Air Force.

Cryptanalytic Section of the Italian Army Intelligence Service.--Servizio Informazioni Militari (SIM).

Cryptanalytic Section of the Italian Navy Intelligence Service.--Servizio Informazioni Speciali (SIS).

CSDIC. Combined Services Detailed Interrogation Center.

D 6. "List of German Cover-names with equivalents and descriptions of British cipher systems worked on by OKM/4 SKL/III." Translation documents T 515 - T 520. A TICOM document.

D 15. "Translation of ten cryptanalytical reports by OKM/4 SKL/III on British Naval systems from folder entitled "Research Progress 30/11/44-21/3/45", in T 520.

D 16. Translation of Annual Progress Reports by Pers Z S covering 1927, 1941, 1942. A TICOM publication.

D 41. Translation of Cryptanalytic Reports by OKM/4 SKL/III on British Naval Systems, from Folder entitled "Research Progress 1/12/43-1/11/44." TICOM 519.

D 54. Translation of Eight Pers Z S Reports on Cipher Systems of Various Countries.

D 57. "Notes and Minutes of High-Level Meetings held at OKW/Chi." Translation of T 1650. A TICOM publication.

D 59. Notes on Cipher Security and Minutes of Meetings held at OKW/Chi.

D 60. Miscellaneous Papers from a file of RR Dr. Huettenhain of OKW/Chi.

D 68. Further Misc. Papers from a File of Huettenhain.

DF 9. Captured Wehrmacht Sigint Document: Translation of Activity Report of OKW/Chi for the Period 1st January, 1944 to 25th June, 1944.

Doenitz, Karl, Grand Admiral. Commander in Chief, German Navy; Reich Chancellor after Hitler's death.

ETOUSA. European Theater of Operations, United States Army.

FA (Forschungsamt).--Goering's Research Bureau.

Fenner, Wilhelm, Senior Specialist. Chief of Division B of OKW/Chi (cryptanalysis).

Foreign Office Cryptanalytic Section.--Sonderdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes (Pers Z S).

Foreign Office Cryptographic Section.--Chiffrierdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes (Pers Z Chi).

Forschungsamt (FA).--Goering's Research Bureau.

Fricke, Walther, Technician (Lt. Grade), Dr. Chief of Section IIb of OKW/Chi (development of German systems).

Gamba, Vittorio, General. Commander of Italian Cryptanalytic Section from World War I to Armistice of World War II.

German War Ministry.--Reichskriegsministerium.

Gimmler, _____, Maj. Gen. Chief of Army Ordnance, Development and Testing Group, Signal Branch (Wa Pruef 7), 1939-1943. Chief Signal Officer to Commander in Chief West, 1943 - 1945. Chief of Armed Forces Communications Group (Chef Ag WNV).

Goering's Research Bureau.--Forschungsamt (FA).

Group IV of Division II in the Office of the Chief Air Force Signal Officer.--Oberkommando der Luftwaffe/General-nachrichtenfuehrer II, Gruppe IV (OKL/Gen Nafue II/IV).

Himmler, Heinrich. Reichsfuehrer SS, Minister of Interior, Chief of German Police.

HLS Ost (Horchleitstelle Ost).--Intercept Control Station East.

Horchleitstelle Ost (HLS Ost).--Intercept Control Station East.

Huettenhain, Erich, Specialist Dr. Chief cryptanalyst of OKW/Chi from 1937 to end of war. Chief of Group IV (cryptanalytic research); also chief of Section IVd (training).

I 1. "Final Report on TICOM Team 3 on Final Exploitation on Burgscheidungen." A TICOM publication.

I 12. "Translation of the Preliminary Interrogation of O.R.R. Tranow of 4/SKL III/OKM, carried out at Flensburg on 24-25 May 1945 by TICOM Team 6." A TICOM publication.

I 13. "Composite Report on Two Interrogations of Oberstlt. Friedrich, Chief of the G.A.F. Sigint Service, 18/5/45 and 9/6/45." A TICOM publication.

I 19. Report on Interrogation of KONA 1 at Revin France June 1945.

I 21. "Preliminary Interrogation of Oberst Mettler, R.R. Dr. Huettenhain, Sdf. Dr. Fricke and Oblt. Schubert (OKH/Chi), 15 June 1945." A TICOM publication.

I 22. "Interrogation of German Cryptographers of Pers Z S Department of the Auswaertiges Amt." A TICOM publication.

I 25. "Interrogation of RLM/Forschungsamt Members: Dr. Paetzel R. R. Fingerhut, R. R. Oden, Dr. Klautsche and Min. Rat. Seifert, at Schloss Gluecksburg on 15, 21 June 1945." A TICOM publication.

I 26. "Interrogation of Oblt. Schubert (OKH/Chef HNW/Gen.-d.NA) on Russian Military and Agents' Systems." A TICOM publication.

I 29. "Third Interrogation of Oberstltn. Friedrich, Chief of the G. A. F. Signals Intelligence Service." A TICOM publication.

I 31. "Detailed Interrogations of Dr. Huettenhain, formerly head of research section of OKW/Chi, 18th-21st June 1945." A TICOM publication.

I 45. "OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Machines." A TICOM publication.

I 48. "Report on Special Interrogation of Drs. Huettenhain and Fricke, Oberst Mettig, and Lt. Morgenroth carried out on 29th July 1945." A TICOM publication.

I 54. "Second Interrogation of Five Members of the RLM/Forschungsamt." A TICOM publication.

I 58. "Interrogation of Dr. Otto Buggisch of OKW/Chi." A TICOM publication.

I 60. "Further Interrogation of Oblt. Schubert of OKH/GdNA." A TICOM publication.

I 67. "Paper by Dr. Otto Buggisch of OKH/ In 7/VI and OKW/Chi on Cryptanalytic Machines." A TICOM publication.

I 70. "Paper on the German Sigint Service by Oberstltn. Friedrich." A TICOM publication.

I 74. "Interrogation Report on Obgefr. Koller, formerly Auswertestelle 4 and Nachrichten Aufklaerungskompanie 611." A TICOM publication.

I 76. "Interrogation Reports on Lehwald, Haupts, Klett and Lauerbach. Also I 76 Supplement (Diagrams)." A TICOM publication.

I 78. "Interrogation of Oberstlt. Mettig on the History and Achievements of OKH/AHA/In 7/VI.

I 80. "P.O.W. Interrogation Report--Obgefr. Clement Schuck Insp. VII/6 (OKH)." A TICOM publication.

I 84. "Further Interrogation of R. R. Dr. Huettenhain and Sdf. Dr. Fricke of OKW/Chi." A TICOM publication.

I 85. "P.O.W. Interrogation Report on Reg. Rat Flicke, Techn, Insp. Pokojewski, Stabsintendant Hatz of OKW/Chi." A TICOM publication.

I 89. "Report by Prof. Dr. H. Rohrbach of Pers. Z. S. on American Strip Cipher." A TICOM publication.

I 93. "Detailed Interrogation of Members of OKM 4 SKL III at Flensburg." A TICOM publication.

I 96. "Interrogation of Oberstlt. Mettig on the Organization and Activities of OKW/Chi." A TICOM publication.

I 105. "Interrogation Report on Frau von Nida (Wife of Major Wolfgang von Nida, one-time Deputy Head of OKW/Chi)." A TICOM publication.

I 106. "Final Interrogation Report on the Norway Party (NAA 11)." A TICOM publication.

I 109. "Translation of a Report by Lt. Ludwig of Chi Stelle Obd.L. (Ref.B) based on questions set for him at A.D.I.-(K)." A TICOM publication.

I 111. "Further Interrogation of Oberstlt. Mettig of OKW/Chi on 14th September 1945." A TICOM publication.

I 113. "Interrogation of Major Dr. Rudolf Hentze, Head of Gruppe IV (Cryptanalysis) General der Nachrichtenaufklaerung." A TICOM publication.

I 115. "Further Interrogation of Oberstlt. Mettig of OKW/Chi on the German Wireless Security Service (Funküberwachung). A TICOM publication.

I 116. "Report of Interrogation of Ltn. Alex Dettmann and Oberwachtmeister Sergius Samsonow of OKH (Gen.d.NA) at Oberursel, Germany, during August 1945." A TICOM publication.

I 120. "Translation of Homework by Obltn. W. Werther, Company Commander of 7/LN Rgt. 353, written on 12th August 1945 at A.D.I. (K)." A TICOM publication.

I 126. "Homework by Major Feichtner." A TICOM publication.

I 130. "Homework by Hauptmann Herold, O.C. Ln. Regt. III/353." A TICOM publication.

I 131. "Obstlt. Mettig of OKW/Chi on WA Pruef 7 and RLM/Forschungsamt." A TICOM publication.

I 135. "Homework by Lt. Ludwig of Chi-Stelle Ob.d.L. (Ref.B)." A TICOM publication.

I 142. "P/W Barthel's Account of German Work on British, American, Swedish, and French Machine Ciphers." A TICOM publication.

I 143. "Report on the Interrogation of Five Leading Germans at Nuerenberg on 27th September 1945." A TICOM publication.

I 144. "Further Interrogation of Lt. Muentz of 4 SKL III.

I 146. "Detailed Interrogation of Members of OKM 4 SKL III at Flensburg." A TICOM publication.

I 147. "Detailed Interrogation of Members of OKM 4 SKL III at Flensburg." A TICOM publication.

I 154. "Interrogation of Uffz. Rudolph Schneider of In 7/VI." A TICOM publication.

I 160. "Homework by Sonderfuehreer Kuehn of Gen. D. N. A. on General Organisation and Work of French Referat." A TICOM publication.

I 163. "Report on Interrogation of Hptm. Scheidl, Ltn. Sann and Ltn. Smolin, all of I/LN Rgt. 353 (East), on German Sigint Activity Against Russian Air Forces." A TICOM publication.

I 170. "Report on French and Greek Systems by Oberwachtmeister Dr. Otto Karl Winkler of OKH/FNAST 4." A TICOM publication.

I 172. "Interrogations of Hagen and Paschke of Pers Z S." A TICOM publication.

I 193. "Interrogation of SS Obersturmbahnfuehrer Urban, Liaison Officer of RSHA/VI with the Crypto Bureau of Hungarian General Staff." A TICOM publication.

IF 15. "Final Report of TICOM Team 1 on the Exploitation of Kaufbeuren and the Berchtezgaden area." From TICOM.

IF 40. "Final Report of TICOM Team 2." From TICOM.

IF 51. "Report of TICOM Team 4--visit to Southern Germany and Austria, 14th June to 12th July 1945." From TICOM.

IF 101. "Narrative and report of proceedings of TICOM Team 6, 11 April-6 July 1945." From TICOM.

IF 107. Interrogation of POW Werner K. H. Graupe regarding German cryptographic organization and solution of allied codes.

IF 108. Interrogation of Oblt. Arntz. CSDIC (U.K.) SIR 1606.

IF 120. First detailed interrogation report on Thomas Barthel. CSDIC/CMF/Y 40.

IF 123. "Consolidated report on information obtained from the following: Erdmann, Grubler, Hempel, Karrenberg, Schmitz, Suschowk. CSDIC (U.K.) SIR 1717.

IF 126. "Interrogation report on Kotschy and Boscheinen." CSDIC (U.K.) SIR 1335.

IF 132. "Notes by Huettenhain and Fricke on OKW/Chi and the German I. S." A TICOM publication.

IF 165. Special report by Kirby, on TICOM Team 6's relation with OKW/Chi personnel.

IF 166. Special report by Kirby on Sdf. Dr. Fricke.

IF 167. Final report on the visit of TICOM Team 5 to the Schliersee area.

IF 175. Seabourne report, Vol. XIII. "Cryptanalysis within the Luftwaffe SIS." From Commanding General, 9th Air Force.

IF 180. Seabourne Report, Vol. V. "The Chi-Stelle." From Commanding General, 9th Air Force.

IF 181. Seabourne Report, Vol. VI. "Origins of the Luftwaffe SIS and History of its Operations in the West." From Commanding General, 9th Air Force.
IF 182. Seabourne Report, Vol. VII. "Technical Operations in the West." From Commanding General, 9th Air Force.
IF 187. Seabourne Report, Vol. XII. "Technical Operations in the East." From Commanding General, 9th Air Force.
IF 188. Four Newspaper Articles. Subject: Goering's conversations concerning Austrian Anschluss. Associated Press. 4,5,6,7, November 1945.
IF 209. "Italian Communication Intelligence." Report by Admiral Maugin with U. S. Navy Introduction.
IF 1500. "Italian Intelligence Service: Report on "Organization and Working of the Servizio Informazioni Esercito (S.I.E.) within the Period 1/11/41--15/6/43." A TICOM Publication.
IF 1502. "First Detailed Interrogation Report of Guiseppe Samarughi." CSDIC/CMF/Y 29.
IF 1517. "First Detailed Interrogation of Augusto Bigi, who worked in the Cryptographic Section of SIM before the armistice and in SID afterward." CSDIC/CMF/Y 4.
IF 1518. "First Detailed Interrogation of Vittorio Gamba, director of SIM Cryptographic Section until Armistice." CSDIC/CMF/Y 7.
IF 1520. "First Detailed Interrogation of Guido Emer." CSDIC/CMF/Y 10.
IF 1523. "First Detailed Interrogation of Giovanni Gramola, pertaining to Turkish, French, British, and USA traffic." CSDIC (MAIN)/Y 24.
IF 1524. "First Detailed Interrogation Report on Three SID Cryptographers: de Witt, Biagi, Carlini." CSDIC/CMF/Y 32.
IF 1526. "Second Detailed Interrogation Report on Five Italian SID Cryptographers: de Witt, Biagi, Ulieni, Carlini, and Barbagallo." CSDIC/CMF/Y 35.
IF 1527. "First Detailed Interrogation Report of Alberto Barbagallo, Italian Naval Cryptographer." CSDIC/CMF/Y 34.

In 7/IV (Inspektion 7/IV).--Signal Security Agency of th Army High Command.
In 7/VI. (Oberkommando des Heeres, Inspektion 7/VI).--Inspectorate 7/VI.
Inspectorate 7/VI.--Oberkommando des Heeres, Inspektion 7/VI (OKH/In 7/VI, or simply In 7/VI). A predecessor of the Signal Intelligence Agency of the Army High Command (OKH/GdNA).
Inspektion 7/IV (In 7/IV).--Signal Security Agency of the Army High Command.
Intercept Control Station East.-- Horchleitstelle Ost (HLS Ost).--A predecessor of the Signal Intelligence Agency of the Army High Command (OKH/GdNA).
Italian Air Force Intelligence Service.--Servizio Informazioni Aeronautica (SIA).

Italian Defense Intelligence Service.--Servizio Informazioni Difesa (SID).

Jodl, Alfred, General. Chief of Operations Staff, Armed Forces High Command (Chef OKW/Ia).

Keitel, Wilhelm, Field Marshal. Chief of Armed Forces High Command (Chef OKW).

Kettler, Hugo, Col. Chief of OKW/Chi 1943-1945.

Kommandeur der Nachrichtenaufklaerung (KONA).--Army Signal Intelligence Regiment.

KONA (Kommandeur der Nachrichtenaufklaerung).--Army Signal Intelligence Regiment.

Krauss, _____, Admiral. Chief of OKM/4 SKL/III.

LN Regt (Luftnachrichtenregiment).--Air Signal Regiment.

Luftnachrichtenregiment (LN Regt).--Air Signal Regiment.

Meteorological Intercept Control.--Wetternachrichtenueberwachung (WENUEB).

Mettig, _____, Lt. Col. Second in command of OKW/Chi, Dec 1943-1945. Chief of Division a (cryptography).

Military Intelligence.--Abwehr.

Narodni Kommissariat Vnutrinikh Del (NKVD).--Peoples' Commissariat for Internal Affairs. A Russian secret police organization.

NKVD (Narodni Kommissariat Vnutrinikh Del).--People's Commissariat for Internal Affairs. A Russian secret police organization.

Oberkommando des Heeres/Chef des Heeresnachrichtenwesens (OKH/Chef HNW.--Chief Signal Officer of the Army.

Oberkommando des Heeres/General der Nachrichten Aufklaerung (OKH/GdNA).--Signal Intelligence Agency of the Army High Command.

Oberkommando des Heeres/Inspektion 7/VI (OKH/In 7/VI).--Inspectorate 7/VI of the Army High Command.

Oberkommando der Luftwaffe/Generalnachrichtenfuehrer II, Gruppe IV (OKL/Gen Nafue II/IV).--Group IV of Division II in the Office of the Chief Air Force Signal Officer.

Oberkommando der Luftwaffe/Luftnachrichtenabteilung 350 (OKL/LN Abt 350).--Signal Intelligence Agency of the Air Force High Command.

Oberkommando der Marine/4 Seekriegsleitung III (OKM/4 SKL III).--Signal Intelligence Agency of the Navy High Command.

Oberkommando der Wehrmacht/Chef Amtsgruppe Wehrmachtnachrichtenverbindungen (OKW/Chef Ag WNV).--Chief, Armed Forces Signal Communications Group.

Oberkommando der Wehrmacht/Chiffrierabteilung (OKW/Chi).--Signal Intelligence Agency of the Supreme Command Armed Forces.

Oberkommando der Wehrmacht/Waffenfuehrungsstab/Chef der Wehrmachtnachrichtenverbindungen (OKW/WFSt/Chef WNV).--Chief Signal Officer of the Supreme Command Armed Forces.

Oberkommando der Wehrmacht/Wehrmachtnachrichtenverbindungen/Funkueberwachung III (OKW/WNV/Fu III).--Radio Defense Corps.

OKH/Chef HNW (Oberkommando des Heeres/Chef des Heeresnachrichtenwesens).--Chief Signal Officer of the Army.

OKH/GdNA (Oberkommando des Heeres/General der Nachrichten Aufklaerung).--Signal Intelligence Agency of the Army High Command.

OKH/In 7/VI (Oberkommando des Heeres/Inspektion 7/VI).--Inspectorate 7/VI of the Army High Command.

OKL/Gen Nafue II/IV (Oberkommando der Luftwaffe/Generalnachrichtenfuehrer II, Gruppe IV).--Group IV of Division II in the Office of the Chief Air Force Signal Officer.

OKL/LN Abt 350 (Oberkommando der Luftwaffe/Luftnachrichtenabteilung 350).--Signal Intelligence Agency of the Air Force High Command.

OKM/4 SKL II (Oberkommando der Marine/4 Seekriegsleitung II).--Signal Security Agency of the Navy High Command.

OKM/4 SKL III (Oberkommando der Marine/4 Seekriegsleitung III).--Signal Intelligence Agency of the Navy High Command.

OKW/Chef Ag WNV (Oberkommando der Wehrmacht/Chef Amtsgruppe Wehrmachtnachrichtenverbindungen).--Chief, Armed Forces Signal Communications Group.

OKW/Chi (Oberkommando der Wehrmacht/Chiffrierabteilung).--The Signal Intelligence Agency of the Supreme Command Armed Forces.

OKW/WFSt/Chef WNV (Oberkommando der Wehrmacht/Waffenfuehrungsstab/Chef der Wehrmachtnachrichtenverbindungen).--Chief Signal Officer of the Supreme Command Armed Forces.

OKW/WNV/Fu III (Oberkommando der Wehrmacht/Wehrmachtnachrichtenverbindungen/Funkueberwachung III).--Radio Defense Corps.

People's Commissariat for Internal Affairs.--Narodni Kommissariat Vnutrinikh Del (NKVD). A Russian secret police organization.

Pers Z Chi (Chiffrierdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes).--Foreign Office Cryptographic Section.

Pers Z S (Sonderdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes).--Foreign Office Cryptanalytic Section.

Praun, Albert, Maj. Gen. Succeeded Fellgiebel as Chief Signal Officer of Armed Forces, 1944.

Radio Defense Corps of the Supreme Command Armed Forces.--Oberkommando der Wehrmacht/Wehrmachtnachrichtenverbindungen/Funkueberwachung III (OKW/WNV/Fu III).

Referat Vauck (Vauck's Section, named for its chief, First Lt. Vauck).--Agents Section of In 7/VI.

Reich Defense Ministry.--Reichswehrministerium.

Reich Main Security Office.--Reichsicherheitshauptamt (RSHA).

Reichsicherheitshauptamt (RSHA).--Reich Main Security Office.

Reichskriegsministerium.--German War Ministry.

Reichswehrministerium.-- Reich Defense Ministry.

von Ribbentrop, Joachim. German Foreign Minister.

Rommel, Erwin, Field Marshall. Commander of the Panzer Army of Africa in 1942.

RSHA (Reichsicherheitshauptamt).--Reich Main Security Office.

Servizio Informazioni Aeronautica (SIA).--Italian Air Force Intelligence Service.

Servizio Informazioni Difesa (SID).--Italian Defense Intelligence Service.

Servizio Informazioni Militari (SIM).--Cryptanalytic Section of the Italian Army Intelligence Service.

Servizio Informazioni Speciali (SIS).--Cryptanalytic Section of the Italin Navy Intelligence Service.

Schubert, _____, 1st Lt. Cryptanalyst with the Signal Intelligence Agency of the Army High Command. (OKH/GdNA).

SIA (Servizio Informazioni Aeronautica).--Italian Air Force Intelligence Service.

SID (Servizio Informazioni Difesa).--Italian Defense Intelligence Service.

Signal Intelligence Agency of the Air Force High Command.--Oberkommando der Luftwaffe/Luftnachrichtenabteilung 350 (OKL/LN Abt 350).

Signal Intelligence Agency of the Army High Command.--Oberkommando des Heeres/General der Nachrichten Aufklaerung (OKH/GdNA).

Signal Intelligence Agency of the Commander in Chief of the Air Force.--Chiffrierstelle, Oberbefehlshaber der Luftwaffe (Chi-Stelle Ob d L).

Signal Intelligence Agency of the Navy High Command.--Oberkommando der Marine/4 Seekriegsleitung III (OKM/4 SKL III).

Signal Intelligence Agency of the Supreme Command Armed Forces.--Oberkommando der Wehrmacht/Chiffrierabteilung (OKW/Chi).

Signal Security Agency of the Army High Command.--Inspektion 7/IV (In 7/IV).

Signal Security Agency of the Navy High Command.--Oberkommando der Marine/4 Seekriegsleitung II (OKM/4 SKL/II).

SIM (Servizio Informazioni Militari).--Cryptanalytic Section of the Italian Army Intelligence Service.

SIS (Servizio Informazioni Speciali).--Cryptanalytic Section of the Italian Navy Intelligence Service.

Sonderdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes (Pers Z S).--Foreign Office Cryptanalytic Section.

T 517. Stand der Arbeiten (Report of work done on British and American Naval Ciphers).

T 240. T 100 Serie 1726 (Recovered letter-figure Substitution Code).

T 2038. Berichte der Gruppen Polen, Finnland, Litauen, Lettland, Tscheckoslovakei, Jugoslavien, Bulgarien.

Target Intelligence Committee (TICOM). A joint combined committee organized in the fall of 1944 in England for the exploitation of European Axis signal intelligence centers of special interest.

TF 29. Die Ueberwachung des Nachrichtenverkehrs im Kriege (Supervision of Information Channels in War).

TF 31. "Schluesselanleitung zum Rosterschluessel 44 (RS 44)."

TF 32. "Rasterersatzverfahren."

TICOM (Target Intelligence Committee).--A joint combined committee organized in the fall of 1944 in England for the exploitation of European Axis signal intelligence centers of special interest.

Tranow, _____, Senior Specialist Dr. Head of Subsection IIIf (Britain and USA) of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III).

Verlaessliche Nachricht (VN).--"Reliable Report." Translation into German of decoded diplomatic message.

VN (Verlaessliche Nachricht).--"Reliable Report." Translation into German of decoded diplomatic message.

Waffenpruefung 7 (Wa Pruef 7).--Army Ordnance Development and Testing Group, Signal Branch.

Waffenschutzstaffel (Waffen-SS).--Armed Elite Guard. Components of Elite Guard serving at front.
Waffen-SS (Waffen-Schutzstaffel).--Armed Elite Guard. Components of Elite Guard serving at front.
Wa Pruef 7 (Waffenpruefung 7).--Army Ordnance Development and Testing Group, Signal Branch.
WENUEB (Wetternachrichtenueberwachung).--Meteorological Intercept Control.
Wenzel,_____, Senior Specialist. Head of Section 9 of the FA.
Wetternachrichtenueberwachung (WENUEB).--Meteorological Intercept Control.

TOP SECRET

THE SIX PRINCIPAL GERMAN CRYPTOLOGIC ORGANIZATIONS

AS OF SPRING, 1945.

CRYPTOLOGIC SECTIONS OF FOREIGN OFFICE

GOERING'S "RESEARCH" BUREAU

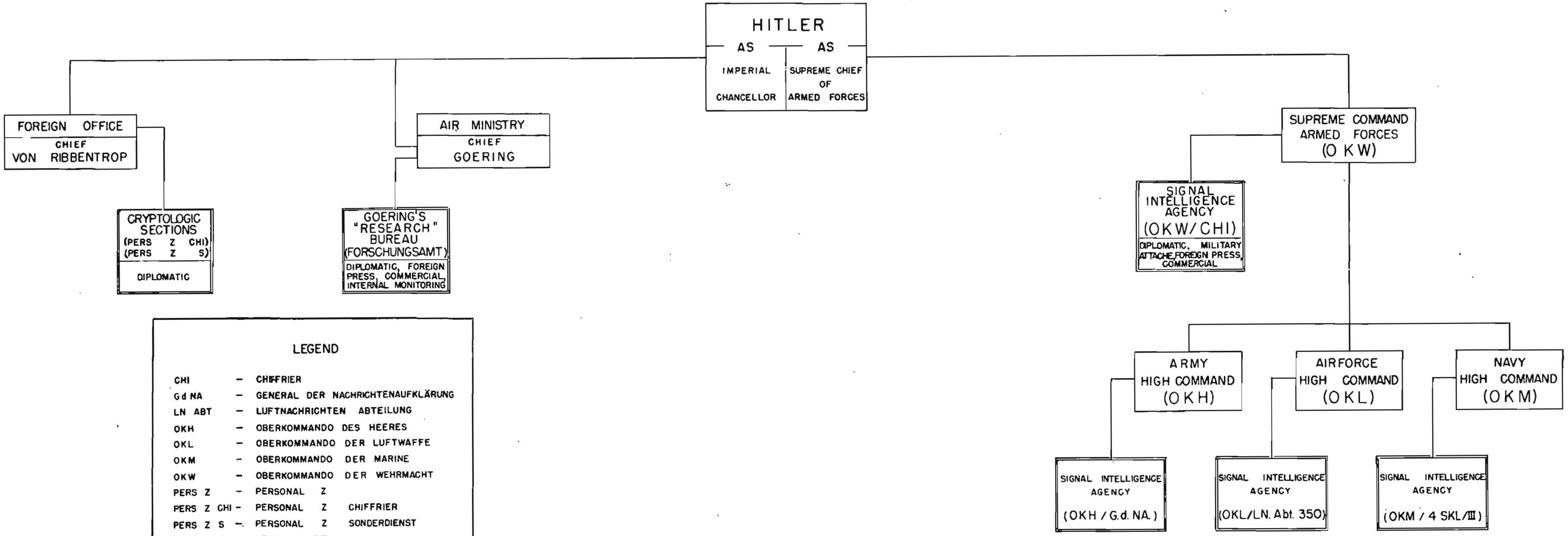
SIGNAL INTELLIGENCE AGENCY OF SUPREME COMMAND ARMED FORCES

SIGNAL INTELLIGENCE AGENCY OF ARMY HIGH COMMAND

SIGNAL INTELLIGENCE AGENCY OF AIRFORCE HIGH COMMAND

SIGNAL INTELLIGENCE AGENCY OF NAVY HIGH COMMAND

CHAINS OF COMMAND


HITLER
AS
AS
IMPERIAL CHANCELLOR
SUPREME CHIEF OF ARMED FORCES
FOREIGN OFFICE
CHIEF
VON RIBBENTROP
AIR MINISTRY
CHIEF
GOERING
CRYPTOLOGIC SECTIONS
(PERS Z CHI)
(PERS Z S)
DIPLOMATIC
GOERING'S "RESEARCH" BUREAU (FORSCHUNGSAMT)
DIPLOMATIC, FOREIGN PRESS, COMMERCIAL, INTERNAL MONITORING
SUPREME COMMAND ARMED FORCES (O K W)
SIGNAL INTELLIGENCE AGENCY (OKW/CHI)
DIPLOMATIC, MILITARY ATTACHE, FOREIGN PRESS, COMMERCIAL
ARMY HIGH COMMAND (O K H)
AIRFORCE HIGH COMMAND (O K L)
NAVY HIGH COMMAND (O K M)
SIGNAL INTELLIGENCE AGENCY (OKH / G.d. NA.)
SIGNAL INTELLIGENCE AGENCY (OKL/LN. Abt. 350)
SIGNAL INTELLIGENCE AGENCY (OKM / 4 SKL/III)

LEGEND

CHI	–	CHIFFRIER
Gd NA	–	GENERAL DER NACHRICHTENAUFKLÄRUNG
LN ABT	–	LUFTNACHRICHTEN ABTEILUNG
OKH	–	OBERKOMMANDO DES HEERES
OKL	–	OBERKOMMANDO DER LUFTWAFFE
OKM	–	OBERKOMMANDO DER MARINE
OKW	–	OBERKOMMANDO DER WEHRMACHT
PERS Z	–	PERSONAL Z
PERS Z CHI	–	PERSONAL Z CHIFFRIER
PERS Z S	–	PERSONAL Z SONDERDIENST
SKL	–	SEEKRIEGSLEITUNG

ESTIMATED TOTAL PERSONNEL – 31,000

CHART NO.

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
AFGHANISTAN 1	(ALL GOV'T AGENCIES, INCLUDING EMBASSIES, CONSULATES, FOREIGN OFFICE, PRIME MINISTER'S OFFICE, AND BANK.)	3-LETTER 1-PART CODE. (SOMETIMES ENCIPHERED WITH FIGURES, TWO FIGURES SUBSTITUTED FOR EACH LETTER, THEN SENT IN 1Ø-FIGURE GROUPS.)	?	AFGH. 1	(AFA)	1939 OR BEFORE-(CURRENT)	1942 PERS Z S	RECOVERED 1Ø% - 2Ø%	T 1Ø62 T 1Ø67 T 1Ø68 T 2Ø52	(ASA HAS RESULTS OF BRITISH PARTIAL RECOVERY, ABOUT 25% OF GROUPS, MAKING TRAFFIC PRACTICALLY 1ØØ% READABLE.)	--
ARGENTINA 1	DIPLOMATIC	5-LETTER 1-PART CODE. (1ØØ,ØØØ GROUPS.)	?	AB3	(ARA)	(1926-JANUARY 1946?)	? PERS Z S	RECOVERED LESS THAN 5%	T 3Ø15	(75% READABLE)	--
ARGENTINA 2	DIPLOMATIC	5-FIGURE 1-PART CODE. 95,ØØØ GROUPS IN MAIN VOCABULARY, TOTAL "11Ø,ØØØ." AFTER 1926 NUMBER 1ØØ ADDED TO EACH 5-PLACE GROUP.	?	?	(ARB)	(1926-1945)	1927 PERS Z S	SOLVED	D 16, REPORT 1, P 2 D 16, REPORT 2, P 3 I 172 P 5	(1ØØ% COMPROMISED)	--
ARGENTINA 3	DIPLOMATIC?	?-PART CODE. SOMETIMES ENCIPHERED BY MEANS OF AN EASY SYSTEM. IN MANY VOLUMES CONTAINING A LARGE NUMBER OF GROUPS.	?	?	?	? - ?	? SIM	?	IF 1518	(UNKNOWN)	--
ARGENTINA 4	DIPLOMATIC	?-PART CODE	?	?	?	?-194Ø-?	194Ø SIM	READ	IF 1524	(UNKNOWN)	--
BELGIUM 1	(COMMERCIAL AND DIPLOMATIC)	4-LETTER 1-PART CODE. SOMETIMES DIGRAPHICALLY ENCIPHERED WITH DAILY CHANGING TABLES.	?	?	(BEA) AND (BEB)	(BEA: 1939-CURRENT) (BEB: 1942-CURRENT)	194Ø PERS Z S 194Ø SIM PERHAPS ALSO FA	1ØØ% COMPROMISED BY SIM. READ BY PERS Z S.	I 22 P 19 I 25 P 2 D 54 P 12 P 18 IF 1517 P 3	(BEGAN BREAKING CODE 1943. COMPROMISED 1944. BEGAN BREAKING ENCIPHERMENT 1944. BOTH CURRENTLY READ.)	--
BELGIUM 2	DIPLOMATIC?	4-LETTER 1-PART CODE. ENCIPHERED DIGRAPHICALLY WITH SAME DAILY CHANGING TABLES AS BELGIUM 1. CODE GROUP "KAMI" = "FULL STOP."	?	?	?	?-1942. PERHAPS LATER.	194Ø PERS Z S	READ	I 22 P 19 D 54 P 12 P 18	(UNKNOWN)	--
BELGIUM 3	DIPLOMATIC	3-LETTER UNENCIPHERED CODE.	?	?	(BEC?)	(1943-CURRENT)	? ?	?	I 22 P 19	(BOOK 8Ø% BROKEN)	(BEC ONLY 3-LETTER UNENCIPHERED SYSTEM ASA KNOWS)
BELGIUM 4	COLONIAL	4-FIGURE ?-PART CODE. TRANSPOSED 1/2 OF GROUP AND USED DIGRAPHIC SUBSTITUTION FOR OTHER 1/2. COULD BE USED AS 5-FIGURE "IN WHICH CASE THE VALUE IN THE SECOND COLUMN HAD TO BE TAKEN."	?	?	?	? - ?	? PERS Z S	READ COMPLETELY	I 22 P 19	(UNKNOWN)	(NO FIGURE CODES KNOWN)
BELGIUM 5	DIPLOMATIC	4-FIGURE 4-LETTER 1-PART CODE ENCIPHERED BY 31 DAILY CHANGING TABLES, USED SAME DAY EACH MONTH.	?	?	?	? - 194Ø	? SIM	READ	IF 1522 P 3 P 8	(UNIDENTIFIED)	--

BELGIUM 6	DIPLOMATIC	4-FIGURE ?-PART CODE.	?	?	?	?-194Ø-?	194Ø SIM	READ	IF 1517
									IF 1524
										(UNIDENTIFIED)	--

BELGIUM 7	DIPLOMATIC?	?-FIGURE CODE OF 1Ø,ØØØ GROUPS ENCIPHERED WITH NUMBER AND LETTER TABLES OF 1ØØ PLACES.	?	?	?	? - 194Ø	194Ø PERS Z S	TABLES NEARLY SOLVED. MOST OF TRAFFIC READ BY 194Ø	D 54 P 12	(UNKNOWN)	(NO FIGURE CODES KNOWN)

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
BELGIUM	9	MILITARY.	3-FIGURE SYSTEM ENCIPHERED WITH SUBSTITUTION TABLES IN SUCH A WAY THAT THE FIRST FIGURE OF EACH GROUP REMAINED UNCHANGED AND THE SECOND AND THIRD WERE EACH ENCIPHERED INDIVIDUALLY.	?	?	?	? - ?	? OKW/CHI	READ	I 31 P 6	(UNKNOWN)	(NO FIGURE CODES KNOWN)
BOLIVIA	1	DIPLOMATIC	5-LETTER 1-PART CODE	?	?	(BVD?)	? - ?	? PERS Z S	RECOVERED LESS THAN 3%	T 1311	(25% READABLE)	--
BOLIVIA	2	DIPLOMATIC	5-FIGURE 1-PART CODE WITH 73,ØØØ GROUPS. ENCIPHERED WITH 1,ØØØ AND 1ØØ-PLACE TABLES AND BY TRANSPOSING THE GROUP ELEMENTS.	?	?	(BVA) AND (BVB)	(1939-CURRENT)	? PERS Z S	?	D 16, REPORT 2, P 4 T 1585	(1ØØ% COMPROMISED)	--
BOLIVIA	3	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION CIPHER USING 1Ø ALPHABETS.	?	?	?	?-1927-?	1927 PERS Z S	LONG TELEGRAMS SOLVED. SHORT ONES IMPOSSIBLE.	D 16, REPORT 1, P 3	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
BRAZIL	1	DIPLOMATIC	5-LETTER (2-PART) CODE WITH 82,ØØØ GROUPS.	?	BRAS B 2	(BZD)	(1937 OR BEFORE-CURRENT)	1941 OKW 1941 PERS Z S ? SIM	2,2ØØ GROUPS RECOVERED THEN 1ØØ% COMPROMISED BY OKW WHICH SENT COPY TO PERS Z S	D 16, 1941 REPORT, P 3 D 16, 1942 REPORT, P 4 T 3Ø16 IF 1518	(MORE THAN 5Ø% READABLE. STILL BEING RECOVERED.)	--
BRAZIL	2	DIPLOMATIC	5-LETTER 1-PART CODE WITH 165,625 GROUFS.	?	BRAS B 1	(BZC)	(1941-CURRENT)	1941 PERS Z S	2,2ØØ GROUPS RECOVERED BY 2Ø NOV. 1941. READ ALMOST WITHOUT GAP.	D 16, 1941 REPORT, P 3 D 16, 1942 REPORT, P 4 T 3Ø18	(MORE THAN 5Ø% READABLE. STILL BEING RECOVERED.)	--
BRAZIL	3	DIPLOMATIC	5-FIGURE (2-PART) CODE (REPAGINATED).	?	BRAS Z 3	(BZA)	(PRIOR TO 1941-CURRENT)	1942 PERS Z S	NOT READ	D 16, 1941 REPORT, P 3 D 16, 1942 REPORT, P 4 T 3Ø17	(MORE THAN 5Ø% READABLE; STILL BEING WORKED ON.)	--
BRAZIL	4	DIPLOMATIC	5-FIGURE 1-PART CODE WITH 1ØØ,ØØØ GROUPS.	?	BRAS Z 1	(BZI)	(1937 OR BEFORE - ?)	1941 PERS Z S	READ ALMOST WITHOUT GAP	D 16, 1941 REPORT, P 3 D 16, 1942 REPORT, P 4	(OVER 5Ø% READABLE.)	--
BRAZIL	5	DIPLOMATIC	5-FIGURE ?-PART CODE WITH 1ØØ,ØØØ GROUPS. ENCIPHERED WITH A TABLE OF LETTERS.	?	?	?	?-1941-1942-?	1941 PERS Z S	NOT READ	D 16, 1941 REPORT, P 3 D 16, 1942 REPORT, P 2	(UNIDENTIFIED)	--
BRAZIL	6	DIPLOMATIC	TWO 5-FIGURE CODES, REPAGINATIONS OF ITEM 4.	?	BRAS Z 7 BRAS Z 8	(BZK?)	(BZK: ?-1943)	1941 PERS Z S	READ ALMOST WITHOUT GAP	D 16, 1941 REPORT, P 3 D 16, 1942 REPORT, P 1	(BZK OVER 5Ø% READABLE.)	--
BRAZIL	7	?	5-FIGURE ?-PART CODE.	?	ZAHLEN II	?	? - ?	? PERS Z S	RECOVERED ABOUT 1%	T 3115	(UNIDENTIFIED)	--
BRAZIL	8	?	4-FIGURE ?-PART CODE, REPAGINATED.	?	ZAHLEN I	?	? - ?	? PERS Z S	RECOVERED 15% - 2Ø%	T 3Ø19	(UNIDENTIFIED)	--
BRAZIL	9	?	4-FIGURE ?-PART CODE, REPAGINATED.	?	ZAHLEN IV	?	? - ?	? ?	RECOVERED 5%	T 311Ø	(UNIDENTIFIED)	--
BRAZIL	1Ø	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	ZAHLEN V	?	? - ?	? ?	RECOVERED LESS THAN 1Ø%	T 3111	(UNIDENTIFIED)	--
BRAZIL	11	?	4-FIGURE ?-PART CODE, REPAGINATED.	?	ZAHLEN VI	?	? - ?	? ?	RECOVERED LESS THAN 3%	T 3112	(UNIDENTIFIED)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
BULGARIA	1	DIPLOMATIC	5-FIGURE 1-PART CODE, TWO FAGINATIONS.	?	?	(BUE)	(? - DEC 1945)	? PERS Z S	RECOVERED ABOUT 5Ø%	T 2Ø	(CODE RECOVERED .5% BEFORE RECEIPT OF COPY FROM TICOM.)	--
BULGARIA	2	DIPLOMATIC	5-FIGURE 1-PART CODE, TWO PAGINATIONS. RANGE 36,4ØØ.	88844	BD 15	(BUO)	(1938-JAN 1946)	? PERS Z S ? SIM	RECOVERED 75%; LATER 1ØØ% COMPROMISED.	T 1192 T 2125 T 2339 IF 1525	(CODE RECOVERED ABOUT 2%; LATER 1ØØ% COMPROMISED.)	--
BULGARIA	3	DIPLOMATIC	5-FIGURE 1-PART CODE, REFAGINATED.	?	BD 3Ø	(BUJ)	(? - 1945)	? PERS Z S	RECOVERED 3Ø%-4Ø%	T 24	(NOT WORKED ON BEFORE RECEIPT OF TICOM COPY.)	--
BULGARIA	4	DIPLOMATIC	5-FIGURE 1-PART CODE.	?	BD 19	?	? - ?	? PERS Z S	RECOVERED 5%	T 2335	(UNIDENTIFIED)	--
BULGARIA	5	DIPLOMATIC	5-FIGURE 1-PART CODE.	?	BD 25	?	? - 1944 - ?	? PERS Z S	RECOVERED 1Ø%	T 2334	(UNIDENTIFIED)	--
BULGARIA	6	DIPLOMATIC	5-FIGURE 1-PART CODE.	?	BD 27	?	? - ?	? PERS Z S	4Ø% - 5Ø% RECOVERED	T 2353	(UNIDENTIFIED)	--
BULGARIA	7	DIPLOMATIC	5-FIGURE 1-PART CODE.	?	BD 28	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 1176	(UNIDENTIFIED)	--
BULGARIA	8	DIPLOMATIC	5-FIGURE 1-PART CODE.	?	BD 33	?	? - ?	? PERS Z S	RECOVERED 5%	T 2333	(UNIDENTIFIED)	--
BULGARIA	9	DIPLOMATIC	5-FIGURE 1-PART CODE. INDICATOR: 33311.	?	BD 16	?	? - ?	? PERS Z S	RECOVERED 1Ø% - 15%	T 12; T 13 T 1178 T 1177 T 1179 T 1181 T 2331 T 2332	(UNIDENTIFIED)	--
BULGARIA	10	DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	BD 1	?	? - ?	? PERS Z S	RECOVERED ABOUT 5%	T 2116	(UNIDENTIFIED)	--
BULGARIA	11	DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	BD 3	?	? - ?	? PERS Z S	RECOVERED 5% - 1Ø%	T 2161	(UNIDENTIFIED)	--
BULGARIA	12	DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	BD 26	?	? - ?	? PERS Z S	RECOVERED ABOUT 1Ø%	T 2147	(UNIDENTIFIED)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
BULGARIA	13	DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	BD 31	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 2379	(UNIDENTIFIED)	--
BULGARIA	14	DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	BD 35	?	? - ?	? PERS Z S	VERY LITTLE SUCCESS	T 1185 T 1184	(UNIDENTIFIED)	--
BULGARIA	15	DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	"N.B.D. NEUER"	?	? - ?	? PERS Z S	RECOVERED 15% - 20%	T 2134	(UNIDENTIFIED)	--
BULGARIA	16	PROBABLY DIPLOMATIC	5-FIGURE PROBABLY 1-PART CODE.	?	BULG. 885	?	? - ?	? PERS Z S	VERY LITTLE SUCCESS	T 2135	(UNIDENTIFIED)	--
BULGARIA	17	DIPLOMATIC	5-FIGURE ?-PART CODE.	?	BD 14	?	? - ?	? PERS Z S	RECOVERED 20% - 25%	T 2130	(UNIDENTIFIED)	--
BULGARIA	18	PROBABLY DIPLOMATIC	5-FIGURE ?-PART CODE.	?	"720 1-15"	?	? - ?	? PERS Z S	?	T 2213	(UNIDENTIFIED)	--
BULGARIA	19	PROBABLY DIPLOMATIC	5-FIGURE ?-PART CODE.	?	"062 825 1-15"	?	? - ?	? PERS Z S	?	T 2214	(UNIDENTIFIED)	--
BULGARIA	20	PROBABLY DIPLOMATIC	5-FIGURE ?-PART CODE.	?	"095"	?	? - 1927 - ?	1927 PERS Z S	?	T 2127	(UNIDENTIFIED)	--
BULGARIA	21	PROBABLY DIPLOMATIC	5-FIGURE ?-PART CODE.	?	"507 16-21"	?	? - 1932 - ?	? PERS Z S	RECOVERED LESS THAN 1%	T 2174	(UNIDENTIFIED)	--
BULGARIA	22	PROBABLY DIPLOMATIC	5-FIGURE ?-PART CODE	?	"698"	?	? - ?	? PERS Z S	?	T 2157	(UNIDENTIFIED)	--
BULGARIA	23	MILITARY	5-FIGURE 1-PART CODE	?	BM 7	?	? - ?	? PERS Z S	RECOVERED 5% - 10%	T 2165	(UNKNOWN)	--
BULGARIA	24	MILITARY	5-FIGURE 1-PART CODE	?	BM C 5	?	? - ?	? PERS Z S	RECOVERED LESS THAN 10%	T 2168	(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET~~

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
BULGARIA 25	MILITARY	5-FIGURE ?-PART CODE.	?	BM C 1	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1%	T 2167	(UNKNOWN)	--
BULGARIA 26	MILITARY	5-FIGURE ?-PART CODE WITH APPARENTLY FOUR DIFFERENT POSSIBILITIES FOR THE FIRST THREE FIGURES.	?	BM 11	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1Ø%	T 2169	(UNKNOWN)	--
BULGARIA 27	MILITARY	5-FIGURE ?-PART CODE.	?	BM 12	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1%	T 2132	(UNKNOWN)	--
BULGARIA 28	?	5-FIGURE 1-PART CODE.	?	?	?	? - ?	? PERS Z S	RECOVERED 25%	T 118Ø	(UNKNOWN)	--
BULGARIA 29	?	5-FIGURE 1-PART CODE.	?	"43Ø 16-31"	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1Ø%	T 127Ø	(UNKNOWN)	--
BULGARIA 30	?	5-FIGURE 1-PART CODE.	?	BG B 2	?	? - ?	? PERS Z S	RECOVERED 2Ø%	T 2145	(UNKNOWN)	--
BULGARIA 31	?	5-FIGURE 1-PART CODE.	?	"Ø88 ABD 1-15"	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 2162 T 2163	(UNKNOWN)	--
BULGARIA 32	?	5-FIGURE 1-PART CODE	?	?	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1%	T 2133	(UNKNOWN)	--
BULGARIA 33	?	5-FIGURE 1-PART CODE.	?	"BU 11"	?	? - ?	? PERS Z S	RECOVERED 5% - 1Ø%	T 2149	(UNKNOWN)	--
BULGARIA 34	?	5-FIGURE ?-PART CODE. POSSIBLE 6Ø,ØØØ GROUPS.	?	"BU 4"	?	? - ?	? PERS Z S	RECOVERED ABOUT 1Ø%	T 2159	(UNKNOWN)	--
BULGARIA 35	?	5-FIGURE ?-PART CODE. RECONSTRUCTED ON BASIS OF 1ØØ,ØØØ VALUES.	?	36633 M8	?	? - ?	? PERS Z S	VERY LITTLE SUCCESS	T 2166	(UNKNOWN)	--
BULGARIA 36	?	5-FIGURE ?-PART CODE.	?	?	?	?-1936-1937-?	? PERS Z S	RECOVERED LESS THAN 1%	T 2172	(UNKNOWN)	--
BULGARIA 37	?	5-FIGURE ?-PART CODE.	?	"BULG HOF CODE 4C"	?	? - ?	? PERS Z S	VERY LITTLE SUCCESS	T 2121	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
BULGARIA	38	?	5-FIGURE ?-PART CODE	?	"36333-OHNE 5 16-21"	?	?-1929-?	1929 PERS Z S	VERY LITTLE SUCCESS	T 2129	(UNKNOWN)	--
BULGARIA	39	?	5-FIGURE ?-PART CODE	?	"NHC OR N4C"	?	? - ?	? PERS Z S	?	T 2178	(UNKNOWN)	--
BULGARIA	40	?	5-FIGURE ?-PART CODE	?	"A2 16C 1C-31"	?	? - ?	? PERS Z S	?	T 2160	(UNKNOWN)	--
BULGARIA	41	?	5-FIGURE ?-PART CODE	?	"Ø4C"	?	? - ?	? PERS Z S	?	T 2136	(UNKNOWN)	--
BULGARIA	42	DIPLOMATIC	4-FIGURE 1-PART CODE	?	BD 26	?	? - ?	? PERS Z S	RECOVERED 5%	T 2339	(UNKNOWN)	--
BULGARIA	43	DIPLOMATIC	4-FIGURE 1-PART CODE	?	"JZ.-C. REG. 1"	?	? - ?	? PERS Z S	RECOVERED 30%-40%	T 2131	(UNKNOWN)	--
BULGARIA	44	DIPLOMATIC	4-FIGURE ?-PART CODE	?	BD 27	?	? - ?	? PERS Z S	VERY LITTLE SUCCESS	T 2337	(UNKNOWN)	--
BULGARIA	45	?	4-FIGURE 1-PART CODE	?	"2 FRIEDRICHS"	?	? - ?	? PERS Z S	RECOVERED ABOUT 25%	T 2177	(UNKNOWN)	--
BULGARIA	46	MILITARY ATTACHE?	?-PART CODE. FIRST GROUP AFTER ADDRESS WAS BALKAN.	?	?	?	? - ?	? SIM	NOT READ	IF 1525	(UNKNOWN)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS

AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
CHILE	1	?	5-FIGURE 5-LETTER 2-PART CODE. 1ØØ,ØØØ GROUPS. DIVIDED INTO THREE CONSECUTIVE BOOKS.	?	?	?	BEFORE 1941	? SIM	1ØØ% COMPROMISED.	IF 1517 IF 1518	(UNKNOWN)	--
CHILE	2	DIPLOMATIC	5-LETTER 1-PART CODE. 26,5ØØ GROUPS. FIRST TWO AND LAST TWO LETTERS OF EACH GROUP ENCIPHERED WITH DIGRAPHIC SUBSTITUTION TABLE..	?	?	?	1924 - ?	1924 PERS Z S	SOLVED.	D 16, REPORT 1, P 2	(UNKNOWN)	--
CHILE	3	CONSULAR	5-LETTER ?-PART CODE.	?	CHILE KONSULAR CODE	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 3Ø26	(UNKNOWN)	--
CHILE	4	DIPLOMATIC	1-TO 4-LETTER 1-PART CODE. 42,ØØØ GROUPS.	CLAVE SOLAR	?	(CLA)	(1936-CURRENT)	194Ø PERS Z S	SOLVED. LATER 1ØØ% COMPROMISED.	D 16, REPORT #2, P 4 D 16, REPORT #4, P 4	(COMPROMISED 1ØØ% -- DATE OF EDITION 1936.)	--
CHILE	5	DIPLOMATIC	4-LETTER ?-PART CODE.	?	?	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 14ØØ T 3Ø25	(UNKNOWN)	--
CHILE	6	DIPLOMATIC	?-PART CODE WITH COMPLICATED ENCIPHERMENT.	?	?	?	1941-?	? SIM	?	IF 1517 IF 1518	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
CHINA 1	?	5-LETTER ?-PART CODE.	?	?	?	?	? PERS Z S	RECOVERED LESS THAN 1Ø%	T 1157	(UNKNOWN)	--
CHINA 2	(DIPLOMATIC)	4-LETTER (1-PART) CODE. THOUGHT TO HAVE BEEN ENCODED IN CHINESE CHARACTERS AND ENCIPHERED IN LATIN CHARACTERS.	?	?	(CNS) OR (CNF) OR (CNJ)	(CNS, 1944 - CURRENT) (CNF, 1942 - CURRENT) (CNJ, 1944 - CURRENT)	? SIM	NOT READ	IF 1518 P 5	(CNS, CNF, CNJ BROKEN AND READ BY ASA.)	--
CHINA 3	DIPLOMATIC AND CONSULAR	4-LETTER 1-PART CODE. SOMETIMES ENCIPHERED.	OJYJ	?	(CNS)	(1943-CURRENT)	? PERS Z S	RECOVERED SUBSTITUTION ALPHABETS	T 3	(RECOVERED BY BRITISH. BOOK GIVEN TO ASA. BEING READ.)	--
CHINA 4	DIPLOMATIC	4-LETTER ?-PART CODE, ALTERNATE CONSONANT AND VOWELS.	HUKO	?	?	?	? PERS Z S	PARTIALLY BROKEN	T 2297	(UNKNOWN)	--
CHINA 5	DIPLOMATIC	4-LETTER ?-PART CODE, OCCASIONALLY DIGRAPHICALLY ENCIPHERED.	?	?	?	1935-1937	? PERS Z S	CODE AND ENCIPHERMENT PARTIALLY BROKEN	T 2112 T 2113	(UNKNOWN)	--
CHINA 6	DIPLOMATIC	4-LETTER ?-PART CODE.	?	?	?	?	? PERS Z S	PROBABLY READ. PARTIALLY BROKEN.	T 2291	(UNKNOWN)	--
CHINA 7	DIPLOMATIC	4-LETTER ?-PART CODE, OCCASIONALLY DIGRAPHICALLY ENCIPHERED.	?	?	?	1926-1929	? PERS Z S	FAIRLY COMPLETE RECOVERY OF BOTH CODE AND ENCIPHERMENT	T 2111	(UNKNOWN)	--
CHINA 8	COMMERCIAL	4-LETTER ?-PART CODE, OCCASIONALLY ENCIPHERED DIGRAPHICALLY. USED BETWEEN CHINA AND A CHINESE COMMERCIAL MISSION IN GERMANY.	?	?	?	1937-1938	? PERS Z S	CODE AND ENCIPHERMENT PARTIALLY BROKEN	T 2Ø1Ø T 211Ø	(UNKNOWN)	--
CHINA 9	(DIPLOMATIC)	3-LETTER 2-PART CODE. (USUALLY ENCIPHERED. HAD MANY ENCIPHERMENTS.)	HNM	?	(CNL)	(1943-CURRENT)	? PERS Z S	?	T 1159	(SOLVED BY ASA 1944)	--
CHINA 1Ø	DIPLOMATIC	3-LETTER 1-PART CODE. SOMETIMES ENCIPHERED.	WIN	?	(CNC)	(1939-CURRENT)	? PERS Z S	PARTIALLY READ	T 4	(PARTIALLY RECONSTRUCTED COMPROMISED COPY RECEIVED. COMPLETED BREAKING. NOW BEING READ.)	--
CHINA 11	DIPLOMATIC	3-LETTER 1-PART CODE.	?	UTI	?	?	1941 PERS Z S	SOLVED	I 22 P 21 T 2Ø2 T 214 T 198 T 2296	(UNKNOWN)	
CHINA 12	(DIPLOMATIC)	3-LETTER 1-PART CODE. SOMETIMES ENCIPHERED. HAD MANY ENCIPHERMENTS.	?	DRYO	(CNB)	(? - 194Ø - CURRENT)	? PERS Z S ? OKW	COMPLETELY READ	T 2 T 2292	(PLAIN CODE AND LETTER ENCIPHERMENTS NOT BEING WORKED ON -- LOW INTELLIGENCE VALUE. NUMBER ENCIPHERMENT BEING READ.)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
CHINA	13	MILITARY ATTACHE	3-LETTER ?-PART CODE. ENCIPHERMENT CONSISTED OF TRANSPOSITION WITHIN THE CODE GROUPS. FIRST GROUPS OF TRAFFIC WERE EFR, SKW, OR JKW.	?	?	?	? - 1943	? PERS Z S	ENCIPHERMENT SOLVED. NOT READ.	I 22 P 8	(UNKNOWN)	--
CHINA	14	MILITARY	3-LETTER ?-PART CODE. UNENCIPHERED. DISCRIMINANT WAS NKDBN. CONTAINED MANY SPELLS, USING SIMPLE SUBSTITUTION.	?	?	?	?	? PERS Z S	INVESTIGATED	I 22 P 8	(UNIDENTIFIED)	--
CHINA	15	?	"POST CODE"	?	?	?	?	? OKW	?	I 15Ø P 9	(UNKNOWN)	--
CHINA	16	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION. 26 ALPHABETS. (USED ON CODES CNF, CNL, CNS, CNU, AND CNW.)	SXS	?	(SXS)	(1944-CURRENT)	? PERS Z S	SOLVED	T 3	(ALPHABETS SENT BY BRITISH.)	--
CHINA	17	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION. 1Ø ALPHABETS. (USED WITH CODES CNB, CNC, CNF, CNJ, CNL, CNS, CNU, AND CNW.)	AMC	?	(AMC)	(1943-CURRENT)	? PERS Z S	SOLVED	T 3	(ALPHABETS SENT BY BRITISH.)	--
CHINA	18	DIPLOMATIC	MONOALPHABETIC SUBSTITUTION. (USED WITH CNB, CNC, CND, CNF, CNJ, CNL, CNS, CNU, AND CNW.)	AMA	?	(AMA)	(1943-CURRENT)	? PERS Z S	SOLVED	T 3	(ALPHABETS SENT BY BRITISH.)	--
CHINA	19	DIPLOMATIC	MONOALPHABETIC SUBSTITUTION. DAILY CHANGING ALPHABETS. (USED ON CODES CNB, CNC, CND, CNF.)	ECTIA	?	(ECTIA)	(1943-1945)	? PERS Z S	SOLVED	T 3	(ALPHABETS SENT BY BRITISH.)	--
COLOMBIA	1	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION CIPHER WITH 5 TO 15 ALPHABETS.	?	?	?	? - 1942 - ?	1941 PERS Z S	READ	D 15, REPORT 2, P 4	(UNKNOWN)	--
COLOMBIA	2	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION CIPHER WITH 5 ALPHABETS.	?	?	(COA)	(1927-CURRENT)	1927 PERS Z S	READ	D 16, REPORT 1, P 3	(READABLE)	--
CZECHOSLOVAKIA	1	AIR FORCE	TRANSPOSITION CIPHER.	?	?	?	? - 1937 - ?	1937 OKL	NOT BROKEN	I 121 P 7	(UNKNOWN)	--
CZECHOSLOVAKIA	2	AIR FORCE	DOUBLE TRANSPOSITION CIPHER.	?	?	?	? - 1938 - ?	1938 OKL	SOLVED.	I 112 P 6	(UNKNOWN)	--
CZECHOSLOVAKIA	3	?	DOUBLE TRANSPOSITION CIPHER.	?	?	?	? - 1938 - ?	1938 OKL	?	I 112 P 1Ø	(UNKNOWN)	--
CZECHOSLOVAKIA	4	ARMY	VARIOUS POLYALPHABETIC SUBSTITUTION CIPHERS. USED IN 1925, 1926, AND 1927.	?	?	?	1925-1927	OKL	SOLVED	T 1794	(UNKNOWN)	--
CZECHOSLOVAKIA	5	COMMERCIAL	CODE USED BY SKODA FIRM TO IRAN AND IRAG CONCERNED WITH BRIDGE BUILDING PROJECTS.	?	?	?	? - 1935 - ?	1935 OKL	SOLVED	I 162 P 2	(UNKNOWN)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES).

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
DENMARK 1	DIPLOMATIC	CODE	?	?	?	? - ?	BEFORE 1940 FA	50% OF TRAFFIC READ UP TO 1940	I 162 P 3	(UNIDENTIFIED)	--
DOMINICAN REPUBLIC 1	DIPLOMATIC	SUBSTITUTION CIPHER WITH 5 ALPHABETS.	?	?	(DOA)	?-(CURRENT)	1941 PERS Z S	COMPLETELY READ	D 16, REPORT 2, P 4 T 2507	(READABLE)	--
ECUADOR 1	DIPLOMATIC	2-LETTER 3-LETTER 4-LETTER 2-PART CODE. GROUPS IN FROM OF VC, VCC, OR VCCC. TRANSMITTED IN 10-LETTER GROUPS.	?	?	?	1923-?	1926 PERS Z S	COMPLETELY READ	D 16, REPORT 1, P 3	(UNKNOWN)	--
ECUADOR 2	DIPLOMATIC	2-LETTER 4-LETTER 1-PART CODE. 61,945 GROUPS. INTERSPERSED CLEAR TEXT.	?	?	(ECA)	(?-1941-CURRENT)	1941 PERS Z S ? SIM	SOLVED	D 16, REPORT 2, P 4 T 1592	(80% READABLE)	--
EGYPT 1	DIPLOMATIC?	TWO ?5-FIGURE ?-PART CODES, VALUES IN FRENCH. ENCIPHERED.	?	?	?	? - ?	? SIM	?	IF 1518	(UNIDENTIFIED)	--
ETHIOPIA 1	DIPLOMATIC	5-FIGURE 1-PART CODE. VALUES IN FRENCH.	?	"AETH.1"	(ETA)	(?-CURRENT)	? ?	RECOVERED LESS THAN 5%	T 1061	(ALMOST COMPLETELY READABLE.)	--
ETHIOPIA 2	DIPLOMATIC	DOUBLE TRANSPOSITION	?	?	(ETB)	(?-1944-CURRENT)	? OKH	NO SUCCESS	T 57	(CURRENTLY BEING ATTACKED; NOT YET BROKEN.)	--
FINLAND 1	DIPLOMATIC AND MILITARY ATTACHE	HAGELIN. (5-WHEEL AND 6-WHEEL MACHINES.)	?	?	(FIA-1) (FIA-2)	(1942-CURRENT)	? OKW ? FA	NOT READ BY OKW. READ OCCASIONALLY BY FA.	I 31 P 7 I 54 P 2 I 25 P 6	(SOLVED IN 1943. FIA-1 STILL BEING READ; FIA-2 NOT READABLE, SINCE TABLES CHANGED, BUT BEING WORKED ON.)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS - CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE-- VICHY, FREE FRANCE 1	(DIPLOMATIC)	CIPHER MACHINE, HAGELIN M-2Ø9. (6 WHEELS, VARIBLE PINS, VAPIABLE LUGS, NO SLIDE, MAXIMUM KICK OF 27 OVERLAPPED.)	(M-2Ø9)	?	(FRENCH M-2Ø9)	DURING SAN FRANCISCO CONFERENCE, 1945	1943 OKW	PROBABLY READ	I 58 P 3 I 136 P 2	(READ FRENCH HAGELIN DURING SAN FRANCISCO CONFERENCE.)	--
FRANCE 2	DIPLOMATIC?	5-LETTER 1-PART COCE, APPROXIMATELY 2Ø,ØØØ GROUPS.	?	9	?	?-194Ø-?	194Ø PERS Z S	?	D 54 P 12	(UNIDENTIFIED)	--
FRANCE-- VICHY, FREE FRANCE 3	DIPLOMATIC	4-LETTER 2-PART CODE.	PC 149	6 VARIA 1-352; F 2	(FRG)	(1937-CURRENT)	1944 SID PRIOR TO 1941 PERS Z S	75% RECONSTRUCTED BY ITALIANS. COMPROMISED BY ITALIANS AND GERMANS. READABLE BUT NOT WORKED ON BY PERS Z S DUE TO LACK OF PERSONNEL.	T 1521 T 15Ø4 T 3251 D 54 P 12	(RECOVERED AT ASA IN 1942.)	--
FRANCE 4	DIPLOMATIC?	4-LETTER 2-PART CODE. VCVV OR VCVC. (SIMILAR TO FRG.)	?	F.B. 1, VOL. 1	?	? - ?	? PERS Z S	RECOVERED 5Ø%	T 2Ø33 T 2Ø34 T 2Ø35	(UNKNOWN)	--
FRANCE 5	DIPLOMATIC	4-LETTER 2-PART CODE.	?	?	?	?-1937-?	? OKW	COMPLETELY READ	T 898	(UNKNOWN)	--
FRANCE 6	DIPLOMATIC	4-LETTER (1-PART) CODE, APPROXIMATELY 2Ø,ØØØ GROUPS. (UNENCIPHERED)	VESTA	?	(FCF)	1941-(1944)	AFTER 1941 PERS Z S	RECOVERED 15%	D 54 P 12 T 3256	(BEGAN WORK 1944. COMPROMISED CODE. READ. SCANT MATERIAL.)	--
FRANCE 7	DIPLOMATIC?	4-LETTER 4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	?	?	?	? - ?	? PERS Z S	RECOVERED 4Ø%	T 2Ø19	(UNIDENTIFIED)	--
FRANCE 8	DIPLOMATIC	5-FIGURE 2-PART CODE.	?	F 21	?	1929	? GERMANS	WORKED ON. KNEW SYSTEM.	T 3536 T 3539	(UNIDENTIFIED)	--
FRANCE-- FREE FRANCE 9	DIPLOMATIC?	5-FIGURE 2-PART CODE ENCIPHERED BY SINGLE TRANSPOSITION KEY TAKEN FROM THE ENCODE. KEY VARIES FROM 12 TO 29 LETTERS, NONE DIVISIBLE BY 5.	"1918 TYPE C"	?	?	?-1939-?	? OKW	COMPROMISED	T 1728	(UNIDENTIFIED)	--
FRANCE 1Ø	DIPLOMATIC	5-FIGURE 2-PART CODE.	?	R 2	?	? - ?	? GERMANS	RECONSTRUCTED 15%	T 3152	(UNKNOWN)	--
FRANCE 11	DIPLOMATIC?	5-FIGURE 2-PART CODE.	?	R 4. GEGEN-CODE	?	? - ?	? PERS Z S	PARTIALLY RECONSTRUCTED	T 3Ø88	(UNKNOWN)	--
FRANCE-- FREE FRANCE 12	DIPLOMATIC?	5-FIGURE ?-PART CODE, ENCIPHERED BY TRANSPOSITION.	?	?	?	?-1941-?	1941 OKW ? PERS Z S	NO SUCCESS.	I 58 P 6	(UNIDENTIFIED)	--
FRANCE-- (VICHY) 13	(DIPLOMATIC)	4-FIGURE 2-PART CODE. (UNENCIPHERED)	PC 151	8Ø. 7. BLN. 1Ø3 1-- VAR: 6Ø1--	(FAF)	(1941-1944)	? GERMANS	RECOVERED 5Ø%; COMPROMISED 1ØØ%	T 3246 T 3247 T 15Ø5	(BROKEN WITH HELP FROM GCCS. 5Ø% RECOVERED, 9Ø% READABLE.)	--

~~TOP SECRET~~

3

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 14	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	C 51	?	? - ?	? GERMANS	ABOUT 35% RECOVERED	T 3149	(UNKNOWN)	--
FRANCE 15	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	?	?	?-1937?-?	? OKW	RECOVERED 40%; 85% READABLE.	T 929	(UNKNOWN)	--
FRANCE 16	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	471 BERLIN 1:A-300 E	?	? - ?	? GERMANS	ABOUT 65% RECOVERED	T 3147	(UNKNOWN)	--
FRANCE 17	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	NA 5	?	? - ?	? GERMANS	ABOUT 25% RECONSTRUCTED	T 3148	(UNKNOWN)	--
FRANCE 18	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	FC	?	? - ?	? GERMANS	READ.	T 2536	(UNKNOWN).	--
FRANCE 19	DIPLOMATIC	4-FIGURE 2-PART CODE. PERHAPS USED IN THE NEAR EAST.	?	34 VARIA 1-599	?	? - ?	? GERMANS	ABOUT 30% RECOVERED	T 3155	(UNKNOWN)	--
FRANCE 2Ø	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	11 NAH. OSTEN	?	? - ?	1941 PERS Z S	RECOVERED 25%	T 3249 D 54 P 12	(UNKNOWN)	--
FRANCE--(VICHY) 21	DIPLOMATIC	4-FIGURE 2-PART CODE. (ENCIPHERED WITH RUNNING ADDITIVE.)	(Z 4)	12 FERN-, OST	(FAJ)	(1941)-1943	1943 PERS Z S	RECOVERED 2Ø%	T 325Ø D 54 P 12	(BOOK COMPROMISED 1942.)	--
FRANCE 22	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	FZC 19	?	? - ?	? OKW	RECONSTRUCTED 3Ø%	T 885	(UNKNOWN)	--
FRANCE 23	(DIPLOMATIC)	4-FIGURE (2-PART) CODE. (5 ENCIPHERMENTS USED CONSISTING OF 1 SUBSTITUTION AND 4 ADDITIVE SYSTEMS.)	CTX	?	(FRB)	1944-(CURRENT)	1944 SID	PROBABLY NOT SOLVED	T 1522	(CODE BOOK COMPROMISED 1943. COMPROMISED SUBSTITUTION TABLES AFTER SOME WORK DONE. ADDITIVES BROKEN. ALMOST ALL TRAFFIC COMPLETELY READ.)	--
FRANCE 24	DIPLOMATIC	4-FIGURE 2-PART CODE, (UNENCIPHERED).	(PC 154)	17	(FAE)	(1941-1944)	? GERMANS	RECONSTRUCTED 75%	T 3241 T 3242 T 3243 T 33ØØ T 33Ø1	(BROKEN WITH HELP OF GCCS. RECOVERED 65%.)	--
FRANCE 25	DIPLOMATIC	4-FIGURE 2-PART CODE, (UNENCIPHERED).	(PC 152)	14 BERLIN	(FAC)	(1941-1944)	? GERMANS	RECOVERED 5Ø%	T 3235	(ENCODE COMPROMISED 1943. REMAINDER LARGELY SOLVED.)	--
FRANCE 26	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	?	?	? - ?	? PERS Z S	RECOVERED 1Ø%	T 31Ø1	(UNKNOWN)	--
FRANCE 27	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	111 1-5ØØ	?	? - ?	? PERS Z S	RECOVERED 5Ø%	T 3Ø91	(UNKNOWN)	--
FRANCE 28	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	?	?	? - ?	? GERMANS	COMPROMISED	T 2441	(UNIDENTIFIED)	--
FRANCE 29	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	15 VARIA	?	? - ?	? GERMANS	RECOVERED 35%	T 3236	(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 3Ø	DIPLOMATIC	4-FIGURE 2-PART CODE. UNENCIPHERED. DIGITS IN INDICATOR ADD TO 18.	PC 156; TNU	F 18	(FRH)	1945-(CURRENT)	1945 SID	RECONSTRUCTED 75% BY SID. READ.	T 733; T 745 T 735; T 15Ø8 T 1511; T 152Ø T 1524; T 1521 IF 1526 P 4	(COMPLETELY COMPROMISED BEFORE CODE WAS USED.)	--
FRANCE-- 31 FREE FRANCE	DIPLOMATIC	4-FIGURE 2-PART CODE. (NOW UNENCIPHERED. HAD BEEN ENCIPHERED FOR A SHORT TIME.)	PC 146	5 BERLIN 19Ø1; 5 VARIA 1-19ØØ	(FRL)	(?-1941-CURRENT)	? SID ? PERS Z S	COMPROMISED 1ØØ% BY SID; CODE 75% RECOVERED BY PERS Z S	T 15Ø9; T 2Ø29 T 3299; T 3253 T 3254; T 36Ø	(87% COMPROMISED NOV. 1942. REMAINDER PROVIDED THROUGH TICOM SOURCES SEPT. 1945.)	--
FRANCE 32	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	19 RN	?	? - ?	? GERMANS	RECOVERED 35%	T 3245	(UNKNOWN)	--
FRANCE 33	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	?	?	?-193Ø-?	? PERS Z S	RECONSTRUCTED	T 2Ø18	(UNKNOWN)	--
FRANCE 34	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	33 BERLIN	?	? - ?	? PERS Z S	RECOVERED 2Ø%	T 2Ø32	(UNKNOWN)	--
FRANCE 35	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	F 4	?	? - ?	? PERS Z S	ABOUT 5% RECOVERED	T 2Ø31	(UNKNOWN)	--
FRANCE 36	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	?	?	?-193Ø-?	? OKW	PARTIALLY RECONSTRUCTED	T 893	(UNKNOWN)	--
FRANCE 37	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	?	?	? - ?	? OKW	RECONSTRUCTED 35%	T 892	(UNKNOWN)	--
FRANCE 38	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	358 BERLIN 1-1195; 358 VARIA 1-; 358 VARIA D-E 1-799	?	? - ?	? PERS Z S	APPROXIMATELY 7Ø% RECOVERED	T 3Ø96; T 3Ø86 T 2Ø21; T 2Ø2Ø T 2Ø22	(UNKNOWN)	--
FRANCE 39	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	?	?	? - ?	? OKW	RECOVERED 4Ø%	T 883	(UNKNOWN)	--
FRANCE 4Ø	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	111 1-482	?	? - ?	? GERMANS	RECONSTRUCTED 3Ø%	T 2485 T 2489	(UNKNOWN)	--
FRANCE 41	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	?	?	? - ?	? PERS Z S	PARTIALLY RECOVERED	T 3Ø99	(UNKNOWN)	--
FRANCE 42	(DIPLOMATIC)	4-FIGURE (2-PART) CODE. UNENCIPHERED. DIGITS IN 5-FIGURE INDICATOR ADD TO 2Ø.	?	F 2Ø	(FRJ)	(1945-CURRENT)	1945 SID	WORKED ON.	T 1521	(IN PROCESS OF RECOVERY. FAIRLY READABLE.)	--
FRANCE 43	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	1 BERLIN 1; 1 VARIA 1-	?	? - ?	? PERS Z S	ABOUT 75% RECOVERED	T 3Ø87 T 315Ø T 2Ø17	(UNKNOWN)	--
FRANCE 44	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	2 BERLIN 1-5ØØ; 2 VARIA 1-	?	? - ?	? GERMANS	RECOVERED 75%	T 2486 T 3154	(UNKNOWN)	--
FRANCE 45	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	3 BERLIN 1-?; 3 VARIA 1	?	? - ?	? PERS Z S	ABOUT 75% RECOVERED	T 3157 T 3153 T 2488	(UNKNOWN)	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS

AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE-- VICHY, FREE FRANCE	46	DIPLOMATIC	4-FIGURE 2-PART CODE. (UNENCIPHERED.)	(PC 149)	FRANCIA F 149; 4 BERLIN 1Ø2	(FRO)	?-1935-(CURRENT)	? ITALIANS 1935 GERMANS	COMPROMISED 1ØØ% BY ITALIANS. 75% RECOVERED BY GERMANS.	T 1584 T 3252 T 3255	(APPROXIMATELY 98% READABLE; 55-6Ø% RECOVERED. TICOM MATERIAL ELIMINATES THE NEED FOR FURTHER BOOKBREAKING.)	--
FRANCE-- VICHY	47	(DIPLOMATIC)	A SET OF EIGHT 4-FIGURE (2-PART) CODES, UNENCIPHERED.	"PC" SERIES	F 4, 5, 7, 1Ø, 14, 15, 16, 17	(PROBABLY FAC THROUGH FAH, FMO, OR FAS)	?-(SOME CURRENT)	PRIOR TO 1941 PERS Z S	READ, SOME COMPROMISED, SOME BROKEN.	T 3239; T 324Ø T 33ØØ; T 3299 T 15Ø4; T 15Ø5 T 2Ø29 D 54 P 12	(MAINLY COMPROMISED; SOME BREAKING DONE ON PORTIONS OF FAG AND OTHERS.)	--
FRANCE-- (VICHY, LATER FREE FRANCE)	48	DIPLOMATIC	4-FIGURE 2-PART CODE. (ENCIPHERED.)	PCN 9	19 AP	(FAT)	1941-(1944)	1941 FA	RECONSTRUCTED 4Ø%	T 1Ø93 T 3244	(COMPROMISED VICHY'S BOOK AND TABLES 1942. COMPROMISED 3Ø OUT OF 124 OF THE FREE FRENCH TABLES. BUILT UP MANY OTHERS READ.)	--
FRANCE-- (FREE FRANCE)	49	(DIPLOMATIC)	CIFHER TABLES--DIGRAPHIC SUBSTITUTION OF NUMBERS FOR LETTERS. (CHANGED CUARTERLY BUT REPEATED FROM YEAR TO YEAR.)	TABLES III AND IV	19 AP	(FAT TABLES)	(194Ø-1943)	? ?	COMPROMISED	T 2452	(COMPROMISED 1942. SEE ITEM 48.)	--
FRANCE-- (VICHY, LATER FREE FRANCE?)	5Ø	(DIFLOMATIC)	4-FIGURE (2-PART) CODE WITH LETTER DIGRAPHIC SUBSTITUTION WITH LIMITATIONS OF 1Ø LETTERS. TABLES OF 1ØØ DIGRAPHS CHANGED QUARTERLY. SAME TABLE USED ON DIFFERENT DATES IN SUCCESSIVE MONTHS OF CUARTER. DIGRAPHS TAKEN CUARTERLY. SEVERAL OF THIS TYPE.	(PCN-9)	?	(FAT?) OR (FAU?)	(FAU: 1941-1944) (FAT: 1943-1945)	? PERS Z S	COMPROMISED SOME MATERIAL. PROBABLY READ AFTER 1941.	I 22 P 19 D 54 P 13 T 3532	(IF FAU, WORK STARTED 1942, THEN COMPROMISED; READ. IF FAT, SEE ITEM 48.)	--
FRANCE-- VICHY, FREE FRANCE	51	DIFLOMATIC	4-FIGURE 2-PART CODE. ENCIFHERED--SOME BY TABLES. MANY OF THIS TYPE.	?	?	(FAM, FAN, FAO, FAP, FAL. FMH, OR FAU)	?-194Ø-?	194Ø SIM	HAD COMPROMISED COPY OF ONE CODE AND ONE 1-TIME ENCIPHERING TABLE.	IF 1522 P 2	(COMPROMISED MOST CODES AND TABLES 1942. SOME BREAKING DONE ON FAU AND TABLES OF FMH.)	--
FRANCE	52	DIFLOMATIC	4-FIGURE 2-PART CODE.	PC 28	?	?	?-1925-?	1929 PERS Z S	PARTIALLY RECONSTRUCTED	T 2156	(UNKNOWN)	--
FRANCE	53	DIFLOMATIC	4-FIGURE 2-PART CODE.	(PC 155)	16-1-36ØØ	(FAD)	?-194Ø-(1944)	? GERMANS ? ITALIANS	APPROXIMATELY 75% RECOVERED BY GERMANS AND ITALIANS.	T 3237 T 3238 T 3239 T 324Ø T 15Ø7 T 23Ø6	(ASA HAS COMPROMISED COPY. READ FROM 1942-1944.)	--
FRANCE	54	DIFLOMATIC?	4-FIGURE 2-PART CODE.	?	F 36	?	193Ø - ?	? OKW	RECONSTRUCTED 45%	T 879	(UNKNOWN)	--
FRANCE	55	DIFLOMATIC?	4-FIGURE 2-PART CODE.	?	F 49	?	?-1931-?	? OKW	RECONSTRUCTED 3Ø%	T 881	(UNKNOWN)	--
FRANCE	56	DIPLOMATIC?	4-FIGURE 2-PART CODE.	?	F 5Ø	?	?-1931-?	? OKW	RECONSTRUCTED 33%	T 88Ø	(UNKNOWN)	--
FRANCE	57	DIFLOMATIC?	4-FIGURE 2-PART CODE. USED BETWEEN PARIS AND BEIRUT AND ADDIS-ABBABA.	?	?	?	?-193Ø-1937-?	? PERS Z S	PARTIALLY READ	T 2Ø36	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A						
FRANCE-- VICHY, FREE FRANCE 58	DIPLOMATIC	4-FIGURE 2-PART CODE. SOMETIMES ENCIPHERED WITH DAILY CHANGING REPEATING 5-DIGIT ADDITIVE. (UNENCIPHERED UNTIL JUNE 1944.)	PC 15Ø	F I	(FRA: FRA-3)	?-(1943-CURRENT)	1944 SID PRIOR TO 1945 PERS Z S	READ BY PERS Z S. SID READ FREE FRENCH TRAFFIC 1944-1945. COMPROMISED DEC. 1944.	IF 1526 P 4 I 22 P 19 T 732; T 734 T 1506; T 1503 T 1521; T 792 T 1523; T 1525 T 1529	(TRAFFIC READABLE FROM 1942. BOOKBREAKING CONTINUED UNTIL SEPT. 1945 WHEN ITALIAN COMPROMISED CODE WAS RECEIVED. CURRENT FORMS BEING READ.)	--
FRANCE 59	DIPLOMATIC	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	?	BE (ZAHLEN CODE)	?	? - ?	? GERMANS	RECOVERED 9Ø%	T 359	(UNKNOWN)	--
FRANCE-- FREE FRANCE 6Ø	DIPLOMATIC	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	PR 19	?	?	?-1927-?	? OKW	COMPROMISED	T 1723	(UNKNOWN)	--
FRANCE 61	DIPLOMATIC	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	?	?	?	?-1937?-?	? OKW	RECOVERED 5Ø%	T 1826	(UNKNOWN)	--
FRANCE 62	DIPLOMATIC	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC. LESS THAN 1,3ØØ GROUPS.	?	"CODE LEKE"	?	?-1937?-?	? OKW	RECOVERED 75%	T 1827 T 1828	(UNKNOWN)	--
FRANCE 62	DIPLOMATIC	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC. "SMALL CODE."	?	?	?	?-1937-?	? OKW	RECOVERED 5Ø%	T 183Ø	(UNKNOWN)	--
FRANCE 64	DIPLOMATIC	4-FIGURE 1-PART CODE, REPAGINATED. LESS THAN 2,ØØØ GROUPS.	?	?	?	?-1937?-?	? OKW	RECONSTRUCTED 5Ø%	T 1829	(UNKNOWN)	--
FRANCE 65	DIPLOMATIC?	4-FIGURE 1-PART CODE, REPAGINATED. "SUBSTITUTION ENCIPHERMENT BY TABLE #3."	?	?	?	?-1939-?	? PERS Z S	?	D 54 P 7	(UNKNOWN)	--
FRANCE-- (FREE FRANCE) 66	DIPLOMATIC	4-FIGURE 1-PART CODE.	?	?	?	?-1927-?	? OKW	COMPROMISED	T 1721	(UNIDENTIFIED)	--
FRANCE-- (FREE FRANCE) 67	DIPLOMATIC	4-FIGURE 1-PART CODE.	?	?	?	?-1940-?	? OKW	COMPROMISED	T 1719	(UNKNOWN)	--
FRANCE 68	DIPLOMATIC?	4-FIGURE 1-PART CODE.	H. D. 2	?	?	? - ?	? OKW	PARTIALLY RECONSTRUCTED	T 2496	(UNIDENTIFIED)	--
FRANCE-- VICHY 69	DIPLOMATIC	4-FIGURE ?-PART CODE.	?	?	?	?-1939-?	? GERMANS	READ	T 2494	(UNKNOWN)	--
FRANCE 7Ø	DIPLOMATIC?	4-FIGURE ?-PART CODE. USED TO TRANSMIT ENGLISH TEXT.	?	8	?	? - 1941	? PERS Z S	?	D 54 P 2	(UNKNOWN)	--
FRANCE 71	DIPLOMATIC?	4-FIGURE ?-PART CODE. "SUSPECTED THAT IT COMBINES AN ADDITIVE AND A SUBSTITUTION PROCESS."	?	?	?	?-1940-?	1940 PERS Z S	NOT READ BY PERS Z S PRIOR TO 1941	D 54 P 13	(UNIDENTIFIED)	--
FRANCE 72	DIPLOMATIC?	4-FIGURE ?-PART CODE. ENCIPHERED BY A 1ØØ-PLACE LETTER SUBSTITUTION TABLES.	?	19	?	?-1941-?-	PRIOR TO 1942 FA, PERS Z S	FIRST SOLUTION BY FA USING CAPTURED TABLES.	D 54 P 19	(UNIDENTIFIED)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 73	DIPLOMATIC?	4-FIGURE ?-PART CODE.	?	FU 5, FU 4, FU 3, FU 2, FU 1	?	? - ?	? PERS Z S?	NO BOOKBREAKING DONE.	T 3146; T 3145 T 3144; T 3143 T 3142	(UNIDENTIFIED)	--
FRANCE 74	DIPLOMATIC	"CODE FOREIGN OFFICE OR HANOI MESSAGES."	?	?	?	?-194Ø-?	194Ø SIM	READ	IF 1524	(UNIDENTIFIED)	--
FRANCE 76	DIPLOMATIC?	ADDITIVE ENCIPHERMENT SYSTEM.	CODE 1919 TYPE 2	?	?	?-1939-?	? OKW	COMPROMISED 1ØØ%	T 1624	(UNIDENTIFIED)	--
FRANCE 76	DIPLOMATIC?	"CIPHER TABLES #14." TRIGRAPHIC SUBSTITUTION.	DS-B 614	?	?	?-194Ø-?	? OKW	COMPROMISED	T 918	(UNKNOWN)	--
FRANCE 77	DIPLOMATIC, CONSULAR	4-FIGURE ?-PART CODE. INDICATOR 66666. USED BETWEEN PARIS AND DUBLIN.	?	F CONS DUBLWE	?	? - ?	? ITALIANS	?	T 1521	(UNKNOWN)	--
FRANCE 78	DIPLOMATIC, CONSULAR, COLONIAL	4-FIGURE 2-PART CODE. ALWAYS ENCIPHERED BY SIMPLE DIGIT FOR DIGIT SUBSTITUTION.	RO 12	?	?	1918 - ?	? ?	COMPROMISED 1ØØ%	T 3537	(UNKNOWN)	--
FRANCE 79	CONSULAR	4-FIGURE ?-PART CODE.	?	?	?	?-194Ø-?	? OKW	PROBABLY NOT READ	T 17Ø4	(UNKNOWN)	--
FRANCE 8Ø	COMMERCIAL	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	DICTIONAIRE CHIFFRE HAVAS	?	?	?-1932-?	? OKW	COMPROMISED 1ØØ%	T 1681	(UNKNOWN)	--
FRANCE 81	MILITARY ATTACHE	5-LETTER 5-FIGURE ?-PART CODE. PERHAPS ENCIPHERED BY TRANSPOSITION.	?	F 152	?	1939 - ?	1941 GERMANS	?	T 3549	(UNKNOWN)	--
FRANCE 82	(MILITARY ATTACHE)	5-FIGURE (2-PART) CODE. HAD (1Ø) ENCIPHERMENTS. (FVB-5 USES COLUMNAR TRANSPOSITION WITH NULL PATTERNS ON A KEY TAKEN FROM THE ENCODE.)	(CODE EMPIRE 1943)	?	(FVB; FVB-5; AND POSSIBLY FVB-2 OR FVB-3)	1943-1945	? OKH	PROBABLY NOT BROKEN	I 16Ø PP 7, 19-21 POSSIBLY I 58 P 2	(FVB-2, FVB-3, FVB-5 BROKEN BY ASA IN 1943-1944. FOUR OTHER ENCIPHERMENTS SOLVED. THREE OTHERS IN PROCESS OF SOLUTION. ONLY ONE IS CURRENT.)	--
FRANCE 83	(MILITARY ATTACHE)	5-FIGURE 2-PART CODE.	(JOCAM) OR (CODE EMPIRE)	?	(FNF?) OR (FVB?)	1941 - ?	? OKW	?	I 58 P 2	(IF FNF, BROKEN AND READ. IF FVB, SEE ITEM 82.)	--
FRANCE 84	MILITARY ATTACHE	4-FIGURE 2-PART CODE ENCIPHERED BY ONE-TIME TRANSPOSITION KEYS, 13-27 LETTERS IN LENGTH, TAKEN FROM THE ENCODE. KEYS ARE REVERSED BEFORE USED. FOR USE BY FRANCO POLISH MILITAPY MISSION.	?	?	?	194Ø - ?	? ?	COMPROMISED 1ØØ%	T 3553	(UNKNOWN)	--
FRANCE-- 85 (FREE FRANCE)	(MILITARY ATTACHE)	4-FIGURE 1-PART CODE USING TRANSPOSITION ENCIPHERMENT. (SPECIAL PAGINATIONS ASSIGNED TO EACH STATION. ONE GENERAL PAGINATION.)	?	?	(FVD)	194Ø-(CURRENT)	? OKW	BROKEN AND READ	I 31 P 5	(BROKE 3 ENCIPHERMENTS. FVD-4 IN SOLUBLE STATE. FVD-5 BEING WORKED ON.)	--
FRANCE 86	MILITARY ATTACHE	ONE-TIME TRANSPOSITION KEYS OF VARYING LENGTHS. USED BETWEEN FRANCE AND ROME.	?	?	?	194Ø - ?	? OKW	COMPROMISED 1ØØ%	T 1753	(UNKNOWN)	--
FRANCE 88	MILITARY ATTACHE	2-LETTER ENCIPHERING TABLES REPLACING THE SUDAMERI SYSTEM.	?	?	?	1925 - ?	? OKW	COMPROMISED	T 1819	(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 89	COLONIAL	1-PART CODE, 5 OR MORE LETTERS PER GROUP.	?	?	?	?-1923-?	? ?	COMPROMISED	T 2453	(UNKNOWN)	--
FRANCE--VICHY AND FREE FRANCE 9Ø	COLONIAL	5-LETTER 1-PART CODE.	(1926 B)	?	(FBT)	1926-(1944)	? GERMANS	PARTIALLY RE-CONSTRUCTED AND 1ØØ% COMPROMISED	T 3137 T 3158	(COMPROMISED 1942 AFTER SOME WORK WAS DONE.)	(FBU BASIC BOOK; FBT REPAGINATION)
FRANCE 91	COLONIAL	ENCIPHERMENT TABLE FOR 1926 B.	MX	?	?	? - ?	? ?	WORKED ON	T 2457	(UNKNOWN)	(ASA KNOWS OF NO ENCIPHERMENT ON FBT)
FRANCE 92	COLONIAL?	5-LETTER 1-PART CODE.	?	9 MARNE	?	? - ?	? GERMANS	RECOVERED 2Ø%	T 3248	(UNKNOWN)	--
FRANCE 93	COLONIAL	?-LETTER ?-PART CODE, SOMETIMES ENCIPHERED.	?	?	?	? - 1941	194Ø PERS Z S	NOT READ PRIOR TO 1941 FOR LACK OF HELP	D 54 P 13	(UNIDENTIFIED)	--
FRANCE 94	COLONIAL?	5-FIGURE 2-PART CODE	?	F 13	?	? - ?	? OKW	COMPROMISED 1ØØ%	T 1672	(UNKNOWN)	--
FRANCE 95	COLONIAL	5-FIGURE (1-PART) CODE. (APPROXIMATELY 8,ØØØ GROUPS. SIMITATION ON FIRST DIGITS TO Ø, 1, OR 2. FIRST UNENCIPHERED; LATER SOMETIMES ENCIPHERED BY ADDITIVE ON 1Ø X 1Ø DAILY SQUARE WITH RANDOM COORDINATES.)	(1943)	F COL 29	(FNC)	?-1944-1945	? SID	KNEW INDICATORS	T 1521	(CODE BOOK COMPROMISED 1945 AFTER SOME BOOK BREAKING HAS DONE. ASA SOLVED ENCIPHERMENT.)	--
FRANCE 96	COLONIAL?	5-FIGURE 1-PART CODE. BOOK HAS 3 SETS OF TRIGRAPHIC PAGE DESIGNATIONS FOR EACH PAGE, ALL AT THE SAME INTERVAL AND PROGRESSING BY ONES.	?	?	?	?-1918?-?	? OKW	COMPROMISED 1ØØ%	T 18Ø2	(UNKNOWN)	--
FRANCE 97	COLONIAL (NAVAL, MILITARY, DIPLOMATIC ATTACHE)	4-FIGURE 2-PART CODE. (NOW UNENCIPHERED. HAS HAD 2 MAJOR ENCIPHERMENTS.)	(CODE V)	F COL ØØØ	(FNB)	?-1943-(CURRENT)	? ITALIANS	?	T 1521	(COMPROMISED CODE BOOK. BROKE BOTH ENCIPHERMENTS. READ 1ØØ%.)	--
FRANCE 98	COLONIAL	4-FIGURE 1-PART CODE. SOME GROUPS SENT IN CLEAR. FOR USE IN ALGERIA. SPELL GROUPS BEGIN WITH 51 OR 53 AND END WITH 52 OR 54.	CHIFFRE 6Ø	?	?	? - ?	? ?	COMPROMISED 1Ø2%	T 1621	(UNKNOWN)	--
FRANCE 99	COLONIAL	RUNNING ADDITIVE ENCIPHERING SYSTEM FOR COLONIAL 1923 CODE.	C.M.A.N.	?	?	?-1941-?	? ?	TABLES 1ØØ% COMPROMISED	T 2456	(UNKNOWN)	--
FRANCE 1ØØ	ARMY	HAGELIN CIPHER MACHINE. (6 WHEELS, VARIABLE PINS, VARIABLE LUGS, SLIDE, MAXIMUM KICK OF 27.)	BC 38	BC 38	(BC 38)	(1944-CURRENT)					
FRANCE--FREE FRANCE 1Ø1	(ARMY)	CIPHER MACHINE EMPLOYING FRACTIONATION, SUBSTITUTION, AND RECOMBINATION. (USED 5 X 5 SQUARE. HAD 6 WHEELS AND 2 SETS OF PLUGS. "MODIFIED" VERSION HAD 1Ø WHEELS AND 4 SETS OF PLUGS.)	B-211	B-211 AND V-211 WITH SURCHIFFREUR	(B-211 AND MODIFIED B-211)	(ABOUT 1938-CURRENT)	APPROXIMATELY 1941 OKH, OKW	ORIGINAL VERSION READ. MODIFIED VERSION NOT READ.	I 16Ø P 6 I 111 P 5 I 31 PP 1, 7 D 6Ø P 7	(NOT READ)	--

~~TOP SECRET~~

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE-- FREE FRANCE	1Ø2	(ARMY)	CIPHER MACHINE, HAGELIN TYPE. 5 WHEELS (FIXED LUGS, VARIABLE PINS.)	C-36	C-36	(C-36)	(APPROXIMATELY 1936-CURRENT)	194Ø OKH 194Ø OKW 1939 SIM	SOLVED AND FREQUENTLY READ BY OKH AND OKW. MAY HAVE BEEN READ BY SIM.	I 92 P 3 I 16Ø P 6 I 42 P 4 I 58 P 5 I 48 P 2 I 45 PP 6-7 I 79 PP 2-3 I 78 PP 4, 9 I 31 P 7 IF 1Ø7 P 5 IF 1518 IF 1524 T 1658 T 1673	(READ. CAN BE BROKEN BY STATISTICAL METHODS.)	--
FRANCE	1Ø3	MILITARY	MACHINE CIPHERS.	?	?	?	1939-194Ø	? SIM	NOT READ	IF 1522	(UNIDENTIFIED)	--
FRANCE	1Ø4	ARMY	5-LETTER ?-PART CODE ENCIPHERED BY DIAGONAL TRANSPOSITION BY MEANS OF A NUMERICAL KEY DERIVED FROM A KEY WORD. KEY WORD CHANGED MONTHLY, LATER EVERY TWO WEEKS. IN WEST AFRICA LETTER SUBSTITUTION TABLES WERE INTRODUCED WITH A MONTHLY CHANGE FOR THE INDICATOR GROUPS.	?	?	?	1943-1945	? OKH	READ	I 16Ø P 7	(UNIDENTIFIED)	--
FRANCE	1Ø5	ARMY	5-LETTER ?-PART CODE. FIRST 2 AND LAST GROUPS ARE 5-FIGURE. ENCIPHERED BY DIAGONAL TRANSPOSITION. USED IN EQUATORIAL AFRICA.	?	?	?	1943-APPROXIMATELY 1945	? OKH	READ	I 16Ø P 7, PP 12-14	(UNKNOWN)	--
FRANCE	1Ø6	ARMY	5-LETTER ?-PART CODE. ENCIPHERED BY SIMPLE TRANSPOSITION. "1Ø DAILY KEY CHANGE."	?	?	?	1943 - ?	? OKH	READ	I 16Ø P 6	(UNKNOWN)	--
FRANCE	1Ø7	ARMY	4-LETTER 2-PART CODE, UNENCIPHERED. COULD BE USED AS A 4-FIGURE 1-PART CODE ENCIPHERED BY "TABLES 3, 1Ø2, AND 1Ø3."	M.C.	?	?	1935-194Ø-?	? OKW	COMPROMISED 1ØØ%	T 1646	(UNKNOWN)	--
FRANCE	1Ø8	ARMY?	4-LETTER ?-PART CODE.	?	F 51	?	? - ?	? GERMANS	?	T 3615	(UNIDENTIFIED)	--
FRANCE-- FREE FRANCE	1Ø9	ARMY	3-LETTER 1-PART CODE. FIELD TYPE.	?	?	?	1942-1943	? GERMANS ? SIM	READ BY GERMANS AND SIM. PROBABLY FIRST BROKEN BY GERMANS.	IF 1517 P 5 IF 1523 P 7	(UNKNOWN)	--
FRANCE	11Ø	(ARMY)	3-LETTER 1-PART CODE, THE MIDDLE LETTER BEING ONE OF THE 5 VOWELS. SEVERAL ENCIPHERMENTS WERE USED. LATER THE ENCIPHER KEY CHANGED MORE FREQUENTLY.	?	?	?	1941 - ?	? OKH	READ.	I 17Ø PP 2-3	(UNKNOWN)	--
FRANCE	111	ARMY	3-LETTER 1-PART SMALL CODE. KEY CHANGED EVERY 2 WEEKS.	?	?	?	1942-1944	? OKH	READ	I 16Ø PP 6, 8	(UNKNOWN)	--
FRANCE	112	ARMY	3-LETTER 1-PART SMALL CODE. IDENTICAL IN CONSTRUCTION TO ITEM 111, BUT VOCABULARY MORE ADAPTABLE TO WIRELESS TRAFFIC. KEY CHANGED EVERY 2 WEEKS.	?	?	?	APPROXIMATELY 1943-1944	? OKH	READ	I 16Ø PP 6, 8	(UNKNOWN)	--
FRANCE	113	ARMY, AIR, NAVY	MIXED 3-LETTER, 4-FIGURE, AND 3-FIGURE 2-PART CODE. EMERGENCY CODEBOOK FOR USE IN NORTH AFRICA. BOOK DIVIDED INTO SECTIONS FOR THE USE OF THE THREE SERVICES.	G.M.A.	?	?	1942 - ?	? ?	COMPROMISED 1ØØ%	T 179Ø	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE-- VICHY 114	ARMY	TWO 5-FIGURE 2-PART CODES WITH ABOUT 5Ø,ØØØ GROUPS. VARIOUS SYSTEMS OF ENCIPHERMENTS USED. USED BETWEEN FRANCE AND COLONIAL ARMIES.	?	?	?	? - ?	? SIM	READ AFTER BEING DEPOSITED WITH ARMISTICE COMMISSION	IF 1522 P 1, APPENDIX A	(UNIDENTIFIED)	--
FRANCE 115	(ARMY)	5-FIGURE 2-PART CODE.	?	?	?	1943 - ?	? OKH	BROKEN AND READ	I 17Ø P 4	(UNIDENTIFIED)	--
FRANCE 116	(ARMY)	(5-FIGURE 1-PART CODE. LATER REPAGINATED. 3 ENCIPHERMENTS IN USE SIMULTANEOUSLY.)	SYSTEME CRYPTOGRAPHICUE MODELE 1923	?	--	1923 - ?	? OKW	COMPROMISED 1ØØ%	T 16Ø5 T 1735 T 1814 T 1627	(COMPROMISED BOOK 1927 OR 1928. NO TRAFFIC. NO WORK DONE.)	--
FRANCE 117	MILITARY	TRANSPOSITION KEYS FOR SYSTEM 1923.	1933 D	F 145?; F 137?	--	194Ø - ?	194Ø GERMANS	COMPROMISED 1ØØ%	T 3613	(CODE BOOK COMPROMISED. SEE ITEM 116.)	--
FRANCE 118	ARMY	5-FIGURE ?-PART CODES. USED IN FRANCE, NORTH AFRICA, WEST AFRICA, AND ECUATORIAL AFRICA.	?	?	?	?-1943-1944?	? OKH	NOT READ BY FEBRUARY 1945	I 16Ø P 7	(UNIDENTIFIED)	--
FRANCE-- FREE FRANCE 119	ARMY	4-FIGURE 5-FIGURE CODE SENT IN 5-FIGURE GROUPS. ENCIPHERED BY ADDITIVE SYSTEM.	?	?	?	? - ?	? SIM	NOT READ	IF 1522 P 2	(UNIDENTIFIED)	--
FRANCE 120	ARMY?	4-FIGURE 2-PART CODE. SHORT CODE. SOMETIMES ENCIPHERED BY DIGRAPHIC LETTER SUBSTITUTION.	CODE CHIFFRE NO. 3	?	?	? - ?	? OKW	COMPROMISED 1ØØ%	T 164Ø	(UNKNOWN)	--
FRANCE 121	ARMY	4-FIGURE 2-PART FIELD CODE. ENCIPHERED BY A 11 DIGIT REPEATING ADDITIVE. INDICATOR WAS 55555.	?	F 112 OR RA	?	1937-1939	1937 OKW	SOLVED AND READ. ENCIPHERING TABLES COMPROMISED 1ØØ%.	I 58 P 6 I 176 P 2 T 3684	(UNKNOWN)	--
FRANCE 122	ARMY	4-FIGURE 2-PART CODE. APPROXIMATELY 6,ØØØ GROUPS. ENCIPHERED BY DIGRAPHIC LETTER SUBSTITUTION.	SERIE 67	?	?	?-192Ø-?	? OKW	COMPROMISED 1ØØ%	T 1793 T 1644	(UNKNOWN)	--
FRANCE 123	ARMY	4-FIGURE 2-PART CODE. APPROXIMATELY 55,ØØØ GROUPS. DIGRAPHIC LETTER SUBSTITUTION. SIMILAR TO ITEM 122.	CONCOR DANCE NO. 3	?	?	? - ?	? OKW	COMPROMISED 1ØØ%	T 1794	(UNKNOWN)	--
FRANCE 124	ARMY	4-FIGURE 2-PART CODE.	CODE CHIFFRE SERIE 68	?	?	? - ?	? OKW	COMPROMISED 1ØØ%	T 1666	(UNKNOWN)	--
FRANCE 125	ARMY	4-FIGURE 2-PART CODE. ENCIPHERED BY LETTER SUBSTITUTION WITH VARIANTS. NO GROUP BEGINS WITH Ø.	SERIE 69	?	?	? - ?	? OKW	COMPROMISED 1ØØ%	T 1636	(UNKNOWN)	--
FRANCE 126	ARMY?	4-FIGURE 2-PART CODE.	SERIE 71	?	?	?-194Ø-?	? OKW	ALMOST COMPLETELY RECOVERED	T 877	(UNKNOWN)	--
FRANCE 127	ARMY	4-FIGURE 2-PART CODE. USED BETWEEN NORTH AFRICA AND CORSICA. REVERSED 4TH GROUP SUBTRACTED FROM THE 3RD GROUP ALWAYS GAVE SAME DIFFERENCE FOR ALL MESSAGES.	ATM43	?	?	1943-1945	1944 OKH	RECOVERED AND READ	I 16Ø PP 7, 14-19	(UNKNOWN)	--

TOP SECRET

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	*SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 128	ARMY	4-FIGURE 2-PART CODE, ALWAYS ENCIPHERED.	AFR	?	?	?-1942-?	? GERMANS	COMPROMISED 1ØØ%	T 3683	(UNKNOWN)	--
FRANCE 129	ARMY	4-FIGURE ?-PART CODE WITH SHORT REPEATING ADDITIVE, WHICH MAY HAVE CHANGED WEEKLY. GROUP 1 WAS MESSAGE NUMBER; GROUP 2 GAVE NUMBER OF GROUPS; AND THE LAST GROUP WAS THE INDICATOR GROUP.	?	?	?	1944-1945	? OKH	CAPTURED AND READ	I 16Ø PP 7, 19	(UNKNOWN)	--
FRANCE 13Ø	ARMY	4-FIGURE ?-PART CODE WITH SHORT REPEATING ADDITIVE. USED IN TRANSPORT NETWORKS IN NORTH AFRICA. EXTERNAL CHARACTERISTICS SAME AS THOSE OF ITEM 129. TRANSMITTED IN 3-FIGURE GROUPS.	?	?	?	1944-1945	? OKH	READ	I 16Ø PP 7, 19	(UNKNOWN)	--
FRANCE 131	ARMY	4-FIGURE ?-PART CODE CONSTRUCTED BY A CODE "TABLE" IN WHICH RANDOM 2-DIGIT COORDINATES FORMED THE 4-FIGURE GROUPS. ENCIPHERED BY DAILY CHANGING FIGURE SUBSTITUTION TABLES IN MONTHLY CYCLES.	?	?	?	1944-1945	? OKH	READ	I 16Ø PP 6, 8	(UNKNOWN)	--
FRANCE 132	ARMY	4-FIGURE ?-PART CODE ENCIPHERED BY "ORDINARY" TRANSPOSITION.	?	F 9Ø	?	? - 194Ø	1937 OKW	SOLVED AND READ	T 3611 I 58 P 6 I 176 P 2	(UNKNOWN)	--
FRANCE-- FREE FRANCE 133	ARMY	(4-FIGURE 1-PART CODE NOT STRICTLY ALPHABETIC, ENCIPHERED BY SUBSTITUTION OF A TRIGRAPH FOR THE INITIAL DIGRAPH. SUPERENCIPHERED BY TRANSPOSITION KEY TAKEN FROM THE MAGAZINE "FRANCE LIBRE", VOL. IV, #23.) 5-FIGURE INDICATOR REPEATED AT THE BEGINNING IN REVERSED ORDER.	(GAMMA?)	?	(FRE 4)	(?-1942-CURRENT)	? GERMANS	NOT READ	T 312	(CODE BOOK ABOUT 8Ø% RECOVERED BY GCCS AIDED BY ASA. ENCIPHERMENT SYSTEM ALMOST COMPLETELY COMPROMISED BY GCCS. READ AT ASA SINCE 1944.)	--
FRANCE 134	ARMY	4-FIGURE 1-PART CODE TRANSMITTED IN 5-FIGURE GROUPS. WAS ORIGINALLY A 3-LETTER 2-PART CODE. ENCIPHERMENT BY 1Ø-DIGIT REPEATING ADDITIVE CONSTRUCTED FROM THE DATE.	ATM	?	?	BEFORE 1939-?	? GERMANS	COMPROMISED 1ØØ%	T 3551 T 3528 I 16Ø P 18	(UNKNOWN)	--

FRANCE 135	ARMY	4-FIGURE 1-PART CODE, REPAGINATED. VARIOUS ENCIPHERMENTS USED, SOMETIMES ONE-TIME TRANSPOSITION KEYS, SOMETIMES A REPEATING ADDITIVE.	G.N.1;
			G.C.1;
			G.F.1;
			G.R.1;
			CODE B.L.C
			CODE B.J;
			G.L.1;
			REPERTOIRE 1927
				?	?	1927-194Ø-?	? OKW	COMPROMISED 1ØØ%	T 3541
									T 1653
									T 1652
									T 3542
									T 3545
									T 3546
									T 3552
									T 3554
									T 1751
									T 1755
										(UNKNOWN)	--

FRANCE-- VICHY 136	ARMY?	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC. ENCIPHERED BY ADDITIVE TAKEN FROM A TABLE.	CARNET DE CHIFFREMENT "P.L."	?	?	1941 - ?	? OKW	COMPROMISED 1ØØ%	T 1647	(UNKNOWN)	NOT GIVEN TO ARMISTICE COMMISSION.
FRANCE 137	ARMY	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC. VARIANTS USED ON MOST FREQUENT GROUPS. 2-DIGIT DIFFERENTIAL FOR GROUPS REPRESENTING PLAIN TEXT DIGITS. CODE TO BE USED ONLY WITH ENCIPHERMENT--LETTER OR FIGURE. TRANSPOSITION ONE-TIME KEY USED.	SERIE M	?	?	?-194Ø-?	? OKW	COMPROMISED 1ØØ%	T 1831 T 1725 T 1626 T 1633 T 1665	(UNKNOWN)	NOT TURNED OVER TO GERMANS OR ITALIANS AT ARMISTICE.
FRANCE 138	ARMY-COLONIAL	4-FIGURE 1-PART CODE WITH LETTER ENCIPHERMENT--2 OR 3 ALTERNATIVE LETTERS FOR EACH FIGURE.	?	?	?	? - 1939	? SIM	READ	IF 1519 P 2	(UNIDENTIFIED)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE	139	ARMY	4-FIGURE 1-PART CODE. USED FOR SMALL UNITS. USED UNENCIPHERED IF NO SECURITY REQUIRED. SOMETIMES ENCIPHERED BY 5-DIGIT REPEATING ADDITIVE WHICH FREQUENTLY CHANGED.	SERIE FC; CARNET DE CHIFFREMENT	?	?	?-1938-1939-?	? OKW	COMPROMISED 100%	T 1938 T 1629 T 1630	(UNKNOWN)	--
FRANCE--(FREE FRANCE)	140	ARMY	4-FIGURE 1-PART CODE.	?	?	?	?-1938-?	? OKW	COMPROMISED	T 1629 T 1630	(UNKNOWN)	--
FRANCE	141	ARMY	4-FIGURE 1-PART CODE, TRANSPOSED.	?	?	?	PRIOR TO 1939	PRIOR TO 1939 SIM	READ	IF 1519 P 1	(UNIDENTIFIED)	--
FRANCE--(FREE FRANCE)	142	ARMY	4-FIGURE 1-PART CODE, ENCIPHERED BY LETTER SUBSTITUTION TABLE. FIRST GROUP ALWAYS TTSF.	?	?	(FXB)	1944-(CURRENT)	? OKH	READ	I 160 PP 7, 11	(BROKEN AND BEING READ 100%)	--
FRANCE	143	ARMY, AIR	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	J 2 CODE	?	?	?-1942-?	? OKW	COMPROMISED	T 904	(UNKNOWN)	--
FRANCE	144	ARMY	3-FIGURE 2-PART CODE. PROBABLY A FIELD CODE.	CARNET REDUIT: 222	?	?	1939?-1942-?	? OKW	COMPROMISED 100%	T 1736	(UNKNOWN]	--
FRANCE	145	ARMY?	3-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	CODE DE SERVICE 1926	F 23	?	?-1926-?	? GERMANS	RECONSTRUCTED 60%; PERHAPS PARTIALLY COMPROMISED.	T 3559 T 3651?	(UNKNOWN)	--
FRANCE	146	ARMY	?-FIGURE ?-PART CODE. USED TRANSPOSITION ENCIPHERMENT.	?	F MIL	(FMG 112)	1945 ONLY	? SID	WORKED ON. PROBABLY NOT READ.	T 1521	(UNREADABLE. BEING WORKED ON.)	--
FRANCE	147	ARMY	2-FIGURE SUBSTITUTION TABLE WITH ALTERNATIVE EQUIVALENTS. USED IN SYRIA.	?	?	?	? - ?	? OKH	READ.	I 160 P 6	(UNKNOWN)	--
FRANCE--FREE FRANCE	148	ARMY	CODE VALUES IN BLOCKS DESIGNATED BY FIGURE FOR BLOCK, LETTER FOR LINE. FIGURE COULD BE SUBSTITUTED BY DIGRAPH. USED IN SYRIA.	?	?	?	? - ?	? GERMANS ? SIM	READ PARTIALLY	IF 1523	(UNIDENTIFIED)	--
FRANCE	149	ARMY	SUBSTITUTION TABLES, 2 LETTERS PER NUMBER.	?	?	?	1940 - ?	? OKW	COMPROMISED	T 1749	(UNIDENTIFIED)	--
FRANCE	150	(ARMY)	CIPHER SYSTEM. SIMPLE LETTER SUBSTITUTION. SUBSTITUTION KEYS AND BOXES CHANGED EVERY 14 DAYS	?	?	?	?-1943-?	? OKH	READ	I 170 P 4	(UNIDENTIFIED)	--
FRANCE--FREE FRANCE	151	ARMY	CIPHER?	"CONTROL BEDOUIN"	?	?	? - ?	? OKH	READ	I 74 P 2	(UNKNOWN)	--
FRANCE--FREE FRANCE	152	ARMY	CIPHER?	"SERVICE POLITIQUE"	?	?	? - ?	? OKH	READ	I 74 P 3	(UNKNOWN)	--
FRANCE	153	ARMY	3 SETS OF ENCIPHERING KEYS--LETTER DIGRAPHS.	V.F.	?	?	APRIL 1940	? ?	COMPROMISED 100%	T 3557	(UNKNOWN)	--
FRANCE	154	ARMY?	TRANSPOSITION ENCIPHERMENT BASED ON A KEYWORD TAKEN FROM THE ENCODE.	MA	?	?	? - ?	? ?	ENCIPHERING DIRECTIONS COMPROMISED 100%	T 3543	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 155	(ARMY)	CIPHER SYSTEM USING SIMPLE LETTER TRANSPOSITION.	?	?	?	?-1943-?	? OKH	READ	I 170 P 4	(UNIDENTIFIED)	--
FRANCE 156	ARMY	SIMPLE TRANSPOSTION. USED IN SYRIA.	?	?	?	? - ?	? OKH	READ	I 160 P 6	(UNIDENTIFIED)	--
FRANCE 157	ARMY	21-LETTER REPEATING TRANSPOSITION KEY USED ON CODE RA. USED DURING MONTH OF SEPTEMBER, 1939. REPLACED BY CLEF ZERO B 2.	CLEF ZERO A 2	?	?	1939 ONLY	? OKW	COMPROMISED 100%	T 1736	(UNKNOWN)	--
FRANCE 158	ARMY	TRANSPOSITION ENCIPHERMENT BASED UPON A KEY, 14-25 LETTERS IN LENGTH, TAKEN FROM THE ENCODE FOR USE ON CODE RA. REPLACED BY CLEF ZERO C 2.	CLEF ZERO B 2	?	?	1939 ONLY	? OKW	COMPROMISED 100%	T 1736	(UNKNOWN)	--
FRANCE 159	ARMY	ENCIPHERMENT FOR USE ON CODE RA. REPLACED BY CLEF ZERO D 2.	CLEF ZERO C 2	?	?	1939-1940	? OKW	?	T 1736	(UNKNOWN)	--
FRANCE 160	ARMY	ENCIPHERMENT FOR USE ON CODE RA. REPLACED BY CLEF ZERO E 2.	CLEF ZERO D 2	?	?	1940 ONLY	? OKW	?	T 1736	(UNKNOWN)	--
FRANCE 161	ARMY	13-29 LETTER TRANSPOSITION KEY. LENGTH IS NEVER A MULTIPLE OF 4. FOR USE ON CODE RA.	CLEF ZERO E 2	?	?	1940 ONLY	? OKW	COMPROMISED 100%	T 1736	(UNKNOWN)	--
FRANCE 162	AIR	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC. SOMETIMES ENCIPHERED.	?	?	?	1939-1942-?	? OKW	COMPROMISED 100%	T 1639	(UNKNOWN)	--
FRANCE 163	AIR	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	?	FC 1; 42	?	?-1939-?	1939 GERMANS	PARTIALLY RECONSTRUCTED	T 3544	(UNKNOWN)	--
FRANCE 164	AIR	4-FIGURE 1-PART CODE, ENCIPHERED BY LETTERS.	?	?	?	?-1939-?	1939 OKL	READ	I 112 P 6	(UNKNOWN)	--
FRANCE 165	(AIR)	3-FIGURE 2-PART CODE, CAPTIONATED.	DICTIONNAIRE ET VOCABULAIRE GEOGRAPHIQUE DU CODE AERO; D.S. D 105	?	?	?-1936-?	? OKW	COMPROMISED 100%	T 1643	(UNKNOWN)	--
FRANCE 166	AIR	3-FIGURE 1-PART CODE. ENCIPHERED BY LETTERS WHICH CHANGED 2-5 TIMES A MONTH.	?	?	?	?-1935-?	? OKL	READ	I 112 P 6	(UNKNOWN)	--
FRANCE 167	AIR	WEATHER CODE. SINGLE DIGITS AND LETTERS. ENCIPHERED BY DAILY CHANGING ADDITIVE.	R.A.V.	?	?	? - ?	? OKW	COMPROMISED	T 1804	(UNIDENTIFIED)	--
FRANCE 168	AIR, NAVY	COMBINATION LETTER AND FIGURE CODE. PARTIALLY PLAIN TEXT. USED FOR LIAISON OF ARMY AND NAVY. LESS THAN 100 GROUPS.	LE CODE, AIR-MARINE 1938	?	?	1938 - ?	? OKW	COMPROMISED	T 1733	(UNKNOWN)	--
FRANCE 169	AIR FORCE	CODE ENCIPHERED.	?	D. S. D 107	?	1940-1941	? SIS	READ. CAPTURED CODE INCLUDING KEYS FOR FEB., MAY, AND JUNE 1941	IF 1506	(UNIDENTIFIED)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE 17Ø	NAVY AIR	ADDITIVE ENCIPHERMENT SYSTEM FOR D.S.-D 1Ø7. DAILY CHANGING REPEATING ADDITIVE OF VARYING LENGTHS WHICH CHANGED ACCORDING TO DAY OF MONTH.	D.S.-D 1Ø9	?	?	?-194Ø-1941-?	? OKW ? SIS	COMPROMISED AND READ BY OKW AND SIS	T 18Ø3 IF 15Ø6	(UNKNOWN)	--
FRANCE 171	NAVY AIR	ADDITIVE ENCIPHERMENT (REPLACING?) D.S.-D 1Ø9. SIMILAR TO ITEM 17Ø.	?	?	?	1941-?	? OKW	COMPROMISED	T 18Ø6	(UNKNOWN)	--
FRANCE--VICHY, FREE FRANCE 172	NAVY	4-LETTER 2-PART CODE. 15 VARIANTS FOR EACH VALUE	D.S. 224 OR ISMC4	?	?	194Ø-?	? ?	COMPROMISED 1ØØ%	T 3555	(UNKNOWN)	--
FRANCE 173	NAVY	4-LETTER ?-PART CODE.	ISMC5; D.S.-D 225	?	?	1941-1942	? OKW	COMPROMISED	T 18Ø5	(UNKNOWN)	--
FRANCE 174	NAVY?	4-LETTER CALL SIGN SYSTEM	?	ISMC1 (D.S.D 221) RENO	?	? - ?	? SIS	READ. CAPTURED.	IF 15Ø6	(UNKNOWN)	--
FRANCE 175	NAVY?	3-LETTER CALL SIGNS.	?	N.S.4 (D.S.D244) VATI	?	? - ?	? SIS	READ. CAPTURED.	IF 15Ø6	(UNKNOWN)	--
FRANCE 176	NAVY	COMBINATION LETTER AND FIGURE CODE. SIGNAL CODE.	D.S.-D 1Ø1	?	?	1936 - ?	? OKM	COMPROMISED 1ØØ%	T 573	(UNKNOWN)	--
FRANCE 177	NAVY	COMBINATION LETTER AND FIGURE CODE. SIGNAL CODE.	D.S.-D 1Ø2	?	?	1936 - ?	? OKM	COMPROMISED 1ØØ%	T 483	(UNKNOWN)	--
FRANCE 178	NAVY	5-FIGURE 2-PART CODE, WITH ENCIPHERING TABLES. ENCIPHERMENT SIMILAR TO THOSE MENTIONED IN ITEM 191.	T.B.M. 2	T.B.M. 2	?	1934 ONLY	1934 SIS	READ	IF 15Ø6, 17B, P 3	(UNKNOWN)	--
FRANCE 179	NAVY	5-FIGURE 2-PART CODE WITH ENCIPHERING TABLES. ENCIPHERMENT SIMILAR TO THOSE MENTIONED IN ITEM 87.	T.B.M. 3	T.B.M. 3	?	1934-1935	1934 SIS	READ	IF 15Ø6, 17B, P 5	(UNKNOWN)	--

FRANCE 18Ø	NAVY	5-FIGURE 2-PART CODE.	T.B.M. 54;
			V.N. 2;
			D.S.B. 2Ø5
			D.S.B. 3Ø1
				F.Z. 21	?	1936-1939	1936 OKM	COMPROMISED 1ØØ%	T 589	(ASA HAS COMPROMISED COPY. NO TRAFFIC RECEIVED.)	--

FRANCE--FREE FRANCE, VICHY 181	NAVY	5-FIGURE 2-PART CODE. (USUALLY ENCIPHERED BY RUNNING ADDITIVE TAKEN FROM A CHART.)	T.B.M. 56;
			V.N. 3;
			A.R. 3;
			D.S.B. 3Ø2
				F.Z.26;
				D.S.B.354
				D.S.B.359
				D.S.B.361
					(FBX)	1939-(1943-?)	1939 SIS
							1942 OKM
								COMPROMISED AND READ BY OKM AND SIS.	T 586
									IF 15Ø4 PP 1, 2Ø
									IF 15Ø6
										(HAVE COMPROMISED COPY OF CODE AND ENCIPHERMENT. RECEIVED SOME TRAFFIC IN 1943. READ.)	--

FRANCE--(VICHY, FREE FRANCE) 182	NAVY	5-FIGURE 2-PART CODE.	C.A. 31;
			BDG 31;
			D.S.B 1Ø8
				?	?	?-1939-?	1942 OKM	COMPROMISED	T 588	(UNKNOWN)	--

FRANCE 183	NAVY	5-FIGURE 2-PART CODE.	G.E. 58; D.S.B 2Ø9	?	?	?-194Ø-?	? OKM	COMPROMISED	T 59Ø	(UNKNOWN)	--
FRANCE 184	NAVY	5-FIGURE 2-PART CODE.	B.D.C. 27; D.S.B 1Ø4	F Z. 22	?	1935-1939	1935 OKM	COMPROMISED 1ØØ%	T 585	(UNKNOWN)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE-- VICHY, FREE FRANCE 185	NAVY	5-FIGURE 2-PART CODE.	B.D.G.3Ø1; C.A. 3Ø; D.S.B.1Ø7	B.D.G. 3Ø CIAK; DAMCUT	?	1939 - ?	? OKM ? SIS	COMPROMISED 1ØØ% BY SIS AND OKM. READ BY SIS.	T 587 IF 15Ø6	(UNKNOWN)	--
FRANCE 186	NAVY	5-FIGURE ?-PART CODE. 4Ø,ØØØ GROUPS, WITH ENCIPHERING TABLE AND 4,ØØØ APPENDIX GROUPS.	TBM 21	TBM 21	?	1938-1939	1938 SIS	SOLVED AND READ.	IF 15Ø6, 15 B, PP 1-25	(UNKNOWN)	--
FRANCE 187	NAVY	5-FIGURE ?-PART CODE WITH ENCIPHERING TABLE. 4Ø,ØØØ GROUPS.	TBM 22; POSSIBLY TBM 55; ENCIPHERMENT "A"	?	?	1939 - ?	? SIS	PERHAPS READ.	IF 15Ø6, 168, PP 1-8	(UNKNOWN)	--
FRANCE 188	NAVAL, DIPLOMATIC, CONSULAR, COLONIAL	4-FIGURE 2-PART CODE. ADDITIVELY ENCIPHERED. ADDITIVES WERE CHOSEN FROM 6 SETS OF 31 ADDITIVE TABLES, EACH TABLE WITH 8ØØ DIGITS.	RD 37	?	(FBM)	194Ø-(1944)	? OKM	COMPROMISED 1ØØ%	T 1789 T 584	(CODE 1ØØ% COMPROMISED; ENCIPHERMENTS BROKEN 1942.)	--
FRANCE 189	NAVY	REVISION OF THE ENCIPHERING KEY #68 OF THE NAVAL ATTACHE IN BERNE. RUNNING ADDITIVE: TO BE USED WITH NAVAL CODE RD.	CLEF SPECIALE (#68 FOR BERNE)	?	?	1943 - ?	1943 PERS Z S	COMPROMISED 1ØØ%	T 245Ø	(UNKNOWN)	--
FRANCE 19Ø	NAVY	4-FIGURE 2-PART CODE. ALWAYS ENCIPHERED BY ADDITIVE TABLE. (USES SAME VOCABULARY AS RD 37)	DICTIONAIRE E.X. 36; FORMERLY RD 36	?	--	?-1939-?	1943 PERS Z S	COMPROMISED	T 2442 T 2443 D 3N-A	(NAVY HAS WORKED ON SYSTEM. ASA HAS NOT.)	--
FRANCE 191	NAVY	4-FIGURE 2-PART CODE. 5 SYSTEMS OF ENCIPHERMENT. USED 1ØØ ENCIPHERING TABLES.	TBM 1	TBM 1	?	1931-1934	1933 SIS	CODE AND ENCIPHERMENTS BROKEN AND READ.	IF 15Ø6	(UNKNOWN)	--
FRANCE 192	NAVY	TRIGRAPHIC SUBSTITUTION "TABLES # 13" TO BE USED ON B.D.G., T.B.M., AND V.N. 1.	D.S.-B 613	?	?	?-1939-?	? OKW	COMPROMISED	T 919	(UNKNOWN)	--
FRANCE 193	NAVY	4-FIGURE 1-PART CODE, NOT STRICTLY ALPHABETIC.	D.T.; D.S.B 81Ø	?	?	?-1939-1941-?	? OKW	COMPROMISED	T 9Ø3	(UNKNOWN)	--
FRANCE 194	NAVY?	ENCIPHERED CODE.	?	D.S.D 3Ø4	?	? - ?	? SIS	COMPROMISED; READ.	IF 15Ø6	(UNKNOWN)	--
FRANCE 195	NAVY	DIGRAPHIC SUBSTITUTION SYSTEM, 2 LETTERS FOR EACH FIGURE.	?	?	?	?-194Ø-?	? OKW	COMPROMISED	T 935	(UNKNOWN)	--
FRANCE 196	NAVY	DIGRAPHIC SUBSTITUTION ENCIPHERMENT SYSTEM REPLACING A MARCH 1929 ENCIPHERMENT. COMBINES LETTERS AND FIGURES.	C.C.S. NO. 1; D.S.D 142	?	?	194Ø - ?	? OKW	COMPROMISED INSTRUCTIONS	T 1734	(UNKNOWN)	--
FRANCE 197	NAVY	NAVAL KEY TABLES TO BE USED WITH CODE E.X.	EXZO 5Ø, 6Ø, 7Ø	?	?	1941 - ?	? ?	COMPROMISED 1ØØ%	T 3562	(UNKNOWN)	--

FRANCE 198	NAVY	TRANSPOSITION ENCIPHERMENT SYSTEM WITH DIGRAPHIC LETTER SUBSTITUTION. USED ON INTERNATIONAL CODE BETWEEN COMMERCIAL SHIPS AND THE NAVY.	D.S.-B 7Ø4	NACOM;
				D.S.-B 7Ø4;
				INTERNATIONAL CODE N.C. 4
					?	1941 - ?	? OKW
							? SIS
								COMPROMISED 1ØØ% BY OKW AND SIS. READ BY SIS.	T 18Ø3
									IF 15Ø6
										(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
FRANCE	199	NAVY	ENCIPHERMENT SYSTEM TO REPLACE D.S.-B 7Ø4 AND IS SIMILAR TO IT.	N.C. NO.5	?	?	1941 - ?	? OKW	COMPROMISED 1ØØ%	T 18Ø3	(UNKNOWN)	--
FRANCE	2ØØ	NAVY	TRANSPOSITION ENCIPHERING TABLES WITH HOURLY CHANGING KEY. REPLACES VARETRA NO. 16.	D.S.D 12Ø VARETRA NO. 17	?	?	194Ø - ?	? OKW	COMPROMISED 1ØØ%	T 1683	(UNKNOWN)	--
FRANCE--VICHY	2Ø1	POLICE	5-LETTER ?-PART CODE.	?	?	?	?-194Ø-1942-?	? OKW	READ	T 17Ø8	(UNKNOWN)	--
FRANCE	2Ø2	POLICE	4-FIGURE OR 5-FIGURE ?-PART CODE.	?	?	?	?-1929-1938-?	? OKW	READ	T 2626	(UNKNOWN)	--
FRANCE	2Ø3	GENERAL PURPOSES	3-LETTER 1-PART CODE.	?	?	?	? - ?	? ?	COMPROMISED 1ØØ%	T 184Ø	(UNKNOWN)	--
FRANCE	2Ø4	GENERAL PURPOSES?	4-FIGURE 1-PART CODE. PAGINATION AND FIRST 2 DIGUTS TO BE FILLED IN BY USERS.	CHIFFRE 13	?	?	? - ?	192Ø PROBABLY GERMANS	PROBABLY 1ØØ% COMPROMISED	T 3548	(UNKNOWN)	(RESEMBLES SITTLER)
FRANCE	2Ø5	?	4-FIGURE-LETTER 1-PART CODE.	?	H.Z.B.	?	? - ?	? GERMANS	RECOVERED 8%	T 2484	(UNKNOWN)	--
FRANCE	2Ø6	?	4-FIGURE 2-PART CODE.	?	C 53 STAT. 1-279	?	? - ?	? GERMANS	RECOVERED 1Ø%	T 3156	(UNIDENTIFIED)	--
FRANCE	2Ø7	?	4-FIGURE 2-PART CODE.	?	F 5	?	? - ?	? ?	RECOVERED 5%	T 2497	(UNIDENTIFIED)	--
FRANCE	2Ø8	?	4?-FIGURE 2-PART CODE.	CHIFFRE NO. 11Ø	H 26 DAUTE	?	? - ?	? ITALIANS	RECONSTRUCTED 1Ø%	T 9Ø	(UNIDENTIFIED)	--
FRANCE	2Ø9	?	4-FIGURE 1-PART CODE. 9,9ØØ GROUPS.	?	?	?	? - ?	? ?	COMPROMISED 1ØØ%	T 3553	(UNKNOWN)	--
FRANCE--FREE FRANCE	21Ø	?	PROBABLY 4-FIGURE ?-PART CODE WITH ADDITIVE ENCIPHERMENT.	?	?	?	? - ?	? SIM	NOT READ	IF 1522	(UNIDENTIFIED)	--
FRANCE	211	?	4-FIGURE ?-PART CODE.	?	FRANZ	?	?-1925-?	? ?	READ	T 2536	(UNIDENTIFIED)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
GREECE 1	(CONSULAR AND SOME DIPLOMATIC)	4-LETTER (2-PART) CODE. UNENCIPHERED. ONLY 1Ø LETTERS USED TO FORM CODE GROUPS.	(ETA)	GZ	(GRD)	(194Ø-CURRENT)	? OKW AND PERHAPS PERS Z S ? SIM	ALMOST COMPLETELY READ BY GERMANS. READ BY SIM.	T 1Ø65 AND PERHAPS I 22 P 2 D 71	(HAD BRITISH COMPROMISED BOOK. CODE UNREADABLE. VALUES ADDED. TICOM GAVE SOLUTION)	--
GREECE 2	(MILITARY ATTACHE, DIPLOMATIC, AND CONSULAR)	4-LETTER (2-PART) CODE WITH 5TH LETTER ADDED FOR INFLECTION. (UNENCIPHERED)	(IOTA)	?	(GRB)	(1941-CURRENT)	? PERS Z S	READ	I 22 P 2Ø T 2253 T 2255 T 2257	(BEGAN TO READ IN 1944 WITH COMPROMISED BOOK. STILL READ.)	--
GREECE 3	CONSULAR	4-LETTER (2-PART) CODE WITH 5TH LETTER ADDED FOR INFLECTION. UNENCIPHERED. ONLY 1Ø LETTERS TO FORM CODE GROUPS.	BETA	T	(GRC)	(1938-CURRENT)	? PERHAPS PERS Z S	READ, PROBABLY COMPROMISED.	T 1Ø63 AND PERHAPS I 22 P 2Ø T 2Ø52	(BEING READ AS RESULT OF TICOM)	--
GREECE 4	CONSULAR	4-LETTER 2-PART CODE. UNENCIPHERED. ONLY 1Ø LETTERS USED TO FORM CODE GROUPS.	(PHI)	F	(GRH)	BEFORE 1939 - (CURRENT)	1939 PERS Z S	PARTIALLY RECONSTRUCTED	T 2Ø52	(UNKNOWN UNTIL MADE READABLE AS RESULT OF TICOM)	--
GREECE 5	MILITARY ?	4-LETTER ?-PART CODE WITH 5TH LETTER ADDED FOR INFLECTION, ADDITIVELY ENCIPHERED -- PERIOD OF 35.	?	?	?	? - ?	1941 OKW	SOLVED	I 58 P 6	(UNKNOWN)	--
GREECE 6	?	5-FIGURE ?-PART TRANSPOSED CODE.	?	?	?	? - 1941 - ?	1941 OKW	?	I 58 P 2	(UNKNOWN)	--
GREECE 7	(DIPLOMATIC)	4-FIGURE 2-PART CODE. NUMBER DIGRAPHS ENCIPHERED BY LETTER DIGRAPHS. ENCIPHERING TABLE CHANGES WITH DAY OF MONTH.	(ALPHA)	?	(GRA)	(1942-CURRENT)	BEFORE 194Ø SIM ? OKW ? PERS Z S	READ COMPLETELY BY OKW. PROBABLY READ BY SIM.	I 22 P 2Ø IF 1518 P 3 T 781	(IN PROCESS OF BOOK SOLUTION)	--
GREECE 8	(DIPLOMATIC)	4-FIGURE (?)-PART CODE REPAGINATED AND ENCIPHERED BY DIGRAPHIC LE"TER SUBSTITUTION.	DELTA	?	(GRG)	? - 1938 - (CURRENT)	BEFORE 194Ø SIM ? GERMANS	COMPROMISED BY GERMANS. READ BY SIM.	IF 1518 P 2 T 3267 T 3269 T 3Ø5Ø	(READABLE AS RESULT OF TICOM LIGHT TRAFFIC)	--
GREECE 9	?	4-FIGURE 1-PART CODE.	ELLENIKON KRYPTOGRAPHIKON LEXIKON	?	?	? - 1927 - ?	? PERHAPS PERS Z S	1ØØ% COMPROMISED.	T 3Ø51	(ASA HAS COMPROMISED CODE BOOK. UNKNOWN SYSTEM).	--
GREECE 1Ø	PROBABLY DIPLOMATIC	2 UNENCIPHERED CODES.	?	?	?	? - ?	? FA	READ	I 25 P 8	(UNIDENTIFIED)	--
GREECE 11	ARMY AND NAVY	CODES	?	?	?	? - ?	AFTER 194Ø OKH	BROKEN BY OKH	I 17Ø P 2	(NO MILITARY SYSTEMS WORKED ON)	--
GREECE 12	AIR	UNENCIPHERED CODE. VERY ELEMENTARY.	?	?	?	? - 1941 - ?	? OKL	READ	I 65 P 3 I 121 P 9	(NO MILITARY SYSTEMS WORKED ON)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
GREECE	13	MILITARY	2-FIGURE SUBSTITUTION CIPHER WITH VARIANTS.	?	?	?	? - 1944 ?	PRIOR TO 1944 OKH	READ	I 17Ø P 5	(NO MILITARY SYSTEMS WORKED ON)	--
GREECE	14	AIR	SINGLE TRANSPOSITION CIPHER.	?	?	?	? - 1941 - ?	1941 OKH	BROKEN AND ALMOST COMPLETELY READ	I 17Ø P 2	(NO MILITARY SYSTEMS WORKED ON)	--
GREECE ELAS	15	ARMY	DOUBLE TRANSPOSITION CIPHER.	?	?	?	1944? - 1945?	APPROX. 1944 OKH	5Ø% - 6Ø% OF THE TRAFFIC READ	I 17Ø P 5	(NO MILITARY SYSTEMS WORKED ON)	--
GREECE	16	DIPLOMATIC	4 LETTER 4 FIGURE 1-PART CODE ENCIPHERED BY TABLES INTO LETTERS. PAGE DIGRAPH COULD PRECEDE OR FOLLOW GROUP DIGRAPH.	?	?	?	? - ?	? SIM	READ?	IF 1518	(UNIDENTIFIED)	--

TOP SECRET

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
HUNGARY 1	?	ENIGMA CIPHER MACHINE.	?	ENIGMA	?	?-1941-?	? OKH ? SIM	GERMANS BUILT MACHINES BUT COULD NOT COMPROMISE WHEEL WIRINGS BECAUSE HUNGARIANS CHANGED THEM AT NIGHT. NOT READ BY SIM.	I 84 P 3 IF 1518	(UNKNOWN)	--
HUNGARY 2	DIPLOMATIC	5-FIGURE (2)-PART CODE. ORIGINALLY UNENCIPHERED, BUT LATER ENCIPHERED. 500 PAGE RANGE. INDICATOR WAS LAST GROUP OF MESSAGE CONSISTING OF 5 ODD NUMBERS. (USED ON TOKYO-BUDAPEST CIRCUIT ONLY.)	?	"U.1"	(HUA)	(1938-1945)	1940 OKW	SOLVED UNENCIPHERED; UNABLE TO SOLVE ENCIPHERED.	T 2248	(READ FROM SEPTEMBER 1944 TO END OF WAR. 1932 VII CODE BOOK COMPROMISED.	(HUC, CIRCULAR SYSTEM, USED SAME SYSTEM AND BOOK. READABLE ONLY WITH KEYS DERIVED FROM HUA.)
HUNGARY 3	DIPLOMATIC	5-FIGURE (2)-PART CODE. 300 PAGE RANGE. ASSUMED TO BE ENCIPHERED BY DIGIT-FOR-DIGIT SUBSTITUTION.	?	"U.3"	(HUE?)	1938-1940-?	1940 OKW	NO SUCCESS	T 2248	(NOT READABLE. 1935 VIII CODE BOOK COMPROMISED.)	--
HUNGARY 4	DIPLOMATIC	5-FIGURE (2)-PART CODE. 300 PAGE PANGE. ENCIPHERED BY DIGIT-FOR-DIGIT SUBSTITUTION. INDICATOR WAS LAST GROUP WITH 2 ODD AND 3 EVEN NUMBERS.	?	"U.2"	(HUD)	1938-1940-?	1940 OKW	NO SUCCESS	T 2248	(PARTLY READABLE WITH KEYS DERIVED FROM HUA AND HUC. 1936 IX CODE BOOK COMPROMISED.)	--
HUNGARY 5	?	TRANSPOSITION CIPHER USING REVERSIBLE REVOLVING GRILLE. USED BY HUNGARIAN RAILWAYS ADMINISTRATION.	?	?	?	? - 1941 - ?	1941 OKH	SOLVED	I 58; I 100 IF 126 P 9	(UNKNOWN)	--
IRAN 1	DIPLOMATIC	3-LETTER 1-PART CODE WITH VARICUS ENCIPHERMENT SYSTEMS.	?	?	(IRA)	(1939-CURRENT)	? PERS Z S	SOLVED	I 22 P 20	(100% COMPROMISED. MOST KEYS READ.)	--
IRAN? 2	COMMERCIAL	CODE USED BY CZECHOSLOVAKIA SKODA FIRM TO IRAN AND IRAC CONCERNING BRIDGE BUILDING PROJECTS.	?	?	?	? - 1935 - ?	1935 OKL	SOLVED	I 162 P 2	(UNKNOWN)	--
IRAC?	COMMERCIAL	CODE USED BY CZECHOSLOVAKIA SKODA FIRM TO IRAN AND IRAC CONCERNING BRIDGE BUILDING PROJECTS.	?	?	?	? - 1935 - ?	1935 OKL	SOLVED	I 162 P 2	(UNKNOWN)	--
IRELAND EIRE 1	DIPLOMATIC AND CONSULAR	5-LETTER 1-PART CODE. 84,000 GROUPS. USED UNENCIPHERED AND ENCIPHERED WITH SUBSTITUTION AND WITH REPEATING ADDITIVE WITH A PERIOD OF 330,	GOVERNMENT TELEGRAPH CODE	B 22	(IEB, IEC, AND IEA)	(IEA, IEB: 1942-CURRENT. IEC: 1942-1945)	1938 PERS Z S 1944 FA	BROKE CODE. LATER RECEIVED COMPROMISED COPY. IN 1941 SUBSTITUTION ENCIPHERMENT SOLVED. ADDITIVE NOT WORKED ON IN 1941	D 16, 1941 REPORT P 1 D 16, 1942 REPORT PP 2, 3 I 172 PP 3,4 ALSO SEE I 54 P 3	(PARTIALLY BROKEN IN 1944 WHEN COMPROMISED BOOK WAS OBTAINED. STILL BEING READ. SUBSTITUTION ENCIPHERMENT SOLVED IN 1945. ADDITIVE SYSTEM BEING READ ON DEPTHS. STILL BEING WORKED ON.)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
ITALY 1	(FOREIGN MINISTRY)	(5-LETTER) 2-PART CODE. ABOUT 3Ø,ØØØ GROUPS. NO ENCIPHERMENT.	AR 38	R 19	(ITF) (ITX-6)	194Ø - ?	? PERS Z S	3,Ø25 GROUPS SOLVED	T 2252	(1Ø,25Ø GROUPS RECOVERED. COMPROMISED COPY RECEIVED 1944.)	--
ITALY 2	FOREIGN MINISTRY	5-LETTER 2-PART CODE. PAGE RANGE ABA-OFU. NO INDICATOR, NO ENCIPHERMENT.	(AR 4Ø)	ITALIAN CODE-BOOK 21	(ITG)	1942 - ?	1942 PERS Z S	RECOVERED ? PERCENT	T 2194	(4,ØØØ GROUPS RECOVERED. COMPROMISED COPY RECEIVED 1944.)	--
ITALY 3	?	5-LETTER 2-PART CODE.	?	P 1Ø	?	1937 - ?	? ?	RECOVERED 2Ø%	T 92	(UNIDENTIFIED)	--
ITALY 4	(FOREIGN MINISTRY)	5-FIGURE 1-PART CODE. PAGE RANGE 1ØØ-3Ø2. VALUES IN FRENCH.	H 25	H 26	?	BEFORE 1914 - ?	? PERS Z S	ABOUT 3,ØØØ GROUPS RECOVERED	T 2252	(UNKNOWN IN ASA BEFORE RECEIPT OF COMPROMISED COPY, 1944.)	--
ITALY 5	FOREIGN MINISTRY	5-FIGURE 1-PART CODE. 18,5ØØ OR 18,6ØØ GROUPS. FIRST GROUP WAS INDICATOR.	RA 1 CIFRARIO TASCABILE	R 15	?	1937 - ?	? PERS Z S	RECOVERED 8Ø%	T 88 T 2252 T 3Ø36 T 3Ø37	(COMPLETELY RECONSTRUCTED IN ASA. COMPROMISED COPY RECEIVED 1944.)	--
ITALY 6	FOREIGN MINISTRY	5-FIGURE 1-PART CODE. PAGE RANGE ØØ3-186. 18,4ØØ GROUPS. ENCIPHERED WITH "TABELLA LM" AND 1Ø-PLACE TABLE.	RA	R 11	(ITH)	?	1935-194Ø PERS Z S	RECOVERED 7Ø%	T 2252 T 3Ø35	(COMPLETELY RECONSTRUCTED IN ASA. COMPROMISED COPY RECEIVED 1944.)	--
ITALY 7	FOREIGN MINISTRY	5-FIGURE 2-PART CODE. PAGE RANGE 1ØØ-544. NO ENCIPHERMENT. 13,4ØØ GROUPS.	Y-1	R 4 ZILLI II OR R 7	(ITP)	193Ø-1933	? PERS Z S	5,5ØØ GROUPS SOLVED	T 94 T 2249 T 2252 T 3Ø33	(COMPROMISED COPY RECEIVED IN ASA FROM GCCS IN 1943.)	--
ITALY 8	FOREIGN MINISTRY	5-FIGURE 2-PART CODE. 27,7ØØ GROUPS.	AR 25	R 8	(ITB) (ITX-2)	1933 - ?	? PERS Z S	9,5ØØ GROUPS SOLVED	T 2252 T 3Ø45	(8,1ØØ GROUPS RECOVERED IN ASA. COMPROMISED COPY RECEIVED 1944.)	--
ITALY 9	FOREIGN MINISTRY	5-FIGURE 2-PART CODE. 26,5ØØ GROUPS. ENCIPHERED WITH "TABELLA LM".	AR 29	R 12	(ITC)	1936-1938	? PERS Z S	RECOVERED ABOUT 5Ø%	T 2252 T 3Ø46	(3,75Ø GROUPS RECOVERED.)	--
ITALY 1Ø	FOREIGN MINISTRY	5-FIGURE 2-PART CODE. 26,1ØØ GROUPS. PAGE RANGE 2Ø1-6Ø5.	AR 15	R 13	?	1936 - ?	? PERS Z S	RECOVERED 2Ø%	T 2252 T 3Ø44	(PAGINATION SENT TO ASA BY GCCS, WHERE SYSTEM IS KNOWN AS AR-Y. TRAFFIC NOT SEEN IN ASA.)	(3,ØØØ GROUPS IDENTIFIED IN GCCS.)
ITALY 11	FOREIGN MINISTRY	5-LETTER 2-PART CODE. 29,Ø64 GROUPS. NO ENCIPHERMENT.	AR 3Ø	R 14	(ITD) (ITX-3)	? - ?	1938 PERS Z S	1Ø,125 GROUPS SOLVED	T 2252	(12,4ØØ GROUPS RECOVERED IN ASA. COMPROMISED COPY RECEIVED 1944.)	--
ITALY 12	FOREIGN MINISTRY	5-FIGURE 2-PART CODE. 27,6ØØ GROUPS. PAGE RANGE 2Ø1-652. ENCIPHERED WITH 1ØØ-PLACE TABLE. INDICATOR: Ø BEFORE THE DATE.	AR 17	R 16	?	1937 - ?	1938 PERS Z S	4,442 GROUPS RECOVERED	T 2252 T 3Ø43	(PAGINATION AND ABOUT 2ØØ IDENTIFICATIONS SENT BY GCCS TO ASA. TRAFFIC NOT SEEN IN ASA.)	(KNOWN TO GCCS AS AR-Z.)
ITALY 13	(FOREIGN MINISTRY)	5-FIGURE 2-PART CODE. 26.7ØØ GROUPS.	IMPERO	R 18	(ITA) (ITX-4)	1937 - ? (1938 - ?)	? PERS Z S	6,ØØ6 GROUPS SOLVED; "READ" BY PERS Z S. WORKBOOK: 4Ø% RECOVERED	T 97 T 2252 T 2314 T 3Ø4Ø T 3Ø47 T 1117 I-22 P 3 P 8	(8,5ØØ GROUPS RECOVERED. COMPROMISED COPY RECEIVED, 1944.)	--

CHART NO. 1-2

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
ITALY	14	(FOREIGN MINISTRY)	5-FIGURE 2-PART CODE. 251 PAGES.	(AQUILA)	R 22	(ITX-7)	(PUBLICATION DATE 1942)	? ?	RECOVERED 2Ø%-25%	T 96 T 112Ø	(UNKNOWN IN ASA BEFORE RECEIPT OF COMPROMISED COPY IN 1944.)	--
ITALY	15	(FOREIGN MINISTRY)	5-FIGURE (2-PART) CODE. (17,775 GROUPS.)	(ASSE)	I.T.B. 2Ø	?	(PUBLICATION DATE 1941)	? ?	RECOVERED 7%	T 2196	(COMPROMISED COPY RECEIVED 1944. UNKNOWN IN ASA BEFORE THEN EXCEPT FOR PAGINATION SUPPLIED BY GCCS.)	--
ITALY	16	?	5-FIGURE 2-PART CODE.	?	K 16	?	?	? ?	RECOVERED 2Ø%	T 2Ø93	(UNKNOWN)	--
ITALY	17	?	5-FIGURE 2-PART CODE.	?	K 18	?	1917 - ?	? ?	RECOVERED ABOUT 4Ø%	T 2Ø95	(UNKNOWN)	--
ITALY	18	?	5-FIGURE 2-PART CODE.	?	K 19	?	?	? ?	RECOVERED 5Ø%	T 1Ø4Ø T 2Ø9Ø	(UNKNOWN)	--
ITALY	19	?	5-FIGURE 2-PART CODE.	?	K 2Ø	?	?	? ?	RECOVERED 2Ø%	T 2Ø94 T 3Ø39	(UNKNOWN)	--
ITALY	2Ø	?	5-FIGURE 2-PART CODE.	P 1	P 1	?	1919 - ?	? ?	RECOVERED LESS THAN 5%	T 3Ø42	(KNOWN IN ASA BY NAME ONLY, THROUGH GCCS.)	--
ITALY	21	?	5-FIGURE 2-PART CODE.	P 2	P 2	?	1919-192Ø	? ?	RECOVERED 5Ø%	T 3Ø41	(KNOWN IN ASA BY NAME ONLY, THROUGH GCCS.)	--
ITALY	22	?	5-FIGURE 2-PART CODE.	P 3	P 3	?	BEFORE 1931	? ?	RECOVERED 15%-2Ø%	T 89	(PAGINATION KNOWN IN ASA, SENT BY GCCS.)	(ENCODE WAS SOURCE OF LMB AND LMC ADDITIVE)
ITALY	23	?	5-FIGURE 2-PART CODE.	P 4	P 4	?	1924 - ?	? ?	RECOVERED 4Ø%-5Ø%	T 9Ø	(KNOWN IN ASA BY NAME ONLY, THROUGH GCCS.)	--
ITALY	24	?	5-FIGURE 2-PART CODE. PAGE RANGE 1ØØ-598.	?	S 1	?	?	? ?	RECOVERED 1Ø%-15%	T 2197	(UNKNOWN)	--
ITALY	25	?	5-FIGURE 2-PART CODE. PAGE RANGE ØØØ-211.	?	F.Z. 2 CHIFFRIER-CODE	?	? - 1918 - ?	? ?	RECOVERED 2Ø%	T 2Ø92 T 2Ø97	(UNKNOWN)	--
ITALY	26	?	5-FIGURE POSSIBLY 1-PART CODE.	?	K 14	?	?	? ?	RECOVERED 15%	T 3Ø38	(UNKNOWN)	--
ITALY	27	?	5-FIGURE 2-PART CODE.	?	R 3	?	?	? PERS Z S	RECOVERED 5Ø%-6Ø%	T 91	(UNKNOWN)	--
ITALY	28	?	4-FIGURE ?-PART CODE.	?	K 15 R^{3} 14	?	?	? ?	RECOVERED 3Ø%-4Ø%	T 3Ø4Ø	(UNKNOWN)	--

TOP SECRET

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
ITALY 29	EMBASSY, MADRID	GERMAN DESCRIPTION: "1943. 4-PLACE ITALIAN FIGURE CODE COMPILED ON THE BASIS OF CAPTURED MATERIAL. TRAFFIC: ITALIAN EMBASSY MADRID AND THE ITALIAN REPRESENTATIONS IN SPAIN." PAGE RANGE ØØ-99.	?	?	?	? - 1943 - ?	?	RECOVERED 6%-7%	T 3Ø48 T 3Ø49	(UNKNOWN)	--
ITALY 3Ø	FOREIGN MINISTRY	2-PART CODE. 21,4ØØ GROUPS.	AR 1	?	?	1931 - ? USED IN 1939	1939 PERS Z S	?	T 2252	(UNIDENTIFIED)	--
ITALY 31	FOREIGN MINISTRY	2-PART CODE. ABOUT 3Ø,ØØØ GROUPS. USUALLY UNENCIPHERED.	RA 18	?	?	1938 - ?	194Ø PERS Z S	?	T 2252	(UNIDENTIFIED)	--
ITALY 32	?	2-PART CODE. ABOUT 22,ØØØ GROUPS. ENCIPHERED WITH 1ØØ-PLACE TABLE.	?	TB OHNE BEZEICHNUNG	?	1938 - ?	1943 PERS Z S	RECOVERED ABOUT 3,ØØØ GROUPS	T 2252	(UNIDENTIFIED)	--
ITALY 33	POLICE	4-FIGURE 2-PART CODE.	CIFRARIO "S.P."	?	?	?	1942 PERS Z S	1ØØ% COMPROMISED	T 87	(UNKNOWN IN ASA BEFORE RECEIPT OF COMPROMISED COPY)	SENT BY SCHAUFFLER OF PERS Z S TO PASCHKE OF PERS Z S, 12 SEPT. 1942.
ITALY 34	FOREIGN MINISTRY	CODE-ENCIPHERMENT SYSTEM: ADDITIVE TABLES RUNNING FROM 1 - 3 DAYS.	TABELLA LM	TABELLA LM	(ITA) (ITB) (ITC) (ITP)	1938 - ?	194Ø PERS Z S	BROKEN	T 2252	(ADDITIVE TABLES LARGELY RECOVERED)	--
ITALY 35	?	CODE-ENCIPHERMENT SYSTEM: 1ØØ-PLACE FIGURE-LETTER SUBSTITUTION TABLES.	?	?	?	?	? PERS Z S	?	T 2252	(UNIDENTIFIED)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
JAPAN 1	DIPLOMATIC	MACHINE CIPHER	"TACHI-BANA" OR "ANGOOKI TAIPU A"	JB 48	("RED" MACHINE)	1935-1941	BEFORE, 1939 PERS Z S	READ REGULARLY	I 64 P 3 I 9Ø P 2 P 4 D 5Ø P 33 I 118 PP 7-8 I 22 P 2 P 7 P 16	(SOLVED BY 1936)	--
JAPAN 2	DIPLOMATIC	MACHINE CIPHER, NOT RECOGNIZED BY GERMANS AS DIFFERENT FROM "RED" MACHINE.	"HINOKI" OR "ANGOOKI TAIPU B"	JB 48	("PURPLE" MACHINE) (JAA)	1939-1945	? PERS Z S	NOT READ	D 5Ø PP 22-31, 33 I 64 P 3 I 9Ø PP 2-4 I 118 PP 7-8 I 22 PP 2, 7, 16	(BROKEN 2Ø FEBRUARY 194Ø)	--
JAPAN 3		A SERIES OF LETTER CODES USED BEFORE 1934; GERMAN DESIGNATIONS RUN FROM JB 3 TO JB 28, PLUS JB 3Ø AND JB 31.					? PERS Z S		D 5Ø		--
JAPAN 4	DIPLOMATIC	5-LETTER CODE, GROUPS IN FORM CVCCV. 1Ø,ØØØ VALUES.	?	JB 55	?	194Ø - ?	1941 PERS Z S	NOT SOLVED	D 5Ø P 34	(UNIDENTIFIED)	--
JAPAN 5	?	4-LETTER CODE MADE FROM CO-ORDINATES.	?	JB 51	?	? - ?	?	COMPLETELY RECOVERED WITHIN LIMITS OF AVAILABLE DIAGRAM	T 335	(UNIDENTIFIED)	--
JAPAN 6	DIPLOMATIC	4-LETTER CODE, PRONOUNCEABLE GROUPS.	?	JB 59	?		1941 PERS Z S	NOT READ	D 5Ø P 35	(UNIDENTIFIED)	--
JAPAN 7	?	4-LETTER CODE.	?	KIMI	?	? - ?	?	RECOVERED 1Ø%	T 2ØØØ T 2ØØ1 T 2ØØ2 T 23ØØ	(UNIDENTIFIED)	--
JAPAN 8	(DIPLOMATIC)	2-LETTER 4-LETTER CODE; INDICATOR WAS "LA".	?	JB 29 OR "LA"-CODE	(JAH) OR ("LA")	1925-1945	? OKW ? PERS Z S	OKW: FULLY RECOVERED. PERS Z S: GREATER PART OF TEXTS READ.	D 5Ø P 14 P 16 I 9Ø PP 2-4 I 118 PP 7-8 I 15Ø P 8	(BROKEN IN 1927. 1925 COPY OF CODE CAPTURED. SLIGHTLY CHANGED IN 1934. READ 1ØØ%.)	--
JAPAN 9	DIPLOMATIC	2-LETTER 4-LETTER CODE; 2-LETTER GROUPS CV OR VC; 4-LETTER GROUPS PRONOUNCEABLE. INDICATOR: "IJ". (OTHER INDICATORS: IP, AN, PA, KA)	?	JB 44	(JAI?)	(1941-1945)	? PERS Z S	?	D 5Ø P 33	(SOLVED 1941)	
JAPAN 1Ø	DIPLOMATIC	2-LETTER 4-LETTER CODE. 2-LETTER GROUPS VC OR CV; 4-LETTER GROUPS VVCC. INDICATOR: "HE". USED AS SPELLER.	?	JB 47	("HE")	? - ?	? PERS Z S	?	D 5Ø P 33	(READ)	--
JAPAN 11	?	2-LETTER 4-LETTER CODE. TRANSPOSED ON KEY OF LENGTH 7, 1Ø, 14, OR 15. FIRST CIPHER GROUP OF TEXT TRANSPOSED ACCORDING TO UNIT OF DATE AND PLACED AT END OF MESSAGE. ENCIPHERMENT CHANGED 1 JUNE 194Ø AND 3 NEW 7-PLACE KEYS WERE FOUND.	?	JB 5Ø	("PA-KI")	(1939-194Ø)	? PERS Z S	?	D 5Ø P 34	(READ)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
JAPAN 12	DIPLOMATIC	2-LETTER 4-LETTER CODE. 2-LETTER GROUPS, ANY EXCEPT "PAIRS;" 4-LETTER GROUPS PRONOUNCEABLE.	?	JB 52	("J-12")	1 JAN 194Ø - 31 MAY 194Ø	? PERS Z S	SOME RECOVERED	D 5Ø P 34 T 336	(READ)	--
JAPAN 13	DIPLOMATIC	2-LETTER 4-LETTER CODE WITH INDICATOR IN FORM CVCCV. ENCIPHERED BY TRANSPOSITION; RECTANGLE HAD BLANK CELLS.	?	JB 57	("J-16 K-5")	194Ø-1942	? PERS Z S ? RLM/FA	READ BY PERS Z S VIRTUALLY THE ENTIRE TIME	D 5Ø P 34 PP 42-43 T 38Ø I 22 P 21 I 54	(READ)	--
JAPAN 14	(FOREIGN OFFICE)	2-LETTER 4-LETTER CODE. 4-LETTER GROUPS HAD FORM CCVC OR VCCC. INDICATOR GROUP: "IP".	?	JB 6Ø	(JAI?)	(1941-1945)	? OKW ? PERS Z S	?	D 5Ø P 42 I 15Ø P 8	(SOLVED IN 1941)	--
JAPAN 15	(FOREIGN OFFICE)	2-LETTER 4-LETTER CODE ENCIPHERED BY TRANSPOSITION. RECTANGLE HAD BLANK CELLS.	?	J-13 "FUJI".	(JAE) OR ("J-19")	(1941-1943)	? OKW	SOLVED	I 31 PP 4-5, 8 I 118 PP 7-8 I 84 P 5 I 124 P 3	(SOLVED AUGUST 1941)	--
JAPAN 16	DIPLOMATIC	2-LETTER 4-LETTER CODE, TRANSPOSED ON BASIS OF A REPEATING 19-PLACE KEYWORD. "KOKOK", "GAGAG", ETC., WERE INDICATOR GROUPS.	?	"KOKOK"	?	? - 1942	1941 OKW	READ	I 31 P 5 P 8 I 9Ø PP 2-4 I 118 PP 7-8 I 84 P 5 I 15Ø P 8	(UNIDENTIFIED)	--
JAPAN 17	DIPLOMATIC	2-LETTER 4-LETTER CODE. 2-LETTER GROUPS OF FORM VC OR CV AND 4-LETTER GROUPS PRONOUNCEABLE. INDICATOR GROUP: "KO".	?	?	(JAW)	? - 194Ø - ?	194Ø PERS Z S	?	D 5Ø P 35	(COMPROMISED)	--
JAPAN 18	DIPLOMATIC	2-LETTER 4-LETTER CODE ENCIPHERED BY DOUBLE ? TRANSPOSITION.	?	?	?	1942-1943	1942 PERS Z S	READ FROM MIDDLE OF 1942 TO JUNE OR JULY 1943	I 22 P 8	(UNIDENTIFIED)	--
JAPAN 19	DIPLOMATIC	2-LETTER 3-LETTER 4-LETTER CODE. 2-LETTER GROUPS ANY, EXCEPT "PAIRS AND DOUBLE VOWELS;" 3-LETTER GROUPS VOWELS; 4-LETTERGROUPS PRONOUNCEABLE.	?	JB 53	("J-14")	1 JAN 194Ø - 15 AUG 194Ø	? PERS Z S	?	D 5Ø P 34	(READ)	--
JAPAN 2Ø	DIPLOMATIC	2-LETTER 3-LETTER 4-LETTER CODE. 2-LETTER GROUPS ANY, EXCEPT "FAIRS AND DOUBLE VOWELS;" 3-LETTER GROUPS VOWELS, TAKEN FROM "J-14"; 4-LETTER GROUPS PRONOUNCEABLE.	?	JB 54	("J-15"?)	15 AUG 194Ø- 31 OCT 194Ø	? PERS Z S	?	D 5Ø P 34	(READ)	--
JAPAN 21	DIPLOMATIC	SUCCESSOR TO PA-K 1. 2-LETTER 3-LETTER 4-LETTER CODE. 2-LETTER ANY, EXCEPT "PAIRS AND DOUBLE VOWELS;" 3-LETTER VOWELS, TAKEN FROM J-14; 4-LETTER PRONOUNCEABLE.	?	JB 58	("K-3")	1 JUL 194Ø - 1 DEC 194Ø	? PERS Z S	?	D 5Ø P 34 P 35	(READ)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
JAPAN	22	?	3-LETTER CODE, 12ØØ VALUES IN BOX 1ØX12Ø.	?	JB 35	("XA")	1934 - ?	1934 PERS Z S	BROKEN	T 1124	(READ)	--
JAPAN	23	?	3-LETTER CODE, SIMILAR TO JAPAN 22.	?	JB 37	("XB")	1934 - ?	1934? PERS Z S	BROKEN	T 1124 T 5Ø	(READ)	--
JAPAN	24	DIPLOMATIC	2-LETTER 3-LETTER CODE, TRANSPOSED. RECTANGLE WAS 25X1Ø. ORIGINALLY USED "SIGNATURE" NULLS, (LATER ADOPTED BLANK CELLS INSTEAD.)	?	JB 54	(JBA)	(1943-1945)	? PERS Z S	BROKEN	I 22 P 17 T 346 T 345	(5Ø% - 1ØØ% READABLE TILL MARCH 1945; 25% - 5Ø% IN APRIL 1945; UNDER 25% AFTER APRIL 1945.)	--
JAPAN	25	DIPLOMATIC	2-LETTER 4 (?)-LETTEB CODE, TRANSPOSED. RECTANGLE HAD WIDTH OF 25, DEPTH OF 1Ø, WITH BLANK CELLS. IN JAN 1944, BLANK CELLS RAN VERTICALLY AND HORIZONTALLY.	?	?	(JBA)	(1943-1945)	? OKW	BROKEN	I 9Ø PP 2-4	(5Ø% - 1ØØ% READABLE TILL MARCH 1945; 25% - 5Ø% IN APRIL 1945; UNDER 25% AFTER APRIL 1945.)	(JBA IS A 2-LETTER 3-LETTER CODE BUT CHANGE IN NULLS DESCRIBED TOOK PLACE IN JBA IN DEC 1944)
JAPAN	26	DIPLOMATIC	2-LETTER CODE: INDICATOR GROUP: "CA".	?	JB 56	(JAJ)	1936-1945	194Ø PERS Z S	READ SMALL AMOUNT	D 5Ø P 34 T 3179	(BROKEN, FALL 194Ø)	(OFTEN ENCIPHERED BY JAA, JBB, JBC, OR JBD)
JAPAN	27	DIPLOMATIC	2-LETTER 1-PART CODE, CV, ENCIPHERED BY SINGLE TRANSPOSITION WITH RECTANGLE 6 WIDE, 5 OR 1Ø DEEP WITH BLANKS DISTRIBUTED EVENLY THROUGHOUT. THREE KEYS. USED BETWEEN JAPAN AND BURMA, PHILLIPINES, ETC.	?	ABABA, BCBCB, CDCDC, ETC.	?	1942-1943	1942 PERS Z S ? OKW	PERS Z S: ? OKW: READ UNTIL 1944	I 3Ø PP 2-4 I 22 P 17	(UNIDENTIFIED)	--
JAPAN	28	DIPLOMATIC	?-LETTER ?-PART CODE, TRANSPOSED. RECTANGLE HAD BLANK CELLS. DAILY KEY.	?	?	?	? - 1943	? OKW	?	I 9Ø PP 2-4	(UNIDENTIFIED)	--
JAPAN	29	DIPLOMATIC	4-FIGURE 12ØØ-VALUE CODE ENCIPHERED BY BOOK ADDITIVE. ADDITIVE BOOK HAD 4ØØ,ØØØ ADDITIVE VALUES, EACH PAGE OF BOOK BEING DRAWN UP 2Ø X 25. THE POINT AT WHICH THE ENCIPHERER STARTED TO USE THE ADDITIVE WAS INDICATED BY AN INDICATOR GROUP, E.G. TLUSR. AFTER THE ADDITIVE PROCEDURE WAS COMPLETED, THE FIGURES WERE CONVERTED TO LETTERS, THE SAME LETTERS ALWAYS REPRESENTING THE SAME NUMBERS.	?	?	(JAM)	(1942-1944)	? OKW	?	I 9Ø PP 2-4	(BROKEN JAN 1945, 25% - 5Ø% READABLE; WORK DISCONTINUED APR 1945)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
JAPAN 30	(FOREIGN OFFICE)	4-FIGURE CODE WITH ONLY 2,500 GROUPS. ENCIPHERED BY BOOK ADDITIVE AND SIMPLE LETTER SUBSTITUTION USING THE LETTERS CFGKLNORSY.	?	JB 62	(JBC)	(1943-1945)	? PERS 7 S	ADDITIVE STRIPPED AND BOOK-BREAKING BEGUN	I 22 P 17	(BROKEN JAN 1944; 2 ADDITIVE BOOKS USED, SECOND EFFECTIVE 1 FEB 1944, BOTH RECOVERED. 100 % READABLE.)	--
JAPAN 31	DIPLOMATIC-COMMERCIAL	DIGRAPHIC SUBSTITUTION AND TRANSPOSITION APPLIED TO 4 CODES, DESIGNATED AHSAJ, ETGAV, AMNUM, ILNIM. AHSAJ WAS A 3, 4, 5-LETTER CODE; ETGAV WAS 6-LETTER; AMNUM WAS 5-LETTER; ILNIM WAS UNKNOWN. EACH CODE HAD 10,000 VALUES. 2 ENCIPHERING TABLES: CIFOL USED ON EVEN DAYS, VEVAZ ON ODD DAYS.	?	"CIFOL-VEVAZ"	("CIFOL-VEVAZ")	(1940 - ?)	? OKW	40% - 50% RECOVERED	I 31 P 8 I 90 PP 2-4 I 118 PP 7-8 I 150 P 8	--	
JAPAN 32	DIPLOMATIC	MONOALPHABETIC SUBSTITUTION CIPHER WITH 2-LETTER GROUPS FOR PUNCTUATION; INDICATOR GROUP: "YUG".	?	JB 41	("YUG")	1936-1941	? PERS Z S	?	D 50 P 33	(READ)	
JAPAN 33	COMMERCIAL	MONOALPHABETIC SUBSTITUTION ACCORDING TO THE DAY OF THE MONTH. INDICATOR: "IRADE".	?	?	?	? - 1940 - ?	? OKW	?	D 50 P 35 P 42	--	--
JAPAN 34	DIPLOMATIC	TRANSPOSITION CIPHER WITH 5-FIGURE INDICATOR GROUP.	?	?	?	? - 1940 - ?	? PERS Z S	?	D 50 P 35	(UNIDENTIFIED)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
LATVIA	1	DIPLOMATIC	TRANSPOSITION CIPHER, BOTH SINGLE AND DOUBLE, SOMETIMES SUPERENCIPHERED WITH VIGENERE SUBSTITUTION.	?	?	?	? - ?	? PERS Z S	?	I 22 P 1Ø	(UNKNOWN. ONLY PLAIN TEXT MESSAGES RECEIVED AT ASA.)	--
LITHUANIA	1	DIPLOMATIC	TRANSPOSITION CIPHER, BOTH DOUBLE AND SINGLE, SOMETIMES SUPERENCIPHERED WITH VIGENERE SUBSTITUTION.	?	?	?	? - ?	? PERS Z S	- ?	I 22 P 1Ø	(LITHUANIAN TRAFFIC NOT WORKED ON BY ASA.)	--
LITHUANIA	2	AIR FORCE	TRANSPOSITION CIPHER WITH REVOLVING GRILLE.	?	?	?	1938-1939	1938 OKL	READ CURRENTLY	I 121 P 4	(LITHUANIAN TRAFFIC NOT WORKED ON AT ASA.)	--
MANCHURIA	1	DIPLOMATIC	5-FIGURE 2-PART CODE.	?	?	(MAA)	1942-1945	? ?		T 1	(NOT WORKED ON AT ASA.)	--
MANCHURIA	2	?	5-LETTER ?-PART CODE.	?	?	?	1938 - ?	? PERS Z S	?	T 76 P 36	(UNKNOWN)	--
MANCHURIA	3	?	5-LETTER ?-PART CODE. INDICATOR ABXYZ.	?	?	?	194Ø - ?	? PERS Z S	?	T 76 P 36	(UNKNOWN)	--
MANCHURIA	4	?	4-LETTER ?-PART CODE OF FORM CVCV. USED BETWEEN BERLIN AND ROME.	?	?	?	USED ONLY IN MARCH 194Ø	? PERS Z S	?	T 76 P 37	(UNKNOWN)	--
MANCHURIA	5	?	4-FIGURE 2-PART CODE. ALL MESSAGES STARTED WITH GROUP Ø3Ø11.	?	?	?	? - ?	? OKW	COMPROMISED.	I 177 P 3	(UNKNOWN)	--
MANCHURIA	6	DIPLOMATIC	TRANSPOSITION CIPHER WITH BLANK CELLS IN RECTANGLE AND DAILY CHANGING KEY. USED JAPANESE LANGUAGE.	?	?	?	1936 - ?	194Ø PERS Z S	SOLVED.	T 76 P 36, PP 39-41	(UNKNOWN)	--
MANCHURIA	7	PROBABLY COMMERCIAL	TRANSPOSITION CIPHER WITH CHANGING ENCIPHERMENTS GOVERNED BY DATE AND NUMBER.	?	?	?	1935 - ?	? PERS Z S	?	I 76 P 35	(UNKNOWN)	--
MANCHURIA	9	?	TRANSPOSITION ENCIPHERMENTS OF A BASIC JAPANESE 3-LETTER BOOK.	?	?	?	? - ?	? PERS Z S	?	I 22 P 21	(UNKNOWN)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
MEXICO 1	DIPLOMATIC	5-LETTER 1-PART CODE, WITH 20,000 PRONOUNCEABLE GROUPS. USED WITH A DAILY ENCIPHER TABLE AND WORKED ON SLIDING SCALE PRINCIPLE.	?	?	?	?-1940-?	? SIM	READ	IF 1517	(UNKNOWN)	--
MEXICO 2	DIPLOMATIC	5-LETTER 1-PART CODE. 100 DIFFERENT ENCIPHERMENTS: EACH GROUP ENCIPHERED BY A GROUP IN BASIC CODE OF FROM 1 TO ABOUT 150 PLACES LATER.	?	"POMOS"	(MXA)	(?-1941-1945)	1941 PERS Z S	SOLVED	D 16	(80% READABLE)	--
MEXICO 3	DIPLOMATIC	5-LETTER 1-PART CODE.	?	"MEXIKO ÜBER P"	(MXB)	(? - 1945)	? ?	RECOVERED LESS THAN 5%	T 2519	(75% - 80% READABLE)	(USED IN 1945 BY ONLY PORT-AU-PRINCE LEGATION)
MEXICO 4	DIPLOMATIC	5-LETTER 1-PART CODE, 20,000 PRONOUNCEABLE GROUPS. DAILY ENCIPHERING TABLE. CODE MIXED WITH CLEAR.	?	?	?	? - ?	? SIM	READ	IF 1517	(UNIDENTIFIED)	--
MEXICO 5	DIPLOMATIC	5-LETTER ?-PART CODE.	?	"XEPIT"	?	1941 - ?	1942 PERS Z S	READ. 100% COMPROMISED.	D 16	(ASA STATES THIS SYSTEM MAY BE A PART OF MXA OR MXB)	--
MEXICO 6	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION CIPHER WITH 26 ALPHABETS, 5 OF WHICH WERE USED AT A TIME. KEY LASTED SEVERAL DAYS. STARTING IN 1927, KEY CHANGED WITH EACH MESSAGE. SEPARATE SUBSTITUTION ALPHABETS FOR ENCIPHERMENT OF INDICATOR GROUP.	?	?	?	1926 - ?	1926 PERS Z S	READ	D 16	(UNKNOWN)	--
MEXICO 7	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION CIPHER WITH 20 ALPHABETS.	?	?	(MXC)	(?-CURRENT)	1942 PERS Z S 1942 SIM	READ BY SIM.	D 16 IF 1517	(100% READABLE)	--
NETHERLANDS 1	DIPLOMATIC, MILITARY, AND NAVAL ATTACHES	4-LETTER 4-FIGURE 1-PART CODE. (USED WITH AND WITHOUT ENCIPHERMENT. 220 GROUP REPEATING ADDITIVE USED IN ENCIPHERMENT.)	?	?	(NEB) AND (NEB-1)	1939, PERHAPS EARLIER-(CURRENT)	1939 PERS Z S	PARTIALLY BROKEN	D 54, REPORT 3, P 6 T 2490 T 2491 T 2493 T 2495	(CODE BROKEN. ENCIPHERMENT IN READABLE STATE.)	--
NETHERLANDS 2	?	FRENCH FIGURE CODE, 1-PART REPAGINATED. ENCIPHERMENT BY DIGRAPHIC SUBSTITUTION AND TRANSPOSITION WITHIN THE GROUP.	?	?	?	?-1939-?	1939 PERS Z S	PARTIALLY RECOVERED	D 54, REPORT 3, P 7 T 2045 T 2047 T 2048	(UNKNOWN)	--
NETHERLANDS 3	?	MESSAGES TO AND FROM THE ROME LEGATION.	?	?	?	? - ?	? SIM	A SMALL NUMBER OF MESSAGES READ	IF 1518 P 3	(UNIDENTIFIED)	--
NORWAY 1	DIPLOMATIC	5-LETTER ?-PART UNENCIPHERED CODE.	?	?	?	? - 1940?	BEFORE 1940 FA	READ COMPLETELY TO 1940. NOT AFTER 1940.	I 162 P 3	(UNIDENTIFIED)	--

~~TOP SECRET~~

~~TOP SECRET~~

CHART NO. 1-2

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
PERU 1	DIPLOMATIC	5-LETTER 1-PART CODE. INTIAL DIGRAPHS SUBSTITUTED BY DIGRAPHIC TABLES AND FINAL TRIGRAPH SUBSTITUTED BY TRIGRAPHIC TABLES.	?	?	(PEA)	(1924-CURRENT)	? PERS Z S ? SIM	?	T 1588 D 15	(COMPROMISED)	--
PERU 2	DIPLOMATIC	5-LETTER 2-PART CODE WITH 10,000 TO 20,000 PRONOUNCEABLE GROUPS.	?	?	?	1920-1927-?	? PERS Z S	NOT READ	D 16	(UNKNOWN)	--
PERU 3	DIPLOMATIC	5-LETTER 2-PART CODE. (ENCIPHERMENT MAYBE "PEA" OR PREDECESSOR.)	?	"PERU: LIMA-GENF"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1391	-	--
PERU 4	DIPLOMATIC	5-LETTER 2-PART CODE. (ENCIPHERMENT MAY BE "PEA" OR PREDECESSOR.)	?	"PERU: LIMA-GENF"	?	? - ?	? ?	RECOVERED LESS THAN 5%	T 1397	-	--

TOP SECRET

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
POLAND 1	NAVY	5-FIGURE 1-PART CODE	SZYFR ZASADNICZY "MAR 2"	?	?	(1924-1926)	1939 OKW	1ØØ% COMPROMISED	T 477	(UNKNOWN)	NOTE ACCOMPANYING THIS DOCUMENT SAYS THERE WERE THREE CODEBOOKS IN ALL.
POLAND 2	NAVY	5-FIGURE 1-PART CODE	SZYFR ZASADNICZY "MAR 3"	?	?	(1924-1926)	1939 OKW	1ØØ% COMPROMISED	T 478	(UNKNOWN)	NOTE ACCOMPANYING THIS DOCUMENT SAYS THERE WERE 3 CODES IN ALL.
POLAND 3	NAVY	1-PART CODE, PERHAPS 5-FIGURE.	SZYFR "1937"	?	?	? - ?	? OKM	1ØØ% COMPROMISED	T 476	(UNIDENTIFIED)	--
POLAND 4	DIPLOMATIC	4-FIGURE (2-PART) CODE ENCIPHERED BY ADDITIVE.	?	PD 1?	(FLD)	? - 1944 - ?	194Ø FA 1944 OKW 1941 PERS Z S	FA READ UNTIL 1943; OKW READ REGULARLY.	I 124 P 3 I 162 P 4 T 2Ø38	(NO GROUPS RECOVERED. 1942-1943, 4Ø% OF LONDON-NEW YORK TRAFFIC DECIPHERED. 1943-1944, VERY LITTLE DECIPHERED)	--
POLAND 5	DIPLOMATIC	4-FIGURE ?-PART CODE	?	N P D	?	? - ?	? - ?	RECOVERED ABOUT 4Ø%	T 2155	(UNIDENTIFIED)	--
POLAND 6	DIPLOMATIC	4-FIGURE ?-PART CODE	?	O F D	?	? - ?	? - ?	RECOVERED 3Ø% - 4Ø%	T 2152	(UNIDENTIFIED)	--
POLAND 7	DIPLOMATIC	4-FIGURE 2-PART CODE	?	P P D 5	?	? - ?	? - ?	RECOVERED 4Ø% - 5Ø%	T 215Ø T 2154	(UNIDENTIFIED)	--
POLAND 8	DIPLOMATIC	4-FIGURE 2-PART CODE	?	C P D	?	? - ?	? - ?	RECOVERED ABOUT 4Ø%	T 2137 T 2151 T 2176	(UNIDENTIFIED)	--
POLAND 9	DIPLOMATIC	4-FIGURE ?-PART CODE WITH 1Ø,ØØØ GROUPS. ENCIPHERED WITH ADDITIVE TABLE 24 X 26.	?	?	?	? - 1943	? OKW	MOST OF TRAFFIC READ	I 31 PP 2Ø - 21	(UNIDENTIFIED)	--
POLAND 1Ø	DIPLOMATIC	4-FIGURE ?-PART CODE WITH 1Ø,ØØØ GROUPS. ENCIPHERED WITH ADDITIVE TABLES 8Ø X 1ØØ.	?	?	?	1943 - ?	? OKW	MOST OF TRAFFIC READ	I 31 PP 2Ø - 21	(UNIDENTIFIED)	--
POLAND 11	DIPLOMATIC	4-FIGURE ?-PART CODE, VALUES IN FRENCH.	?	FRANZ. CODE DER POLN. DIPLOMATIE?	?	? - ?	? - ?	RECOVERED ABOUT 1Ø%	T 2144	(UNIDENTIFIED)	--
POLAND 12	?	4-FIGURE 2-PART CODE	?	?	?	? - ?	? - ?	RECOVERED ABOUT 25%	T 2153	(UNIDENTIFIED)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
POLAND	13	FOREIGN OFFICE	4-FIGURE 2-PART CODE. ENCIPHERED ON KEY TAKEN FROM BOOK. PAIR OF ENCIPHERMENT TABLES USED FOR EACH OUTSTATION. INDICATORS: TWO 5-FIGURE GROUPS AT BEGINNING OF MESSAGE.	?	FD 1	?	1934-1942	1939 PERS Z S 1939 FA? ? OKH	1941-1942 ALL MESSAGES READ, MOST OF THEM CURRENTLY	I 63 PP 2-4 I 111 P 2 D 3N, ITEM 1, P 5 T 2Ø33	(UNIDENTIFIED)	--
POLAND	14	MILITARY ATTACHE	4-FIGURE (2-PART) CODE ENCIPHERED BY ADDITIVE.	?	?	(PLF)	? - 1942 - ?	1945 OKW	READ	I 118 PP 8-9	(ABOUT 6Ø GROUPS RECOVERED. 1942-1943, 6Ø% OF WASHINGTON-LONDON TRAFFIC DECIPHERED. 1943-1944, 1Ø% OF WASHINGTON-LONDON TRAFFIC DECIPHERED.)	--
POLAND	15	?	3-FIGURE ?-PART CODE	?	POLNISCHER DREISTELLER-CODE I	?	? - ?	? - ?	RECOVERED ABOUT 9Ø%	T 2148	(UNIDENTIFIED)	--
POLAND	16	?	3-FIGURE ?-PART CODE	?	POLNISCHER DREISTELLER-CODE II	?	? - ?	? - ?	RECOVERED ABOUT 9Ø%	T 2148	(UNIDENTIFIED)	--
POLAND	17	?	3-FIGURE ?-PART CODE	?	?	?	? - ?	? - ?	RECOVERED ABOUT 9Ø%	T 2148	(UNIDENTIFIED)	--
POLAND	18	AIR FORCE	2-PART CODE, 2,ØØØ VALUES. ENCIPHERED.	?	?	?	? - ?	? OKL	1ØØ% COMPROMISED	I 121 P 6 P 7	(UNIDENTIFIED)	--
POLAND	19	NATIONAL RESISTANCE MOVEMENT	TRANSPOSITION-SUBSTITUTION CIPHER: CLEAR TEXT WRITTEN INTO 1Ø X 12 SQUARE, TAKEN OUT IN COLUMNS IN ORDER, CONVERTED TO FIGURES BY 2-FIGURE SUBSTITUTION. TRANSMITTED IN 3-FIGURE GROUPS.	?	Ø66	?	? - ?	? OKH,	READ	I 26 P 6 P 14	(UNIDENTIFIED)	--
POLAND	2Ø	NATIONAL RESISTANCE MOVEMENT	TRANSPOSITION-SUBSTITUTION CIPHER.	?	Ø9Ø	?	? - ?	? OKH,	READ	I 25 PP 14-15	(UNIDENTIFIED)	--
POLAND	21	NATIONAL RESISTANCE MOVEMENT	TRANSPOSITION-SUBSTITUTION CIPHER.	?	117	?	? - ?	? OKH,	READ	I 26 P 6 PP 14-15	(UNIDENTIFIED)	--
POLAND	22	NATIONAL RESISTANCE MOVEMENT	TRANSPOSITION-SUBSTITUTION CIPHER	?	118	?	? - ?	? OKH,	READ	I 26 P 6 PP 14-15	(UNIDENTIFIED)	--
POLAND	23	NATIONAL RESISTANCE MOVEMENT	TRANSPOSITION-SUBSTITUTION CIPHER.	?	181	?	? - ?	? OKH	READ	I 26 P 6 PP 14-15	(UNIDENTIFIED)	--
POLAND	24	NATIONAL RESISTANCE MOVEMENT	SIMPLE TRANSPOSITION CIPHER.	?	?	?	? - 1944 - ?	1944 OKH	BROKEN	I 26 P 14	(UNIDENTIFIED)	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
PORTUGAL 1	DIPLOMATIC	5-FIGURE 1-PART CODE WITH 5Ø,ØØØ GROUPS. ENCIPHERED DIFFERENTLY ON DIFFERENT CIRCUITS: ADDITIVE FOR CIRCUIT APPLIED TO LINE NUMBER; TRANSPOSITION OF GROUP ELEMENTS; 1,ØØØ-PLACE SUBSTITUTION TABLES APPLIED TO PAGE NUMBERS.	?	?	(POC?) (POD?) (POE?)	(POC: 1941-CURRENT) (POD: 1939-CURRENT) (POE: ?-1945)	1941 PERS Z S	?	D 16, 1941 REPORT, P 2	(POC, POD, POE ALL 1ØØ% COMPROMISED; ALL HAVE THE SAME BASIC BOOK.)	--
PORTUGAL 2	DIPLOMATIC	5-FIGURE 1-PART CODE, WITH 61,5ØØ GROUPS. ENCIPHERED.	?	328	(POJ)	(1941-CURRENT)	1942 PERS Z S	READ	D 16, 1942 REPORT, P 3 T 3Ø2Ø T 3Ø24 T 3Ø22	(1ØØ% COMPROMISED)	--
PORTUGAL 3	DIPLOMATIC	5-FIGURE 1-PART CODE WITH 5Ø,ØØØ GROUPS. ENCIPHERED WITH 1,ØØØ-PLACE SUBSTITUTION TABLES.	?	3Ø2	(POL)	(1942-CURRENT)	1942 PERS Z S	READ	D 16, 1942 REPORT, P 3	(1ØØ% COMPROMISED)	--
PORTUGAL 4	DIPLOMATIC	5-FIGURE 1-PART CODE (WITH 5Ø,ØØØ GROUPS. ENCIPHERED WITH TABLES.)	?	352	(POU)	(1943-CURRENT)	? ?	LARGELY RECOVERED	T 3Ø22	(9Ø% RECOVERED; COMPLETELY READABLE.)	--
PORTUGAL 5	DIPLOMATIC	5-FIGURE 1-PART CODE, 61,5ØØ GROUPS. ENCIPHERED.	?	299	?	?-1942-?	1942 PERS Z S	READ	D 16, 1942 REPORT, P 3	(UNIDENTIFIED)	--
PORTUGAL 6	DIPLOMATIC	5-FIGURE 1-PART CODE: BASIC BOOK OF WHICH "299" AND "328" WERE REPAGINATIONS. 24 SUBSTITUTION TABLES USED WITH IT.	?	2Ø5	?	?-1942-?	1942 OKW 1942 PERS Z S	1ØØ% COMPROMISED; LOANED BY OKW TO PERS Z S FOR PHOTOSTATING INCLUDING 9 TABLES; REST OF TABLES BROKEN. READ 1ØØ%.	D 16, 1942 REPORT, P 3	(REPAGINATION "328" IS ASA'S POJ.)	--
PORTUGAL 7	DIPLOMATIC	5-FIGURE 1-PART CODE WITH 61,5ØØ GROUPS. ENCIPHERED WITH TWENTY 1ØØ-PLACE SUBSTITUTION TABLES FOR LINE NUMBERS AND ON SOME CIRCUITS ALSO WITH 1,ØØØ-PLACE TABLE FOR PAGES. DIFFERENT TRANSPOSITION OF GROUP ELEMENTS FOR EACH CIRCUIT.	?	?	?	?-1941-?	1941 PERS Z S	LARGE PART OF MESSAGES READ WITH SOME GAPS. BERLIN-LISBON TRAFFIC NOT READ; TRAFFIC SMALL AND KEYS CHANGED RAPIDLY.	D 16, 1941 REPORT, P 2	(UNIDENTIFIED)	--
PORTUGAL 8	DIPLOMATIC	5-FIGURE 1-PART CODE WITH 61,9ØØ GROUPS. ENCIPHERED WITH TWENTY 1ØØ-PLACE SUBSTITUTION TABLES FOR LINE NUMBERS AND ON SOME CIRCUITS ALSO WITH 1,ØØØ-PLACE TABLE FOR PAGES. DIFFERENT TRANSPOSITION OF GROUP ELEMENTS FOR EACH CIRCUIT.	?	?	?	?-1941-?	1941 PERS Z S	ENCIPHERMENTS BROKEN, BEGINNINGS MADE ON CODE, BUT NOT READ.	D 16, 1941 REPORT, P 2	(UNIDENTIFIED)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM.	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
PORTUGAL 9	?	5-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 3127	(UNIDENTIFIED)	--
PORTUGAL 1Ø	?	5-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 1Ø%	T 3Ø23	(UNIDENTIFIED)	--
PORTUGAL 11	DIPLOMATIC	4-FIGURE 1-PART CODE, REPAGINATED.	?	62 146	?	?-1936-?	? ?	RECOVERED 3Ø%	T 1336	(UNIDENTIFIED)	--
PORTUGAL 12	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	?	?	? - ?	? ?	RECOVERED 3Ø% - 5Ø%	T 1332	(UNIDENTIFIED)	--
PORTUGAL 13	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	5Ø2	?	? - ?	? ?	RECOVERED 2Ø% - 3Ø%	T 1333	(UNIDENTIFIED)	--
PORTUGAL 14	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	611	?	? - ?	? ?	RECOVERED 2Ø% - 3Ø%	T 1334	(UNIDENTIFIED)	--
PORTUGAL 15	?	4-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 5%	T 1335	(UNIDENTIFIED)	--
PORTUGAL 16	?	4-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1337	(UNIDENTIFIED)	--
PORTUGAL 17	?	4-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 5%	T 1338	(UNIDENTIFIED)	--
PORTUGAL 18	?	4-FIGURE ?-PART CODE.	?	557 93	?	? - ?	? ?	RECOVERED LESS THAN 3%	T 134Ø	(UNIDENTIFIED)	--
PORTUGAL 19	DIPLOMATIC	4-FIGURE ?-PART CODE.	?	55 141	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1386	(UNIDENTIFIED)	--
PORTUGAL 2Ø	DIPLOMATIC	MONOALPHABETIC SUBSTITUTION CIPHER.	?	?	?	?-1942-?	1942 PERS Z S	READ	D 16, 1942 REPORT, P 3	(UNKNOWN)	--
PORTUGAL 21	DIPLOMATIC	5-LETTER ?-PART CODE.	?	?	?	?-1937-?	? SIM	READ. COMPROMISED.	T 159Ø	(UNIDENTIFIED)	---
PORTUGAL 22	DIPLOMATIC	5-LETTER 5-FIGURE CODE, 6Ø,ØØØ GROUPS. ENCIPHERED BY ESTIMATED 2ØØ TABLES.	?	?	?	? - ?	? SIM, SID	READ	IF 1526	(UNIDENTIFIED)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
PORTUGAL	23	DIPLOMATIC	5-FIGURE 1-PART CODE. LINE DIGRAPHS ON PAGE IN EITHER ASCENDING OR DESCENDING ORDER. USED LISBON-ANKARA-BERN.	?	?	?	? - 1945	1945 SID	READ	IF 1517 IF 1526	(UNIDENTIFIED)	--
PORTUGAL	24	DIPLOMATIC	5-FIGURE AND 2-FIGURE ?-PART CODE REPAGINATED FOR DIFFERENT LINKS. UNENCIPHERED. TRAFFIC GENERALLY OF MARITIME NATURE.	?	?	?	?-1944-?	? SID	READ	IF 1526	(UNIDENTIFIED)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUMANIA 1	DIPLOMATIC	5-FIGURE 2-PART CODE (ENCIPHERED WITH MONO-ALPHABET)	?	R 18	(ROD)	(?-1945-?)	? - ?	100% COMPROMISED	T 752 T 1097 T 1098 T 1095	(WORKED ON INTERMITTENTLY DURING 1942, 1943, 1944, AND 1945. ENCIPHERMENT STILL BEING ATTACKED, END 1945.)	--
RUMANIA 2	DIPLOMATIC	5-FIGURE 2-PART CODE (ENCIPHERED WITH BOOK ADDITIVE)	?	?	(ROF)	(?-1945-?)	? - ?	100% COMPROMISED	T 751	(WORKED ON INTERMITTENTLY DURING 1942, 1943, 1944, AND 1945. ADDITIVES STILL BEING ATTACKED, END 1945.)	--
RUMANIA 3	DIPLOMATIC	5-FIGURE 2-PART CODE (ENCIPHERED WITH REPEATING ADDITIVE)	?	?	(ROH)	(?-1945-?)	? - ?	100% COMPROMISED	T 746	(WORKED ON INTERMITTENTLY DURING 1942, 1943, 1944, AND 1945. ADDITIVES STILL BEING ATTACKED, END 1945.)	--
RUMANIA 4	DIPLOMATIC	5-FIGURE 2-PART CODE, 70,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	?	R 11	?	? - ?	? PERS Z S	RECOVERED 5% - 10%	T 2220 D 54 P 15	(UNIDENTIFIED)	--
RUMANIA 5	DIPLOMATIC	5-FIGURE 2-PART CODE, 70,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	?	R 12	?	? - ?	? PERS Z S	RECOVERED 5% - 10%	T 2221 D 54 P 15	(UNIDENTIFIED)	--
RUMANIA 6	DIPLOMATIC	5-FIGURE 2-PART CODE, 70,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	?	R 13	?	? - ?	? PERS Z S	RECOVERED ABOUT 5%	T 2216 T 2222 D 54 P 15	(UNIDENTIFIED)	--
RUMANIA 7	DIPLOMATIC	5-FIGURE 2-PART CODE, 100,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	?	14	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 2219 D 54 P 15	(UNIDENTIFIED)	--
RUMANIA 8	DIPLOMATIC	5-FIGURE 2-PART CODE, 100,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	CIFRU GRIGORCEA	15	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 1095 D 54 P 15	(UNIDENTIFIED)	--
RUMANIA 9	DIPLOMATIC	5-FIGURE 2-PART CODE, 100,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	?	R 16	?	? - ?	? PERS Z S	RECOVERED 5% - 10%	T 2217 T 2225 D 54 P 15	(UNIDENTIFIED)	--
RUMANIA 10	DIPLOMATIC	5-FIGURE 2-PART CODE, 100,000 GROUPS. ENCIPHERED WITH 10-PLACE TABLE.	?	17	?	1940 - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 2224 D 54 P 15	(UNIDENTIFIED)	--

RUMANIA 11	DIPLOMATIC	5-FIGURE ?-PART CODE WITH 50,000 - 60,000 GROUPS. ENCIPHERED BY FIGURE SUBSTITUTION TABLE.	?	?	?	? - ?	? SIM, SID	CODE 100% COMPROMISED; ENCIPHERMENT BROKEN.	IF 1517 P 8
									IF 1526 P 6
										(UNIDENTIFIED)	--

RUMANIA 12	?	5-FIGURE 2-PART CODE.	?	R 6	?	? - ?	? - ?	RECOVERED 5% - 10%	T 1006	(UNIDENTIFIED)	--
RUMANIA 13	?	5-FIGURE 2-PART CODE.	?	R 7	?	? - ?	? - ?	RECOVERED LESS THAN 5%	T 1007	(UNIDENTIFIED)	--
RUMANIA 14	?	5-FIGURE 2-PART CODE	?	R 8	?	? - ?	? - ?	RECOVERED 5% - 15%	T 2223	(UNIDENTIFIED)	--
RUMANIA 15	?	5-FIGURE 2-PART CODE.	?	9	?	? - ?	? - ?	RECOVERED 5% - 10%	T 2215	(UNIDENTIFIED)	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUMANIA 16	?	5-FIGURE 2-PART CODE	?	1Ø	?	? - ?	? ?	RECOVERED LESS THAN 5%	T 2218	(UNIDENTIFIED)	--
RUMANIA 17	?	5-FIGURE 2-PART CODE.	?	?	?	? - ?	? ?	RECOVERED ABOUT 1Ø%	T 1138	(UNIDENTIFIED)	--
RUMANIA 18	DIPLOMATIC	5-FIGURE ?-PART CODE. FIGURE SUBSTITUTION ENCIPHERMENT. SEVERAL BOOKS USED SIMULTANEOUSLY.	?	?	?	? - ?	? SIM	1ØØ% COMPROMISED.	IF 1521	(UNIDENTIFIED)	--
RUMANIA 19	DIPLOMATIC	5-FIGURE ?-PART CODE. 5Ø,ØØØ - 6Ø,ØØØ GROUPS. ENCIPHERED WHEN HIGH SECURITY WAS DESIRED. KEYS WERE 49 X 5 AND 58 X 5 LONG.	?	?	?	? - ?	? SIM, SID	1ØØ% COMPROMISED.	IF 1526	(UNIDENTIFIED)	--
RUMANIA 2Ø	MILITARY ATTACHE	5-FIGURE 2-PART CODE. EACH PAGE NUMBERED BY ONE OF FOUR 3-FIGURE GROUPS PRINTED AT TOP. PAGE DIVIDED INTO TWO PARTS, EACH PART CONTAINING 5 BLOCKS OF 1Ø GROUPS EACH. ENCIPHERED WITH A SYSTEM CALLED BY ROMANIANS "FISE."	?	?	?	1942-1943	? SIM	READ	IF 1521	(UNIDENTIFIED)	--

RUMANIA 21	MILITARY ATTACHE	TRANSPOSITION CIPHER. RECTANGLE DIVIDED INTO 4 SMALLER ONES, EACH 7 X 1Ø OR 7 X 7. SOME BLANK CELLS. CLEAR TEXT WRITTEN IN ON A PATTERN.	AMG 1943	?	?	?-1943-?	? SIM	READ	IF 1521
									IF 1515
									T 1596
										(UNIDENTIFIED)	--

RUMANIA 22	MILITARY ATTACHE	TRANSPOSITION CIPHER. 6 RECTANGLES, 6 X 5; CLEAR TEXT WRITTEN IN ON PATTERN.	CIFRUL DE MEMORIE	?	?	?-1943-?	1943 SIM
							? SID
								READ	IF 1517
									IF 1521
										(UNIDENTIFIED)	--

RUMANIA 23	AIR FORCE	TRANSPOSITION CIPHER.	?	?	?	?-1939-?	? OKL	NOT READ	I 121 P 8	(UNKNOWN)	--
RUMANIA 24	POLICE	CIPHER, DESCRIBED AS "ELEMENTARY", BUT NO DETAILS AVAILABLE.	?	?	?	? - ?	? OKL	READ CURRENTLY	I 121 P 9	(UNKNOWN)	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA 1	ARMY	HAGELIN S-211 MACHINE, OLD STYLE, EMPLOYING FRANCTIONATION, SUBSTITUTION, AND RECOMBINATION.	K 37	K 37	--	? - ?	1941 OKH	ACCOMPLISHED THEORETICAL SOLUTION ON 1Ø-LETTER CRIB. AUTUMN 1941, MODEL OF MACHINE CAPTURED.	I 136 P 2 I 53 P 5 I 92 P 4	--	--
RUSSIA 2	ARMY	SPELCH ENCIPHERER, TIME SCRAMBLING TYPE.	?	X^2	--	1939-1945	1939 OKH/GDNA, WA PRUEF 7	NOT BROKEN.	I 73 I 31 P 12 IF 123 P 13	--	--
RUSSIA 3	ARMY	TELETYPE ENCIPHERER, KEY GENERATOR TYPE.	?	Z	--	? - ?	1943 OKH	NOT READ	I 31 P 12	--	--
RUSSIA 4	ARMY	5-FIGURE ?-PART CODE ENCIPHERED WITH ONE-TIME PAD.	?	?	--	? - 1945	? OKH	?	I 19 C I 116	--	--
RUSSIA 5	ARMY: BRIGADE, DIVISION STAFFS UPWARD TO GENERAL STAFF	5-FIGURE ?-PART CODE	Ø11-A	?	--	194Ø-1941?	? OKH	?	T 8Ø5	--	--
RUSSIA 6	ARMY: BRIGADE, DIVISION STAFFS UPWARD TO GENERAL STAFF	5-FIGURE ?-PART CODE	Ø23-A	?	--	194Ø?- ?	? OKH	?	T 8Ø5	--	--
RUSSIA 7	ARMY: BRIGADE, DIVISION STAFFS UPWARD TO GENERAL STAFF	5-FIGURE ?-PART CODE	Ø45-A	?	--	194Ø - ?	? OKH	?	T 8Ø5	--	--
RUSSIA 9	ARMY: BRIGADE, DIVISION STAFFS UPWARD TO GENERAL STAFF	5-FIGURE ?-PART CODE	Ø62-A	?	--	194Ø - ?	? OKH	?	T 8Ø5	--	--
RUSSIA 9	ARMY: BRIGADE, DIVISION STAFFS UPWARD TO GENERAL STAFF	5-FIGURE ?-PART CODE	Ø91-A	?	--	? - 1945	? OKH	?	T 8Ø5	--	--
RUSSIA 1Ø	ARMY: TANK	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	PT-B	?	--	? - 1945	? OKH	1ØØ% COMPROMISED, MARCH 1945	I 19 C I 19 E	--	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA 11	ARMY: GUARDS TANK	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	? - 1945	? OKH	?	I 19 C I 19 E	--	--
RUSSIA 12	ARMY: TANK	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	? - 1945	? OKH	?	I 19 C I 19 E	--	--
RUSSIA 13	ARMY: GUARDS TANK	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	? - 1945	? OKH	?	I 19 C I 19 E	--	--
RUSSIA 14	ARMY	4-FIGURE ?-PART CODE	?	?	--	? - 1945	? OKH	PARTLY READ	I 19 C I 19 E	--	--
RUSSIA 15	ARMY	4-FIGURE ?-PART CODE	?	?	--	1941-1945?	? OKH	?	I 26	--	--
RUSSIA 16	ARMY	4-FIGURE ?-PART CODE	?	?	--	1945 - ?	? OKH	?	I 19 C I 19 E	--	--
RUSSIA 17	ARMY	3-FIGURE ?-PART CODE	?	?	--	1941-1945	? OKH	?	I 19 C I 26	--	--
RUSSIA 18	ARMY	2-FIGURE SUBSTITUTION CIPHER USING A 1Ø X 1Ø SQUARE CONTAINING ALPHABET, FIGURES, ETC. DAILY CHANGING KEY.	?	?	--	194Ø-1943	? SIM	?	IF 1517	--	--
RUSSIA 19	ARMY	2-FIGURE SUBSTITUTION CIPHER	PT 41	?	--	1941-1945	? OKH	?	I 26 T 9Ø5	--	--
RUSSIA 2Ø	ARMY	2-FIGURE SUBSTITUTION CIPHER	PT 41 N	?	--	1941-1945?	? OKH	?	I 26	--	--
RUSSIA 21	ARMY GROUPS, ARMIES, CORPS	2-FIGURE SUBSTITUTION CIPHER	PT 42	?	--	1942 - ?	? OKH	?	I 19 C I 19 D	--	--
RUSSIA 22	ARMY	TRANSPOSITION CIPHER USING REVOLVING GRILLE	?	?	--	1944 - ?	? OKH	?	I 19 C	--	--
RUSSIA 23	ARMY	TRANSPOSITION CIPHER	?	?	--	1944 - ?	? OKH	?	I 19 C	--	--
RUSSIA 24	ARMY, AIR FORCE	4-FIGURE ?-PART CODE	OKK 5-8	?	--	1939-1941?	? OKH	?	I 116 T 9Ø5	--	--
RUSSIA 25	ARMY, AIR FORCE	2-FIGURE SUBSTITUTION CIPHER	PT 35	?	--	1935-1939	? OKH	?	T 9Ø5	--	--

CHART NO. 1-2

TOP SECRET

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA	26	ARMY GROUPS, ARMIES, CORPS, DIVISIONS, AIR FORCE	2-FIGURE SUBSTITUTION CIPHER	PT 39	?	--	1939-1942	? OKH	?	I 19 C I 19 D I 26 T 8Ø5	--	--
RUSSIA	27	ARMY: DIVISIONS, REGIMENTS. AIR FORCE	2-FIGURE SUBSTITUTION CIPHER	PT 42 N	R 27 C 731	--	1942-1944	? OKH	?	I 19 C I 19 D T 3349	--	--
RUSSIA	28	AIR FORCE	4-FIGURE ?-PART CODE	VAK 38	?	--	1938 - ?	? OKH	?	T 8Ø5 I 116	--	--
RUSSIA	29	AIR FORCE	4-FIGURE ?-PART CODE	?	?	--	1944-1945	? OKH	?	I 19 C I 19 E	--	--
RUSSIA	3Ø	AIR, CIVILIAN	3-FIGURE ?-PART CODE, UNENCIPHERED	?	?	--	1943-1944	? OKH	READ	I 116	--	--
RUSSIA	31	AIR FORCE	2-FIGURE SUBSTITUTION CIPHER	PT 43	?	--	? - 1945	? OKH	NOT BROKEN	I 19 C I 1Ø6	--	--
RUSSIA	32	NKVD*	5-FIGURE 1-PART CODE	?	N5/529/S R 52 C 156Ø	--	? - 1945	? OKH	?	I 55 T 2534	--	--
RUSSIA	33	NKVD	5-FIGURE ?-PART CODE ENCIPHERED WITH ONE-TIME PAD ADDITIVE.	?	CH ?	--	1944 - ?	? OKM	?	T 5Ø4	--	--
RUSSIA	34	NKVD	5-FIGURE ?-PART CODE ENCIPHERED WITH ONE-TIME PAD ADDITIVE	?	?	--	1944 - ?	? OKM	?	T 542 T 5Ø4	--	--
RUSSIA	35	NKVD	5-FIGURE ?-PART CODE ENCIPHERED BY DIGRAPHIC SUBSTITUTION.	?	?	--	? - 1945	? OKH	?	I 26 I 116 T 8Ø5	--	--
RUSSIA	36	NKVD, DIVISION OF REGIMENT TO DIVISION OF BATTALION SIZE	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE	WHITE SEA	?	--	1943-1944	1944 OKH	1Ø% OF TRAFFIC READ	I 1Ø6	--	--
RUSSIA	37	NKVD	4-FIGURE 2-PART CODE	Ø49	R 47 11Ø2	--	? - 1944	? OKH	?	I 55 I 1Ø6 T 2577	--	--
		*PEOPLE'S COMMISSARIAT FOR INTERNAL AFFAIRS										

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U. S. A.						
RUSSIA	38	NKVD*--REGIMENTS, BATTALIONS	4-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION. SUBSTITUTION.	ZERNO	R 47 1800	--	1943-1945	? OKH	?	I 19 C I 17; I 106 I 55; T [illegible]	--	--
RUSSIA	39	NKVD	4-FIGURE 1-PART CODE	?	?	--	1941?-1945	? OKH	?	I 26	--	--
RUSSIA	40	NKVD	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	?	--	1939 - ?	? OKH	?	T 8Ø5	--	--
RUSSIA	41	NKVD	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	?	--	1941?-1945	? OKH	?	I 26	--	--
RUSSIA	42	NKVD	4-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	VIZA	?	--	? - 1945	? OKH	?	T 5Ø5	--	--
RUSSIA	43	NKVD	4-FIGURE 2-PART CODE ENCIPHERED BY DIGRAPHIC SUBSTITUTION.	NIVA	?	--	? - 1945	? OKH	?	I 116 T 8Ø5	--	--
RUSSIA	44	NKVD	4-FIGURE 2-PART CODE	?	R 42 16ØØ	--	? - ?	? OKH	?	I 1Ø6	--	--
RUSSIA	45	NAVY	5-FIGURE 2-PART CODE ENCIPHERED WITH ONE-TIME PAD ADDITIVE.	?	KLAGENFURT I, II	--	1941-1942	? OKM	NOT SOLVED	T 564 T 541	--	--
RUSSIA	46	NAVY	5-FIGURE 2-PART CODE ENCIPHERED WITH DOUBLE ADDITIVE.	?	KOENIGSBERG	--	1942-1943	? OKM	NOT SOLVED	T 564	--	--
RUSSIA	47	NAVY	5-FIGURE 2-PART CODE ENCIPHERED WITH PERMUTED ADDITIVE.	?	FASAN	--	? - ?	? OKM	?	I 4Ø	--	--
RUSSIA	48	NAVY	5-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	KOMMANDEUR	--	1936-1941	? OKM	NOT SOLVED	I 16 T 564	--	--
RUSSIA	49	NAVY	5-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	TROMSOE	--	1942-1943?	? OKM	NOT SOLVED	I 4Ø T 564	--	--
RUSSIA	50	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	GAMVIK	--	1943-1944	? OKM	NOT SOLVED	T 542 T 564 D 39	--	--
RUSSIA	51	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	GRAZ	--	? - ?	? OKM	READ AT TIMES	T 564 I 4Ø	--	--
RUSSIA	52	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	M 4/374/S NAMSOS	--	1942?-1943	? OKM	AT TIMES ABOUT 5Ø% READABLE	I 4Ø T 542; T 561 T 562; T 564	--	--

*PEOPLE'S COMMISSARIAT FOR INTERNAL AFFAIRS

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA 53	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	?	--	1941-1942?	? OKM	50% READABLE	I 16 T 564	--	--
RUSSIA 54	NAVY	4-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION TO MARCH 1941, WITH ADDITIVE THEREAFTER.	?	R 42 C KKF	--	1939-1941?	? OKM	VARIED AT DIFFERENT TIMES	T 564 I 16 I 40	--	--
RUSSIA 55	NAVY	4-FIGURE 1-PART CODE ENCIPHERED WITH ADDITIVE.	?	M 5/4/493/S ELBING	--	1943-1945	? OKM	NOT SOLVED	I 40 T 542 T 564 D 39	--	--
RUSSIA 56	NAVY	4-FIGURE 1-PART CODE ENCIPHERED WITH ADDITIVE.	?	NARVIK	--	1942-1943	? OKM	AT TIMES ABOUT 50% READABLE	I 40 T 542; T 562 T 564	--	--
RUSSIA 57	NAVY	4-FIGURE 1-PART CODE ENCIPHERED WITH ADDITIVE.	?	WIEN	--	? - ?	? OKM	READ AT TIMES	I 40 T 564 T 1032	--	--

RUSSIA 58	NAVY: SIGNAL STATIONS	4-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	DF 9
			DF 26
				M 4/490/S ALLENSTEIN I;
				M 4/559/S ALLENSTEIN II;
				M 4/635/S ALLENSTEIN III
					--	1943-1945	? OKM	SOLVED	T 542
									T 564
										--	--

RUSSIA 59	NAVY	4-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	?	HARSTAD	--	1943 - ?	? OKM	?	T 562	--	--
RUSSIA 60	NAVY	4-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	?	OSLO	--	1942-1944	? OKM	READ ALMOST 100% AT TIMES	I 40; I 55 T 542; T 562 T 564; T 253	--	--
RUSSIA 61	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	BERGEN	--	1943-1943	? OKM	NOT SOLVED	T 562; T 564	--	--
RUSSIA 62	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	GASTEIN	--	1943-1944	? OKM	NOT SOLVED	T 564	--	--
RUSSIA 63	NAVY	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE.	?	RIGA SUBSTITUTE	--	1942 - ?	? OKM	NOT SOLVED	T 564	--	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA	64	NAVY	5-FIGURE ?-PART CODE ENCIPHERED WITH ADDITIVE.	?	THORN	--	1943-1943	? OKM	READ CURRENTLY PART OF TIME	T 564	--	--
RUSSIA	65	NAVY	5-FIGURE ?-PART CODE ENCIPHERED WITH ADDITIVE.	?	TILSIT	--	? - 1942	? OKM	NOT READ	T 564	--	--
RUSSIA	66	NAVY	4-FIGURE ?-PART CODE ENCIPHERED WITH ADDITIVE.	?	M 5-4561 S	--	1944 - ?	? OKM	NOT SOLVED	T 542 T 564	--	--
RUSSIA	67	NAVY	4-FIGURE ?-PART CODE ENCIPHERED WITH ADDITIVE.	?	?	--	1944 - ?	? OKM	NOT SOLVED	T 564; T 542 D 39	--	--
RUSSIA	68	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	ALTA	--	1943 - ?	? OKM	PARTLY READ	T 562	--	--
RUSSIA	69	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	GOLDAP	--	1944 - ?	? OKM	?	T 564	--	--
RUSSIA	70	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	GRAUDENZ	--	1943-1945	? OKM	READ TO DIFFERENT EXTENTS AT VARIOUS TIMES.	I 16; I 40 T 542; T 545 T 564 D 39	--	--
RUSSIA	71	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	KYBERG	--	1943 - ?	? OKM	?	T 562 I 40	--	--
RUSSIA	72	NAVY	4-FIGURE ?-PART, CODE ENCIPHERED BY SUBSTITUTION.	?	SPITTAL	--	1944 ONLY	? OKM	READ	T 564	--	--
RUSSIA	73	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 4/485/S TANNENBERG	--	1945 - ?	? OKM	?	T 564; T 542	--	--
RUSSIA	74	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	VILLACH	--	1942 - ?	1942 OKM	READ	T 564 I 45	--	--
RUSSIA	75	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	WERA	--	1943 - ?	? OKM	?	T 564	--	--
RUSSIA	76	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	WINDAU	--	JAN 1945 - ?	? OKM	?	I 40 D 39 T 563 T 564	--	--

TOP SECRET

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS

AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA 77	NAVY	4-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 4/542/S M 4/590/S	--	1943-1944	? OKM	SOLVED	T 542; T 564	--	--
RUSSIA 78	NAVY	4-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 4/544/S	--	1943-1944	? OKM	NOT SOLVED	T 564; T 542	--	--
RUSSIA 79	NAVY	2-FIGURE 3-FIGURE 4-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	?	DRONTHEIM	--	1942 - ?	1942 OKM	SOLVED	T 564	--	--
RUSSIA 80	NAVY	3-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 3/333/S	--	1944 - ?	? OKM	?	T 542	--	--
RUSSIA 81	NAVY	3-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	T-10-1025	M 3/533/S	--	1943 - ?	? OKM	NOT SOLVED	T 542	--	--
RUSSIA 82	NAVY	3-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 3/533N/S	--	1943 - ?	? OKM	NOT SOLVED	T 542	--	--
RUSSIA 83	NAVY	3-FIGURE 2-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 3/612/S	--	1944 - ?	? OKM	ABOUT 70% READ	T 542	--	--
RUSSIA 84	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	PT 3	BODÖ	--	1943-1944?	? OKM	SOLVED	I 40 T 564; T 562 T 542; T 544	--	--
RUSSIA 85	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	?	LIBAU	--	1944-1945	? OKM	READ	I 40 D 39 T 563; T 564	--	--
RUSSIA 86	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	PT 13	NORDKAP	--	1943 - ?	? OKM	NORDKAP I PARTIALLY SOLVED; NORDKAP II NOT SOLVED.	T 561; T 562 T 564	--	--
RUSSIA 87	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY DIGRAPHIC SUBSTITUTION.	?	STOLF	--	1944 - ?	? OKM	?	I 40 T 564 D 39	--	--
RUSSIA 88	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	?	TAUPCOGEN	--	1944-1945	? OKM	?	T 564 I 40	--	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA	89	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	BTSVVS	M 3/519/S VARDŎ	--	1942-1943	? OKM	READ	I 16; I 40 T 542; T 562 T 564	--	--
RUSSIA	90	NAVY: ARTILLERY BATTERIES, GULF OF FINLAND	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION.	T-19-SN	M 3/500/S	--	1943 - ?	? OKM	PARTLY READ	T 542	--	--
RUSSIA	91	NAVY	3-FIGURE 1-PART CODE ENCIPHERED BY SUBSTITUTION OR BY SUBSTITUTION PLUS ADDITIVE.	?	M 3/490/S	--	APRIL-MAY 1943	? OKM	40% OF VALUES KNOWN	T 542	--	--
RUSSIA	92	NAVY	3-FIGURE 1-PART CODE ENCIPHERED WITH GENERATED ADDITIVE AND SUBSTITUTION.	?	M 3/502/S	--	1944 - ?	? OKM	NOT SOLVED	T 542	--	--
RUSSIA	93	NAVY	3-FIGURE 1-PART CODE, ENCIPHERED BY SUBSTITUTION TO 15 AUGUST 1942. BY ADDITIVE THEREAFTER.	?	MASUREN	--	1941-1943	1942 FINNS 1942 OKM	READ PRACTICALLY 100%	T 564 I 12; I 16	--	--
RUSSIA	94	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION AND ADDITIVE.	?	DANZIG	--	1942-1944	? OKM	NOT SOLVED	T 564	--	--
RUSSIA	95	NAVY	3-FIGURE ?-PART CODE ENCIPHERED WITH ADDITIVE.	?	LYBERG	--	1943 - ?	? OKM	?	T 564	--	--
RUSSIA	96	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	BUKET	--	MAY-DEC 1943	? OKM	?	T 564	--	--
RUSSIA	97	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	INSTERBURG	--	1942 - ?	? OKM	READ WHEN TRAFFIC WAS SUFFICIENT	T 564	--	--
RUSSIA	98	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	VUK MARBURG	--	1942-1943	1942 OKM	READ CURRENTLY PART OF TIME	T 564	--	--
RUSSIA	99	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	RIGA	--	6 JULY 1942- 25 JULY 1942	1942 OKM	READ CURRENTLY	T 564	--	--
RUSSIA	100	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	SALZBURG	--	1941-1942	1942 OKM	READ CURRENTLY PART OF TIME	T 564 I 40	--	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA 1Ø1	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	SEELAND	--	1943-1945	? OKM	?	I 4Ø; I 16 I 55	--	--
RUSSIA 1Ø2	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	PT 4	SSS	--	8 OCTOBER 1943 -16 OCTOBER 1943	? OKM	NOT SOLVED	T 562; T 564	--	--
RUSSIA 1Ø3	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	STAVANGER	--	1943 - ?	? OKM	?	T 562	--	--
RUSSIA 1Ø4	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 3/468/S	--	1942-1943	? OKM	READ	T 542	--	--
RUSSIA 1Ø5	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 3/519/S	--	1943 - ?	? OKM	?	T 542	--	--
RUSSIA 1Ø6	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	D.S. 17	M 3/524/S	--	AUGUST-NOVEMBER 1943	? OKM	NOT SOLVED	T 542	--	--
RUSSIA 1Ø7	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 3/563/S	--	1943-1944	? OKM	READ ALMOST 1ØØ%	T 542	--	--
RUSSIA 1Ø8	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	MARCH-JUNE 1941	? OKM	SOLVED	T 564	--	--
RUSSIA 1Ø9	NAVY: COASTAL AND RAILWAY BATTERIES ON GULF OF FINLAND	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	1942-1943	1942 OKM	READ	T 564	--	--
RUSSIA 11Ø	NAVY: BATTERIES OF 4Ø2 AND 435 DIVISIONS AND BRIGADE COMMUNICATIONS OFFICERS	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	1943 - ?	1943 OKM	SOLVED	T 564	--	--
RUSSIA 111	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	1944 - ?	? OKM	NOT READ	T 564	--	--
RUSSIA 112	NAVY	3-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	?	--	1944 - ?	? OKM	READ	T 564	--	--

TOP SECRET

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
RUSSIA 113	NAVY	3-FIGURE ?-PART CODE	?	FUVA	--	1941-1942	? OKM	NOT READ	T 564	--	--
RUSSIA 114	NAVY	2-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	TANA	--	1943 - ?	? OKM	?	T 562	--	--
RUSSIA 115	NAVY	2-FIGURE ?-PART CODE ENCIPHERED BY SUBSTITUTION.	?	M 2/249/S	--	NOV-DEC 1942	1942 OKM	SOLVED	T 564; T 542	--	--
RUSSIA 116	NAVY	?-PART CODE	?	M 5/5ØØ/S	--	1943 - ?	? OKM	?	T 542	--	--
RUSSIA 117	ARMY	2-FIGURE ?-PART FIELD CODE. MADE IN 1Ø X 1Ø SQUARES. DAILY CHANGING KEY.	?	?	--	? - ?	? SIM	READ	IF 1517	--	--
RUSSIA 118	?	?-PART CODE.	?	?	--	? - ?	? SIS	1ØØ% COMPROMISED.	IF 15Ø6	--	--
SAUDI ARABIA 1	DIPLOMATIC	?-PART CODE TRANSMITTED IN 5-FIGURE GROUPS.	?	?	?	?-1944-1945	? GERMANS	NOT SOLVED	T 43Ø	(UNKNOWN)	--
SAUDI ARABIA 2	DIPLOMATIC	SUBSTITUTION CIPHER--2 DIGITS PER LETTER. TRAFFIC WAS SMALL.	?	?	(ABD) OR (ABB)	(ABD: 1943-CURRENT) (ABB: ?-1945-CURRENT)	? SIM	READ	IF 1518 P 4	(ABD: BROKEN IN 1945. 1ØØ% READABLE. ABB: BROKEN IN 1944. 1ØØ% READABLE.)	--
SAUDI ARABIA 3	DIPLOMATIC	SUBSTITUTION CIPHER--2 DIGITS PER LETTER. SEE ITEM 2.	?	?	(ABD)	(?-1943-CURRENT)	1942 PERS Z S	READ	T 2Ø52	(BROKEN IN 1945. NOW 1ØØ% READABLE.)	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN	1	DIPLOMATIC	4-FIGURE 2-PART CODE, ENCIPHERED BY MEANS OF A 1ØØ-GROUP-LONG ENCIPHER KEY.	(CLAVE 1537 OR CLAVE 1539)	?	(SPA?) OR (SPE?)	(1938-CURRENT)	1939 SIM	BROKEN	IF 1517 IF 1518	(BOTH COMPROMISED)	--
SPAIN	2	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	SP. 234	?	? - ?	? PERS Z S	RECOVERED 5%	T 1358	(UNKNOWN)	--
SPAIN	3	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	SP. 1339	?	? - ?	? PERS Z S	RECOVERED 2Ø%-25%	T 1383 T 2534	(UNKNOWN)	--
SPAIN	4	DIPLOMATIC	4-FIGURE 2-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1361	(UNKNOWN)	--
SPAIN	5	DIPLOMATIC	4-FIGURE (1-PART CODE REPAGINATED.) 1Ø,ØØØ GROUPS. LAST TWO PLACES OF EACH GROUP ARE READ FIRST.	(Ø4)	"Ø4"	(SPB)	(1915-CURRENT)	1927, 1942 PERS Z S	RECOVERED 3Ø% - 4Ø%	T 1382 D 16, REPORT 2, P 3	(COMPROMISED. BEING READ.)	--
SPAIN	6	DIPLOMATIC	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES. 1Ø,ØØØ GROUPS.	?	"3Ø1"	?	?-1927-?	1927 PERS Z S	RECOVERED 5Ø% - 6Ø%	T 1373 D 16, REPORT 1, P 2	(UNKNOWN)	--
SPAIN	7	CONSULAR	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES. 1Ø,ØØØ GROUPS.	?	"311"	?	?-1927-?	1927 PERS Z S	RECOVERED 5Ø% - 6Ø%	T 1377 T 1378 T 1382 D 16, REPORT 1, P 2	(UNKNOWN)	--
SPAIN	8	CONSULAR	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"156"	?	?-1938-?	? ?	RECOVERED 15% - 2Ø%	T 125Ø T 1251	(UNKNOWN)	--
SPAIN	9	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"CODE 1Ø7"	?	? - ?	? ?	RECOVERED 8Ø% - 85%	T 1344	(UNKNOWN)	--
SPAIN	1Ø	?	4-FIGURE 1-PART CODE.	?	"1Ø8"	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1%	T 1211 T 3Ø11	(UNKNOWN)	--
SPAIN	11	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"CODE 1Ø9"	?	? - ?	? PERS Z S	RECOVERED 5Ø% - 6Ø%	T 1212 T 1213	(UNKNOWN)	--

TOP SECRET

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN 12	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	CODE 111	?	? - ?	? PERS Z S	RECOVERED 4Ø% - 5Ø%	T 1214	(UNKNOWN)	--
SPAIN 13	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"119"	?	? - ?	? PERS Z S	RECOVERED 5Ø% - 6Ø%	T 1224	(UNKNOWN)	--
SPAIN 14	?	4-FIGURE 1-PART CODE.	?	"124"	?	? - ?	? PERS Z S	RECOVERED 2Ø%	T 1226	(UNKNOWN)	--
SPAIN 15	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"127"	?	? - ?	? PERS Z S	RECOVERED 1Ø% - 2Ø%	T 1345	(UNKNOWN)	--
SPAIN 16	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	SP. 134	?	? - ?	? PERS Z S	RECOVERED LESS THAN 1%	T 1346	(UNKNOWN)	--
SPAIN 17	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"152"	?	? - ?	? PERS Z S	RECOVERED LESS THAN 5%	T 1256	(UNKNOWN)	--
SPAIN 18	?	4-FIGURE 1-PART CODE.	?	"157"	?	? - ?	? PERS Z S	RECOVERED 5Ø% - 6Ø%	T 1242 T 1243	(UNKNOWN)	--
SPAIN 19	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"166"	?	? - ?	? PERS Z S	RECOVERED 5%	T 1239 T 1255	(UNKNOWN)	--
SPAIN 2Ø	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"167"	?	?-1932-?	? PERS Z S	RECOVERED 5Ø% - 6Ø%	T 1244 T 1245 T 1246	(UNKNOWN)	--
SPAIN 21	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"168"	?	? - ?	? PERS Z S	RECOVERED 25%	T 124Ø	(UNKNOWN)	--
SPAIN 22	?	4-FIGURE 1-PART CODE.	?	"SP. 172"	?	? - ?	? PERS Z S	RECOVERED 4Ø%	T 1234 T 1233 T 1347	(UNKNOWN)	--
SPAIN 23	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"SP. 175"	?	? - ?	? PERS Z S	RECOVERED 1Ø%	T 1348	(UNKNOWN)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN 24	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"SP. 179"	?	? - ?	? ?	RECOVERED LESS THAN 10%	T 1349	(UNKNOWN)	--
SPAIN 25	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"213"	?	? - ?	? ?	RECOVERED 5% - 10%	T 1352	(UNKNOWN)	--
SPAIN 26	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	"SP. 217"	?	? - ?	? ?	RECOVERED 60% - 75%	T 1353 T 1354	(UNKNOWN)	--
SPAIN 27	?	4-FIGURE 1-PART CODE.	?	"SP. 229"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1357	(UNKNOWN)	--
SPAIN 28	?	4-FIGURE 1-PART CODE.	?	"239"	?	? - ?	? ?	RECOVERED 5%	T 1359	(UNKNOWN)	--
SPAIN 29	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	"SP. 243"	?	? - ?	? ?	RECOVERED LESS THAN 5%	T 1360	(UNKNOWN)	--
SPAIN 30	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	"SP. 249"	?	? - ?	? ?	RECOVERED 5%	T 1362	(UNKNOWN)	--
SPAIN 31	?	4-FIGURE 1-PART CODE, REPAGINATED.	?	"261"	?	? - ?	? ?	RECOVERED 60%	T 1370	(UNKNOWN)	--
SPAIN 32	?	4-FIGURE 1-PART CODE.	?	"271"	?	?-1937-?	? ?	RECOVERED LESS THAN 5%	T 1371	(UNKNOWN)	--
SPAIN 33	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	?	?	? - ?	? PERS Z S	RECOVERED 30% - 40%	T 1210	(UNKNOWN)	--
SPAIN 34	?	4-FIGURE 1-PART CODE.	?	?	?	? - ?	? ?	RECOVERED 70%	T 1329	(UNKNOWN)	--
SPAIN 35	?	4-FIGURE 1-PART CODE.	?	?	?	? - ?	? ?	RECOVERED 20% - 30%	T 1384	(UNKNOWN)	--
SPAIN 36	?	4-FIGURE 1-PART CODE.	?	?	?	? - ?	? ?	RECOVERED 65% - 70%	T 1343	(UNKNOWN)	--
SPAIN 37	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	?	?	? - ?	? ?	RECOVERED 50%	T 1372	(UNKNOWN)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN 38	?	4-FIGURE 1-PART CODE, RANDOMIZED ON PAGES.	?	?	?	? - ?	? ?	RECOVERED 1Ø% - 15%	T 12Ø8	(UNKNOWN)	--
SPAIN 39	?	4-FIGURE 1-PART CODE.	?	"113"	?	? - ?	? ?	RECOVERED. 5Ø%	T 1215; T 1216 T 1217; T 1218 T 1219; T 122Ø T .1221; T 1222	(UNKNOWN)	--
SPAIN 4Ø	?	4-FIGURE 1-PART CODE.	?	"SP. 121"	?	? - ?	? ?	RECOVERED 1Ø% - 15%	T 1225	(UNKNOWN)	--
SPAIN 41	?	4-FIGURE 1-PART CODE.	?	"14Ø"	?	? - ?	? ?	RECOVERED 2Ø% - 25%	T 1257	(UNKNOWN)	--
SPAIN 42	?	4-FIGURE 1-PART CODE.	?	"148"	?	? - ?	? ?	RECOVERED 1Ø%	T 1238	(UNKNOWN)	--
SPAIN 43	?	4-FIGURE 1-PART CODE.	?	"165"	?	? - ?	? ?	RECOVERED 1Ø% - 15%	T 126Ø	(UNKNOWN)	--
SPAIN 44	?	4-FIGURE 1-PART CODE.	?	"N.3Ø3 SP"	?	? - ?	? ?	RECOVERED 5Ø% - 6Ø%	T 1375	(UNKNOWN)	--
SPAIN 45	?	4-FIGURE ?-PART CODE.	?	"SP. 73"	?	? - ?	? ?	NO SUCCESS	T 1263	(UNKNOWN)	--
SPAIN 46	?	4-FIGURE ?-PART CODE.	?	"112"	?	? - ?	? ?	NO SUCCESS	T 1262	(UNKNOWN)	--
SPAIN 47	?	4-FIGURE ?-PART CODE.	?	"114"	?	? - ?	? ?	NO SUCCESS	T 1261	(UNKNOWN)	--
SPAIN 48	?	4-FIGURE ?-PART CODE.	?	"118"	?	? - ?	? ?	NO SUCCESS	T 1223	(UNKNOWN)	--
SPAIN 49	?	4-FIGURE ?-PART CODE.	?	"126"	?	? - ?	? ?	NO SUCCESS	T 1227	(UNKNOWN)	--
SPAIN 5Ø	?	4-FIGURE ?-PART CODE.	?	"SP. 128"	?	? - ?	? ?	NO SUCCESS	T 1236	(UNKNOWN)	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN	51	?	4-FIGURE ?-PART CODE.	?	"SP. 138"	?	? - ?	? ?	RECOVERED LESS THAN 5%	T 1252	(UNKNOWN)	--
SPAIN	52	?	4-FIGURE ?-PART CODE.	?	"SP. 142"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1253	(UNKNOWN)	--
SPAIN	53	?	4-FIGURE ?-PART CODE.	?	"144"	?	? - ?	? ?	RECOVERED ABOUT 1%	T 1254	(UNKNOWN)	--
SPAIN	54	?	4-FIGURE ?-PART CODE.	?	"155"	?	1931-1936-?	? ?	NO SUCCESS	T 1249	(UNKNOWN)	--
SPAIN	55	?	4-FIGURE ?-PART CODE.	?	"161"	?	? - ?	? ?	RECOVERED LESS THAN 3%	T 1259	(UNKNOWN)	--
SPAIN	56	?	4-FIGURE ?-PART CODE.	?	"164"	?	? - ?	? ?	NO SUCCESS	T 1247	(UNKNOWN)	--
SPAIN	57	?	4-FIGURE ?-PART CODE.	?	"SP. 17Ø"	?	? - ?	? ?	NO SUCCESS	T 1248	(UNKNOWN)	--
SPAIN	58	?	4-FIGURE ?-PART CODE.	?	"SP. 171"	?	? - ?	? ?	NO SUCCESS	T 1228	(UNKNOWN)	--
SPAIN	59	?	4-FIGURE ?-PART CODE.	?	"VALENCIA 174"	?	? - ?	? ?	RECOVERED 5% - 1Ø%	T 1235	(UNKNOWN)	--
SPAIN	6Ø	?	4-FIGURE ?-PART CODE.	?	"SP. 187"	?	? - ?	? ?	VERY LITTLE SUCCESS	T 135Ø	(UNKNOWN)	--
SPAIN	61	?	4-FIGURE ?-PART CODE.	?	"SP. 2Ø9"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1351	(UNKNOWN)	--
SPAIN	62	?	4-FIGURE ?-PART CODE.	?	"253"	?	? - ?	? ?	RECOVERED 6Ø% - 7Ø%	T 1363 T 1364 T 1365 T 1366 T 1367 T 1368	(UNKNOWN)	--
SPAIN	63	?	4-FIGURE ?-PART CODE.	?	"3Ø2"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1374	(UNKNOWN)	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN	64	?	4-FIGURE ?-PART CODE.	?	"SP. 3Ø6"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 1376	(UNKNOWN)	--
SPAIN	65	?	4-FIGURE ?-PART CODE.	?	"SP. 345"	?	? - ?	? ?	RECOVERED LESS THAN 3%	T 1379	(UNKNOWN)	--
SPAIN	66	?	4-FIGURE ?-PART CODE.	?	"4Ø2"	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 138Ø	(UNKNOWN)	--
SPAIN	67	?	4-FIGURE ?-PART CODE.	?	"754 41"	?	? - ?	? ?	NO SUCCESS	T 1381	(UNKNOWN)	--
SPAIN	68	?	4-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	?	T 1265	(UNKNOWN)	--
SPAIN	69	?	4-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 1%	T 12Ø9	(UNKNOWN)	--
SPAIN	7Ø	DIPLOMATIC	2-PART CODE ENCIPHERED BY 1ØØ-GROUP KEY.	?	?	?	1939 - ?	? SIM	NOT READ	IF 1518	(UNIDENTIFIED)	--
SPAIN	71	NAVAL	CIPHER	?	CIPHER NO. 13	?	? - ?	? SIS	1ØØ% COMPROMISED	IF 15Ø6	(UNKNOWN)	--
SPAIN	72	?	4-FIGURE ?-PART CODE.	?	?	?	1941-1942?	1941 SIM	NOT READ	IF 1524	(UNIDENTIFIED)	--
SPAIN REPUBLICAN			GENERAL REMARKS ON SPAIN REPUBLICAN: DESPITE BASIC SIMILARITIES THE SYSTEMS DIFFERED IN INDICATOR AND APPARENTLY IN TYPE OF TEXT.									
SPAIN REPUBLICAN	73	MILITARY	SUBSTITUTION USING DIGRAPHS ØØ TO 99 ARRANGED IN COLUMNS AGAINST AN ALPHABET STRIP CONTAINING 3 NULLS.	?	R. 5	?	? - 1938	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--
SPAIN REPUBLICAN	74	MILITARY	DIGRAPHIC SUBSTITUTION USING SLIDING STRIPS.	?	N.	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--
SPAIN REPUBLICAN	75	MILITARY	DIGRAPHIC SUBSTITUTION USING SLIDING STRIPS.	?	S.N	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--
SPAIN REPUBLICAN	76	MILITARY	DIGRAPHIC SUBSTITUTION USING SLIDING STRIPS.	?	5 C.R	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--
SPAIN REPUBLICAN	77	MILITARY	DIGRAPHIC SUBSTITUTION, 1Ø X 1Ø SQUARE AND COORDINATE SLIDING STRIPS 17 VALUES LONG. SUBSTITUTION BY BOTH LETTERS AND DIGITS.	?	S.N.D	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--
SPAIN REPUBLICAN	78	MILITARY	SUBSTITUTION BY DIGRAPHS ØØ-99. ONE HUNDRED DIFFERENT KEYS WERE USED IN ARRANGING THE SUBSTITUTION.	?	S.O.	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS

AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SPAIN REPUBLICAN 79	MILITARY	DIGRAPHIC SUBSTITUTION USING 1Ø x 1Ø SQUARE AND COORDINATE SLIDING STRIPS. SUBSTITUTION BY BOTH LETTERS AND FIGURES.	?	S. MARZO	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--
SPAIN REPUBLICAN 80	MILITARY	DIGRAPHIC SUBSTITUTION USING 13 x 13 SQUARE AND COORDINATE SLIDING STRIPS. SUBSTITUTION BY MIXED ALPHABETS AND FIGURES.	?	"AIR ALARM"	?	?-1938-?	1938 SIS	READ	IF 15Ø4	(UNKNOWN)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SWEDEN 1	(DIPLOMATIC)	HAGELIN -- SMALL MACHINE, SIMILAR TO M-2Ø9. 6 WHEELS.	?	SM1	(SWA)	? - ?	AFTER SPRING 1944 OKH ? OKW	NOT BROKEN BUT MESSAGES IN DEPTH COULD BE READ	I 142 P 4	(NOT READABLE -- NOT BEING WORKED ON)	--
SWEDEN 2	CONSULAR	MACHINE THOUGHT TO HAVE 15-NUMBERED WHEELS. CALLED BY PW THE KRYTAA BUT MAY HAVE MEANT THE KRYHA OR HAGELIN.	?	?	?	? - ?	? FA	NO SUCCESS	I 162 P 3	(UNKNOWN IF IT HAD 15 NUMBERED WHEELS.)	THOUGHT BY FA TO BE 1ØØ% SECURE
SWEDEN 3	?	TRAFFIC THOUGHT TO HAVE BEEN HAGELIN. 1ST MONTH 25-LETTER ALPHABET USED; 2ND MONTH 26-LETTER ALPHABET USED.	?	?	?	? - ?	1941, AGAIN IN 1944 PERS Z S	NOT READ	I 22 P 7	(TRAFFIC USING 25-LETTER ALPHABET KNOWN AS SWC.)	--
SWEDEN 4	ARMY	HAGELIN -- LARGE MACHINE. THOUGHT BY GERMANS TO HAVE BEEN SIMILAR TO ENIGMA.	?	?	?	? - ?	? OKH	NOT READ BY OKH	I 142 P 4	(UNKNOWN)	--
SWEDEN 5	NAVY	APPARENTLY A MACHINE CIPHER. 4-LETTER SYSTEM.	?	"4-LETTER SYSTEM"	?	? - 1944 - ?	1944 OKM	PROBABLY NO SUCCESS -- SCANT MATERIAL	D 38 P 3, 4	(UNKNOWN)	--
SWEDEN 6	NAVY	MACHINE CIPHER.	?	KARL	?	? - 1944 - ?	1944 OKM	NO SUCCESS	D 38 P 3	(UNKNOWN)	--
SWEDEN 7	NAVY	MACHINE CIPHER.	?	PAUL	?	? - 1944 - ?	1944 OKM	NO SUCCESS	D 38 P 3	(UNKNOWN)	--
SWEDEN 8	NAVY	MACHINE CIPHER	?	RICHARD	?	? - 1944 - ?	1944 OKM	NO SUCCESS	D 38 P 3	(UNKNOWN)	--
SWEDEN 9	NAVY	MACHINE CIPHER	?	OTTO	?	? - 1944 - ?	1944 OKM	MONITORED 1944, 1945. PROBABLY NO SUCCESS	D 38 PP 2,3	(UNKNOWN)	--
SWEDEN 1Ø	NAVY	MACHINE CIPHER	?	SOFHIE	?	? - 1945 - ?	1945 OKM	PROBABLY NO SUCCESS -- SCANT MATERIAL	D 38 P 3	(UNKNOWN)	--
SWEDEN 11	NAVY	5-LETTER ?-PART CODE CVCCV. PROBABLY A COVERNAME SYSTEM.	?	MORSE	?	? - 1944 - ?	1944 OKM	PROBABLY NO SUCCESS	D 38 P 5	(UNKNOWN)	--
SWEDEN 12	NAVY	5-LETTER ? CODE. CVCVC.	?	SEDER	?	? - 1944 - ?	1945 OKM	?	D 38 P 4	(UNKNOWN)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SWEDEN 13	?	3-LETTER ?-PART CODE.	?	SASSNITZ	?	? - 1944 - ?	1945 OKM	BROKEN	D 38 P 4	(UNKNOWN)	--
SWEDEN 14	ARMY	3-LETTER ?-PART FIELD CODE.	?	SC2	?	? - ?	1943 OKH	READ	IF 120 P 5	(NO MILITARY SYSTEMS WORKED ON)	--
SWEDEN 15	ARMY	3-LETTER PARTIALLY 1-PART UNENCIPHERED FIELD CODE.	?	SC3	?	? - ?	1943 OKH	READ	IF 120 P 5	(NO MILITARY TRAFFIC WORKED ON)	--
SWEDEN 16	ARMY	3-LETTER 1-PART CODE.	?	SC4	?	? - ?	1943 OKH	READ	IF 120 P 5	(NO MILITARY TRAFFIC WORKED ON)	--
SWEDEN 17	MILITARY	2-LETTER AND 3-LETTER CODES.	?	?	?	? - ?	AFTER 1944 OKH	READ	I 55 P 11	(NO MILITARY SYSTEMS WORKED ON)	--
SWEDEN 18	?	1-FIGURE 2-LETTER CODE, ?-PART, 475 GROUPS.	?	"FIGURE-LETTER-LETTER"	?	? - 1945 - ?	1945 OKM	INVESTIGATED	D 38 P 5	(UNKNOWN)	--
SWEDEN 19	(DIPLOMATIC)	5-FIGURE 2-PART UNENCIPHERED CODE. NO 5-FIGURE GROUP CONTAINED THE SAME DIGIT TWICE.	?	?	(POSSIBLY SWB-1 OR SWB-2)	? - 1939	1943 PERS Z S 1940 SIM	?	IF 1518 P 3 I 22 P 21	(IF SWB-1, PARTIALLY COMPROMISED. BEING WORKED ON. IF SWB-2, BEING WORKED ON.)	(TRAFFIC IN SWB-1 AND SWB-2 CONTINUED LATER THAN THE CLOSING DATE GIVEN BY PW FOR THIS CODE)
SWEDEN 20	CONSULAR	5-FIGURE AND 4-FIGURE 2-PART UNENCIPHERED CODE. IN 1939 ALMOST ALL LINKS EXCEPT STOCKHOLM - TOKYO WENT OVER TO A MACHINE.	?	?	?	? - 1939, ON MOST LINKS	BEFORE 1939 FA	READ	I 162 P 3	(UNIDENTIFIED)	--
SWEDEN 21	DIPLOMATIC	4-FIGURE ?-PART CODE.	?	?	?	AFTER 1939 - ?	AFTER 1939 SIM	?	IF 1518 P 3	(UNIDENTIFIED)	--
SWEDEN 22	MILITARY	SIMPLE RECIPROCAL SUBSTITUTION.	?	?	?	? - ?	AFTER SEPT 1944 OKH	READ	I 55 P 11	(NO MILITARY TRAFFIC WORKED ON)	--
SWEDEN 23	ARMY	REVOLVING GRILLE TRANSPOSITION CIPHERS.	?	SRA-1 SRA-5	?	? - ?	1943 OKH	READ	IF 120 P 5	(NO MILITARY TRAFFIC WORKED ON)	--

TOP SECRET

CHART NO. 1-

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
SWEDEN	24	ARMY	TRANSPOSITION SYSTEM. "HARDER THAN REVOLVING GRILLE."	?	HGA	?	? - 1944 - ?	1944 PERS Z S 1944 OKH 1944 OKM	PROBABLY NOT BROKEN	IF 120 P 5 D 38 P 4	(NO MILITARY TRAFFIC WORKED ON)	--
SWEDEN	25	MILITARY	ELEMENTARY TYPE TRANSPOSITION.	?	?	?	? - ?	AFTER SEPT 1944 OKH	READ	I 55 P 11	(NO MILITARY SYSTEMS WORKED ON)	--
SWEDEN	26	?	?	?	FFFF	?	? - 1944 - ?	1944 OKM	?	D 38 P 5	(UNKNOWN)	--
SWEDEN	27	?	?	?	FFF	?	? - 1944 - ?	1944 OKM	?	D 38 P 5	(UNKNOWN)	--
SWEDEN	28	DIPLOMATIC	MACHINE CIPHER	?	?	?	1939 - ?	? SIM	NOT READ	IF 1518	(UNIDENTIFIED)	--
SWEDEN	29	DIPLOMATIC	MACHINE	?	?	?	1939 - ?	? SIM	NOT READ	IF 1518	(UNIDENTIFIED)	--
SWEDEN	30	DIPLOMATIC?	5-FIGURE 2-PART CODE. NO DIGIT REPEATED IN A GROUP. UNENCIPHERED.	?	?	?	? - 1939	? SIM	?	IF 1518	(UNIDENTIFIED)	--
SWEDEN	31	DIPLOMATIC	4-FIGURE ?-PART CODE.	?	?	?	1939 - ?	? SIM	?	IF 1518	(UNIDENTIFIED)	--

TOP SECRET

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						

SYRIA 1	ARMY	FRENCH LANGUAGE CODE: TABLE OF 17 LINES AND 8Ø COLUMNS, 3-LETTER GROUPS OF WHICH MIDDLE ONE IS A VOWEL. KEY WORD CHANGED ABOUT ONCE A MONTH. APPROXIMATELY 1,7ØØ WORDS.	?	?	?	?-1941-?	1941 SIM	READ	IF 118C P 3
									IF 118G P 4
										(UNKNOWN)	--

SYRIA 2	POLICE	4-FIGURE ?-PART CODE. ENCIPHERED BY SIMPLE SUBSTITUTION.	?	?	?	?-1943	? OKH	READ	I 17Ø P 3	(UNKNOWN)	--
SYRIA 3	POLICE	CIPHER SYSTEM. SIMPLE FIGURE SUBSTITUTION.	?	?	?	?-1943	? OKH	READ	I 17Ø P 3	(UNKNOWN)	--
SYRIA 4	POLICE	"1Ø X 1Ø MULTIALFHABETICAL TABLE WITH OMOPHONES." (??) "KEY" CHANGED MONTHLY.	?	?	?	? - ?	? ITALIANS	READ	IF 118G F 5	(UNKNOWN)	--
SYRIA 5	?	3-LETTER "CIPHER."	?	?	?	?-1941-?	1941 SIM	"PROBABLY" READ	IF 118C F 3	(UNKNOWN)	--
SYRIA 6	?	3-FIGURE "CIPHER."	?	?	?	?-194;-?	1941 SIM	PROBABLY READ	IF 118C F 3	(UNKNOWN)	--
SYRIA 7	POLICE	"CODE". TABLE OF 1Ø x 1Ø.	?	?	?	?-1941-?	1941 SIM	READ	IF 118C P 3	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
SWITZERLAND 1	DIPLOMATIC	ENIGMA CIPHER MACHINE.	(ENIGMA)	?	(SZD)	(?-1942-CURRENT)	? PERS Z S ? SIM	READ AT DIFFERENT TIMES. SIM DID NOT READ.	I 22 P 14 P 19 I 54 P 2 IF 1526	(THREE TYPES OF TRAFFIC PRESUMED TO BE ENIGMA--SZD-1, SZD-2, AND SZD-3. SZD-1 READ OVER 5Ø%, OTHERS NOT READ.)	--
SWITZERLAND 2	DIPLOMATIC	4-LETTER ?-PART CODE IN FORM VCVC. (BOTH 1-PART AND 2-PART.)	(I.E. 1, 2 3, 4)	?	(SZA FR.) (SZB GER.) (SZC ENG) (SZR FR.)	(?-1939-CURRENT)	? SID, SIM	NO SUCCESS	IF 1526 P 6	(ALL READABLE.)	--
SWITZERLAND 3	DIPLOMATIC	3-LETTER 1-PART CODE. 3,ØØØ GROUPS. FIRST LETTER OF GROUP INDICATED PAGE, SECOND LETTER THE COLUMN, AND THIRD THE LINE. INDICATOR: 5-LETTER GROUP AT BEGINNING. (TWO BOOKS: FRENCH AND GERMAN)	(CODE K)	"S.V. 1"	(SZG)	(1942-CURRENT)	1944 SID ? SIM	75% OF FRENCH BOOK READ; GERMAN BOOK PARTIALLY READ.	IF 1526 PP 6-9 T 1537 T 15Ø2 T 16Ø3 IF 1522	(1ØØ% READABLE THROUGH RECOVERY.)	--
SWITZERLAND 4	CONSULAR	3-LETTER 1-PART CODE. VALUES IN FRENCH AND GERMAN. FIRST LETTER INDICATED PAGE, SECOND LETTER COLUMN, AND THIRD LETTER THE LINE. INDICATOR: FIFTH LETTER OF FIRST GROUP AND FIRST AND FIFTH LETTERS OF SECOND GROUP.	(CODE G)	CONSOLARE GZX	(SZG FR.) (SZH GER.)	(?-1941-CURRENT)	1944 SID	RECOVERED ABOUT 25% OF FRENCH BOOK	IF 1526 PP 9-11 T 1532 T 1537	(1ØØ% READABLE THROUGH RECOVERY.)	--
SWITZERLAND 5	?	3-LETTER 1-PART CODE. VALUES IN GERMAN.	?	?	?	? - ?	? ?	RECOVERED 15% - 2Ø%	T 1533	(UNIDENTIFIED)	--
SWITZERLAND 6	?	?-PART CODE, VALUES IN FRENCH.	?	?	?	? - 1941	? SIM	READ	IF 1517 P 3	(UNIDENTIFIED)	--
THAILAND 1	DIPLOMATIC ?	5-LETTER ?-PART CODE. USED BETWEEN BERNE, STOCKHOLM, AND BANGKOK. (LANGUAGE UNKNOWN, ENCIPHERED WITH ONE OF THREE DIFFERENT FORMS OF SUBSTITUTION.)	?	?	(THB)	(1944-CURRENT)	? GERMANS	PROBABLY NOT SOLVED.	T 2364	(ENCIPHERMENT SOLVED 1945. CODE NOT WORKED ON.)	--
THAILAND 2	DIPLOMATIC	5-FIGURE 1-PART CODE. ENGLISH LANGUAGE USED. USED WITH AND WITHOUT ENCIPHERMENT. SOMETIMES USED REPEATING 5-FIGURE ADDITIVE. (WHICH CHANGED EVERY FEW MONTHS, OR MONOALPHABETIC, OR POLYALPHABETIC SUBSTITUTION USED.)	?	?	(THA)	(?-1941-CURRENT)	1941 PERS Z S 1942 FA	ALMOST COMPLETELY READ	D 16, REPORT 2, P 2 D 16, REPORT 3, P 3 T 2375 T 237Ø T 2368 T 2376	(BROKEN AND READ IN 1943. NOW 1ØØ% READABLE.)	--
THAILAND 3	(COMMERCIAL ?)	5-LETTER ?-PART CODE. USED BY MINISTER OF FINANCE.	?	?	?	?-1941-1943-?	? GERMANS	PROBABLY NOT READ	T 2364	(UNKNOWN)	--
THAILAND 4	(COMMERCIAL ?)	?-PART CODE USED BETWEEN BANGKOK AND BREMEN.	?	?	?	? - 1945	? GERMANS	PROBABLY NOT READ	T 2364	(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
TURKEY 1	DIPLOMATIC	2-PART CODE. ENCIPHERED ABOUT 1/2 THE TIME WITH A REPEATING 5-FIGURE ADDITIVE WHICH CHANGED DAILY BUT WAS SOMETIMES REPEATED FROM YEAR TO YEAR. USED ON RATHER UNIMPORTANT TRAFFIC.	?	?	?	1934-1935	1934? PERS Z S	SOLVED.	I 103 P 2	(UNIDENTIFIED)	--

TURKEY 2	DIPLOMATIC	4-FIGURE 2-PART CODE. LATER GIVEN THREE REPAGINATIONS. SEE ITEMS 3, 4, AND 5.	INKILAP	?	-	?-1930-1940	? SIM	COMPROMISED. READ.	IF 1517 P 3
									IF 1523 PP 2, 3
									PERHAPS IF 118
										(UNKNOWN UNTIL INFORMATION WAS RECEIVED FROM BRITISH. NO WORK DONE. NO TRAFFIC RECEIVED.)	--

TURKEY 3	DIPLOMATIC	REPAGINATION OF ITEM 2. USED IN MONTHLY ROTATION WITH ITEMS 4 AND 5. AFTER 1940 SOMETIMES ENCIPHERED BY 40-FIGURE REPEATING ADDITIVE WHICH FREQUENTLY CHANGED.	ZAFER	?	(TUB)	1935-(1944)	1935 PERS Z S
							1940 SIM
								BROKEN AND READ BY SIM AND PERS Z S	IF 1517 P 3
									IF 1523 PP 2, 3
									I 103 PP 2, 3
										(WORK HAD BEGUN WHEN PHOTOSTAT COPY WAS RECEIVED FROM THE BRITISH IN 1943.)	NOT KNOWN BY ASA TO HAVE BEEN USED IN MONTHLY ROTATION

TURKEY 4	DIPLOMATIC	REPAGINATION OF ITEM 2. USED IN MONTHLY ROTATION WITH ITEMS 3 AND 5. AFTER 1940 SOMETIMES ENCIPHERED BY 40-FIGURE REPEATING ADDITIVE WHICH FREQUENTLY CHANGED.	SAKARIA	?	(TUD)	1935-(CURRENT)	1935 PERS Z S
							1940 SIM
								BROKEN AND READ BY SIM AND PERS Z S	IF 1517 P 3
									IF 1523 PP 2, 3
									I 103 PP 2, 3
										(SOLVED IN 1943 AND 1944.)	

TURKEY 5	DIPLOMATIC	REPAGINATION OF ITEM 2. USED IN MONTHLY ROTATION WITH ITEMS 3 AND 4. AFTER 1940 SOMETIMES ENCIPHERED BY 40-FIGURE REPEATING ADDITIVE WHICH FREQUENTLY CHANGED.	?	?	(TUJ)	1935-(1945)	1935 PERS Z S 1940 SIM	BROKEN AND READ BY SIM AND PERS Z S	IF 1523 PP 2, 3 I 103 PP 2, 3	(SOLVED IN 1943 AND 1944.)	

TURKEY 6	DIPLOMATIC	4-FIGURE 2-PART CODE. SOMETIMES ENCIPHERED BY A 40-FIGURE REPEATING ADDITIVE WHICH FREQUENTLY CHANGED. USED BY THE TURKISH EMBASSIES IN BERLIN AND VICHY?.	CANKAYA	?	(TUE)	1940-(CURRENT)	1941? SIM	RECOVERED 5,000 GROUPS	IF 1517 PP 3, 8, APPENDIX F
									IF 1523 P 3
										(BROKEN AND AIDED BY BRITISH. READ IN 1943. NOW BEING ALMOST COMPLETELY READ.)	--

TURKEY 7	DIPLOMATIC	4-FIGURE (2)-PART CODE. ENCIPHERED BY A 40-FIGURE REPEATING ADDITIVE. USED BETWEEN ANKARA AND THE ROME EMBASSY.	INEUNU (INÖNU)	ROMA	(TUF)	1940-(1945)	1941 SIM	RECOVERED 5,000 GROUPS	IF 1517 P 3
									IF 1523 P 3
										(PARTIALLY BROKEN BY BRITISH IN 1943. NO FURTHER SOLUTION DONE BY BRITISH OR ASA. TRAFFIC RECEIVED AND SOME DECODED AND TRANSLATED.)	--

TURKEY 8	DIPLOMATIC, CONSULAR	SET OF THREE 4-FIGURE PARTIALLY 1-PART CODES IN ARABIC SCRIPT. USED IN MONTHLY ROTATION. SOMETIMES ENCIPHERED BY A 40-FIGURE OR A 5-FIGURE REPEATING ADDITIVE.	(CUMHURIET)	?	(TUK)	1934-(1944)	1934 PERS Z S
							? SIM
								SOLVED AND READ BY PERS Z S. COMPROMISED BY SIM.	I 103 P 2
									IF 1517 P 3
									IF 1523 P 4
										(COMPROMISED BOOK RECEIVED FROM THE BRITISH IN 1944.)	--

TURKEY 9	DIPLOMATIC	4-FIGURE 1-PART CODE. ENCIPHERED BY 40-FIGURE REPEATING ADDITIVE (WHICH FREQUENTLY CHANGED).	?	?	(TUH)	(?-1943-CURRENT)	1943 SIM 1944 PERS Z S	BROKEN AND READ BY SIM. READ BY PERS Z S.	IF 1517 P 3 SEE ALSO I 63 P 2	(BRITISH AND ASA EXCHANGED VALUES AND BROKE BOOK AND ENCIPHERMENT. READ IN 1944)	--

TURKEY 10	MILITARY ATTACHE	5-FIGURE ?-PART CODE. ALL GROUPS BEGAN WITH DIGIT 1. IN 1942 REPLACED BY CODE DESCRIBED IN ITEM 11.	?	?	?	?-1940-1942	? SIM	BROKEN AND READ	IF 1517 P 3
									IF 1523 P 4
										(UNKNOWN)	--

~~TOP SECRET~~

CHART NO.

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
TURKEY 11	MILITARY ATTACHE	5-FIGURE 1-PART CODE. (AT FIRST) FREQUENTLY ENCIPHERED BY A 5-FIGURE (REPEATING) ADDITIVE. (NOW UNENCIPHERED OR ENCIPHERED BY 40-FIGURE REPEATING ADDITIVE.) USED BY ALL TURKISH MILITARY ATTACHES.	?	?	(TUA)	(1940-CURRENT)	1943 SIM PERHAPS PERS Z S	BROKEN AND COMPLETELY READ. ALSO COMPROMISED.	IF 1517 P 8, APPENDIX E SEE ALSO I 63 P 2	(PARTIALLY BROKEN AND AIDED BY BRITISH. LATER 100% COMPROMISED. NOW COMPLETELY READ.)	--
TURKEY 12	DIPLOMATIC, MILITARY ATTACHE	?-FIGURE ?-PART CODE WITH LETTER SUBSTITUTION. USED IN TRAFFIC FROM RUSSIA, BULGARIA, AND ITALY.	?	?	?	? - 1944 - ?	1944 FA 1944 OKH	READ.	IF 126 P 12	(UNKNOWN)	--

TURKEY 13	ARMY, AIR	POLYALPHABETIC SUBSTITUTION CIPHER. USUALLY HAD 5-13 ALPHABETS. MONTHLY KEY CHANGE; GEOGRAPHICAL NAMES USED FOR CODEWORDS. J, W, X ARE USED AS NULLS.	?	?	?	?-1940-1943-?	1940 OKH
							1941 SIM
								READ BY SIM. BROKEN AND READ BY OKH.	IF 1523 P 4, APPENDIX A
									IF 1517 P 6
									IF 126 PP 10, 11
									IF 118C F 3
									IF 115G P 2,3
										(UNKNOWN)	--

TURKEY 14	MILITARY	?-PART CODE. SOMETIMES ENCIPHERED BY A METHOD WHICH ENCIPHERED ONLY ONE OR TWO FIGURES OF EACH GROUP.	?	5 Z	?	?-1936-1939-?	1936, 1939 PERS Z S	SOLVED	I 103 P 3	(UNKNOWN--NO MILITARY TRAFFIC WORKED ON.)	--
TURKEY 15	MILITARY	?-PART CODE.	?	?	?	1939 - ?	AFTER 1939 OKW, PERS Z S	PROBABLY "SPASMODIC SUCCESS ACHIEVED	I 103 P 3	(UNKNOWN)	--
TURKEY 16	MILITARY	?-PART CODE. "A TURKISH PROCEDURE CODE."	?	?	?	?-1941-1943-?	1941 SIM	?	IF 1523 P 5	(UNKNOWN)	--
TURKEY 17	MILITARY	?-PART CODE. ALL TRIGRAMS BEGAN WITH THE LETTER S.	G	?	?	?-1941-1943-?	1941 SIM	?	IF 1523 P 5	(UNKNOWN)	--
TURKEY 18	POLICE	?-PART CODE, LOW GRADE. ONLY 100 GROUPS. OF THE FIELD-CODE TYPE, A SQUARE OF 10X10, WITH COLUMNS AND LINES NUMBERED 1 TO 10, IN ASCENDING ORDER. THE ARRANGEMENT WITHIN THE SQUARE WAS CHANGED PERIODICALLY.	?	?	?	?-1941-1943-?	1941 SIM	READ.	IF 1523 P 6	(UNKNOWN)	--
TURKEY 19	AIR	1-PART CODE. UNENCIPHERED.	?	?	?	? - ?	? OKL	EASILY READ	I 119 P 5	(UNKNOWN)	--
TURKEY 20	AIR	PERIODIC POLYALPHABETIC SUBSTITUTION CIPHER USING SLIDING STRIPS. CHANGED MONTHLY.	?	?	?	? - ?	? OKL	EASILY READ	I 119 P 5	(UNKNOWN)	--
TURKEY 21	AIR	SINGLE TRANSPOSITION CIPHER FOR WEATHER REPORTS.	?	?	?	? - ?	? OKL	EASILY READ	I 119 P 5	(UNKNOWN)	--

TURKEY 22	NAVY	POLYALPHABETIC SUBSTITUTION CIPHER. KEY LENGTH VARIED FROM 5 TO 13; NO KEY WORD USED. KEY CHANGED EVERY 2 OR 3 MONTHS. SIMILAR TO ITEM 13.	?	?	?	?-1941-1943-?	1941 SIM	BROKEN AND READ	IF 1523 P 5
									IF 115C F 3
									IF 118G P 3
										(UNKNOWN)	--

TURKEY 23	NAVY		-	-	-	-	-	PROBABLY NO WORK DONE BY OKM ON ANY NAVY SYSTEMS	I 83 P 2		--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTE AT ASA
			COUNTRY OF ORIGIN	AXIS	U.S.A.					
TURKEY 24	POLICE	SUBSTITUTION CIPHER SYSTEM USING 2 FIGURES FOR EACH LETTER OR NUMBER. MOST FREQUENT LETTERS USED VARIABLES.	?	?	?	?-1941-1943-PERHAPS CURRENT	1941 OKH	READ	IF 126 PP 12, 13	(UNKNOWN)
TURKEY 25	POLICE	SUBSTITUTION CIPHER SYSTEM USING TWO OR THREE FIGURES FOR EACH LETTER. TWO DIFFERENT SUBSTITUTION TABLES USED.	?	?	?	1942-1943-PERHAPS CURRENT	1942? OKH	PROBABLY READ	IF 126 P 13	(UNKNOWN)
TURKEY 26	POLICE	SUBSTITUTION CIPHER SYSTEM USING 2 OR 3 FIGURES PER LETTER. WEEKLY OR MONTHLY KEY CHANGE. TRANSMITTED IN 4, 5, OR 6 FIGURES.	?	?	?	?-1941-1943-?	1941 SIM	READ	IF 1523 P 6	(UNKNOWN)

TURKEY 27	POLICE	MONOALPHABETIC SUBSTITUTION CIPHER. NORMAL ALPHABET SLID AGAINST ITSELF WITH DAILY CHANGING STARTING POINT. THE LETTERS G, X, AND W WERE ONLY USED TO SEPARATE WORDS.	?	?	?	1941-1943-?	1941 SIM
							1941 OKH
								READ	IF 1523 P 6
									IF 126 P 12
										(UNKNOWN)

TURKEY 28	?	?-PART CODE.	?	?	?	? - ?	1943 OKW	SOLVED CRYPTANALYTICALLY. LATER COMPROMISED.	I 132 P 2	(UNIDENTIFIED)
TURKEY 29	?	"NUMBER CODE". USED ONLY BY THE TURKISH PRESIDENT ON THE STATE-YACHT "SAVARONA" ON HIS TRIP TO IZMIR.	?	?	?	1943 ONLY	? OKH	BROKEN	IF 126 P 12	(UNKNOWN)
TURKEY 3Ø	DIPLOMATIC	SMALL SUPPLEMENTARY CODE IN FRENCH. APPROXIMATELY 1,ØØØ GROUPS.	?	"FRENCH" CODE	(FRENCH SUPPLEMENT TO TUK)?	"VERY OLD"	194Ø, 1941 SIM	NOT READ	IF 1523 P 3	(COMPROMISED COPY RECEIVED FROM BRITISH WITH TUK)
TURKEY 31	DIPLOMATIC	?-PART CODE FOR USE ON BERLIN-ANKARA LINK.	?	?	?	? - ?	? SIM	?	D 71	(UNIDENTIFIED)
TURKEY 32	MILITARY, AIR, AND NAVAL ATTACHES	?-PART CODE OF 261 PAGES.	?	?	?	? - ?	? SIS	READ. COMPROMISED.	IF 15Ø6	(UNIDENTIFIED)

TURKEY 33	POLICE	4-FIGURE 2-PART CODE, UNENCIPHERED.	?	?	?	?-1943-?	1943 SIM	READABLE SINCE JUNE 1943	IF 118C P 4
									IF 118F
									IF 118F P 2
										(UNIDENTIFIED)

TURKEY 34	POLICE	SIMPLE TRANSPOSITION CIPHER USING 29-LETTER ALPHABET; DAILY-CHANGING KEY. J, W, AND X ARE NULLS.	?	?	?	?-1941-?	1941 SIM	?	IF 118C P 3
									IF 118F
									IF 118G
										(UNIDENTIFIED)

TURKEY 35	?	"METEOROLOGICAL CODE."	?	?	?	? - ?	1942 OKL	"DECIPHERED"	IF 118B P 17	(UNIDENTIFIED)

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 1	DIPLOMATIC	CIPHER MACHINE OF SWEDISH ORIGIN, PERHAPS HAGELIN, USED FOR MESSAGES FROM ITALIAN THEATER.	?	?	--	?-1944-?	1944 OKW	OKW POSSESSED MACHINE; READ ALL TRAFFIC FROM ITALIAN THEATER.	I 76 P 12	--	--
UNITED KINGDOM 2	DIPLOMATIC	5-LETTER 1-PART CODE WITH 84,ØØØ GROUPS.	GOVERNMENT TELEGRAPH CODE	B 22	--	?-1939-1942-?	1939 PERS Z S	READ SINCE 1939. SUMMER 194Ø, CAPTURED ORIGINAL GIVEN TO PERS Z S.	D 16, REPORT 2, P 1 D 16, REPORT 4, P 1	--	--
UNITED KINGDOM 3	DIPLOMATIC	5-LETTER 1-PART CODE WITH ABOUT 84,ØØØ GROUPS.	GOVERNMENT TELEGRAPH CODE, AFRICA	B 23	--	?-1941-1942-?	1941 PERS Z S	READ ALMOST WITHOUT GAP	D 16, REPORT 2, P 1 D 16, REPORT 4, P 2	--	--
UNITED KINGDOM 4	DIPLOMATIC	5-LETTER ?-PART CODE, UNENCIPHERED.	?	?	--	? - ?	? PERS Z S	BOOK ONLY PARTLY BUILT	I 22 P 12	--	--
UNITED KINGDOM 5	DIPLOMATIC FOREIGN OFFICE	4-LETTER 2-PART CODE WITH 16, 224 GROUPS.	R CODE 1935	B 25;	--	1935-1942-?	PRIOR TO 194Ø PERS Z S	READ ALMOST COMPLETELY. CAPTURED AT BERGEN, 194Ø	D 16, REPORT 2, P 1 D 16, REPORT 4, P 1 I 172 P 3	--	--
UNITED KINGDOM 6	DIPLOMATIC	4-LETTER 2-PART CODE USED IN NEAR, MIDDLE, AND FAR EAST.	R CODE 1941?	B 3Ø	--	?-1941-1942-?	1941 PERS Z S	AT END OF 1942 ABOUT 1,ØØØ GROUPS WERE RECOVERED	D 16, REPORT 2, P 1 D 16, REPORT 4, P 1	--	--
UNITED KINGDOM 7	DIPLOMATIC	4-LETTER 2-PART CODE WITH 16,ØØØ GROUPS.	?	B 31	--	1942 - ?	1942 PERS Z S	AT END OF 1942 2,5ØØ GROUPS RECOVERED. FIRST TELEGRAMS READ IN OCTOBER 1942.	D 16 REPORT 4, P 1	--	--
UNITED KINGDOM 8	DIPLOMATIC	4-LETTER ?-PART CODE, UNENCIPHERED.	?	?	--	?-194Ø-?	? PERS Z S	BOOK CAPTURED IN NORWAY; ALREADY READ BEFORE THIS.	I 22 PP 11-12	--	--
UNITED KINGDOM 9	DIPLOMATIC	2-PART CODE USED MAINLY FOR TRAINING IN 1942 AND 1943. ENCIPHERED BY ADDITIVE. INDICATOR WAS SECOND GROUP.	?	?	--	1942-1943	1942 OKW	SMALL PART OF TRAFFIC READ BEFORE 1943.	I 76 P 14	--	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 1Ø	DIPLOMATIC	?-FIGURE ?-PART CODE.	INTERDEPARTMENTAL CODE	?	--	?-1941-?	1941 PERS Z S 1941 OKW 1941 OKL	BOOK 1ØØ% COMPROMISED 1941. ADDITIVE PARTLY BROKEN BY OKW, OKL. WORK STOPPED 1942.	D 16, REPORT 2, P 1	--	--
UNITED KINGDOM 11	DIPLOMATIC	ADDITIVE ENCIPHERMENT SYSTEM WITH KEYS CHANGING EVERY TWO OR THREE MONTHS. TRAFFIC PREFIXED "PRODROME". TOTAL LENGTH ESTIMATED BY PERS Z S AT 1Ø,ØØØ 4-FIGURE GROUPS.	?	?	--	?-194Ø-1941-?	194Ø PERS Z S ? OKW	PERS Z S RECOVERED 23% OF ADDITIVE; DID NOT ATTACK BOOK. OKW DID NOT READ.	I 22 PP 17-18 I 31 P 6	--	--
UNITED KINGDOM 12	DIPLOMATIC	DOUBLE TRANSPOSITION WITH SAME KEY-LENGTH FOR BOTH RECTANGLES.	?	?	--	? - ?	? OKW	SOME READ	I 31 P 6	--	--
UNITED KINGDOM 13	ARMY	4-LETTER OR 5-LETTER ?-PART CODE ENCIPHERED WITH ADDITIVE.	EMPIRE CODE	?	--	?-1941-1942-?	1941 OKH	BOOK PARTLY BUILT	IF 126 P 13	--	--
UNITED KINGDOM 14	ARMY	3-LETTER ?-PART CODE. SECOND LETTER OF GROUP WAS ALWAYS A VOWEL (INCLUDING Y).	TIGER CODE	?	--	? - ?	? OKW	SOLVED IN SIX MONTHS.	I 76 P 13	--	--

UNITED KINGDOM 15	ARMY-CORPS-DIVISION	4-FIGURE 2-PART CODE ENCIPHERED WITH ADDITIVE WHICH WAS A TABLE WITH STARTING POINTS INDICATED BY 5-LETTER GROUPS. ADDITIVE CHANGED ABOUT EVERY TWO WEEKS. FROM SPRING 1943 ENCIPHERED WITH ONE-TIME PADS.	WAR OFFICE CODE	WOC	--	194Ø-1943	194Ø OKH
							? SIM
								RECONSTRUCTED AND READ UNTIL CODE COMPROMISED IN AFRICA, JULY 1942. COMPROMISED ALSO IN NORWAY, APRIL 194Ø, AND NEAR DUNKIRK JUNE 194Ø. NOT READ BY SIM.	I 51
									I 113 P 4
									IF 1Ø7 P 7
									IF 1517
									IF 1519
										--	--

UNITED KINGDOM 16	ARMY	POLYALPHABETIC SUBSTITUTION SYSTEM EMPLOYING BOOK OF RANDOM ALPHABETS AND NOTCHED CARD FOR SELECTING CIPHER TEXT.	LINEX	LINEX	--	1945 - ?	1945 OKH	NOT READ	IF 144 PP 6-8	--	--
UNITED KINGDOM 17	ARMY, AIR FORCE	2-LETTER CODE WITH 2Ø4 VALUES ARRANGED IN RECTANGLE. CODE GROUPS FORMED FROM COORDINATES ON SLIDING STRIPS.	SLIDEX	BRITISH SIDE-SQUARE, EC PLUS A NUMBER"	SLIDEX	?-1943-?	? OKH ? OKL	OKH READ CURRENTLY; OKL READ CURRENTLY.	I 76 P 4 I 1Ø9 P 38 IF 126 PP 13-14 IF 144 PP 2-3 P 6	--	--
UNITED KINGDOM 18	AIR FORCE COMMAND NETWORKS	CIPHER MACHINE: TRAFFIC SENT IN 5-LETTER GROUPS.	?	?	--	? - ?	? OKL	NOT BROKEN	I 1Ø9 P 35	--	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A						
UNITED KINGDOM	19	AIR FORCE	CIPHER DEVICE	?	"32 COLUMN CAESAR CODING MACHINE"	--	?-1942-?	PRIOR TO 1942 OKH	OKH HAD CAPTURED DEVICE. TRAFFIC READ UNTIL 1942.	IF 126 P 13	--	--
UNITED KINGDOM	2Ø	AIR FORCE	3-LETTER ?-PART CODE.	AIRCRAFT REPORTING CODE	?	--	? - ?	? OKL ? OKM	OKL BROKE REGULARLY TO AN EXPLOITABLE EXTENT. OKM READ WITH MANY GAPS.	I 112 P 3 I 147 P 17	--	--
UNITED KINGDOM	21	AIR FORCE	2-LETTER ?-PART CODE WITH DAILY CHANGE OF KEY.	BOMBER CODE	?	--	?-1942-?	1942 OKL	BROKEN WITH AID OF CAPTURED KEYS.	I 1Ø9 P 38 I 112 P 2	--	--
UNITED KINGDOM	22	AIR FORCE	4-FIGURE ?-PART CODE. FIRST TWO GROUPS REPEATED AT END. USED IN RAF GROUND-GROUND TRAFFIC.	?	?	--	?-194Ø-1943-?	194Ø OKL	BROKEN IN MEDITERRANEAN AREA SPRING 1941 BUT NOT ON WESTERN FRONT. BOOK RECONSTRUCTED. READ WITH LAG OF 2-4 WEEKS. BECAME UNREADABLE NOV 1942.	I 1Ø9 P 35 I 152 PP 12-13	--	--
UNITED KINGDOM	23	AIR FORCE	4-FIGURE ?-PART CODE, ENCIPHERED WITH ADDITIVE.	?	?	--	?-1942-?	1942 OKL	NOT READ AFTER 1942	I 13 P 6	--	--
UNITED KINGDOM	24	AIR FORCE	TRANSPOSITION CIPHER WITH KEY LENGTH OF 1Ø, USED BY TORPEDO BOMBERS ON EXERCISES IN NORTH CHANNEL.	?	SPESSART	--	? - 1944	1943 OKM	READ CURRENTLY	D 6 D 15 P 1Ø D 41 P 5	--	--
UNITED KINGDOM	25	ARMY, NAVY, AIR FORCE	4-FIGURE ?-PART CODE USED FOR TRAFFIC BETWEEN BRANCHES OF THE ARMED FORCES.	INTERSERVICE CIPHER	STRALSUND	--	? - ?	1944 OKM	NOT BROKEN	D 6 I 144 P 3	--	--
UNITED KINGDOM	26	ARMY, NAVY	CIPHER MACHINE WITH 5 WHEELS--2 OUTSIDE WHEELS FIXED.	TYPEX	TYPEX	--	?-194Ø-?	194Ø OKL ? OKH 194Ø OKW BEFORE 1939 OKM	NOT BROKEN. MACHINES WITHOUT WHEELS CAPTURED AT BREST, DUNKIRK, AND/OR NORTH AFRICA, 194Ø. KEYS WERE SOMETIMES CAPTURED.	D 15 P 4 D 4Ø; D 49 I 2 P 3 I 31 P 11 I 49 P 3 I 59 P 5 I 78 P 9 I 93 PP 1Ø,16 I 112 P 3 I 113 P 4 I 119 P 5 I 142 P 2 I 144 PP 2,4 I 161 P 2 PP 4-5 P 6 IF 142 P 8	--	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 27	NAVY	ADDITIVE SUPERENCIPHERING SYSTEM, EMPLOYING GRILLE. 1Ø,ØØØ POSSIBLE DAILY STARTING POSITIONS USED TO SUPERENCIPHER VARIOUS NAVAL CODES.	STENCIL SUBTRACTOR FRAME	"S.S. FRAME"	--	1942 - ?	1943 OKM	OKM READ FOR ONE MONTH; THEN CODE BOOK CHANGED, AND OKM DEVELOPED THEØRETICAL SOLUTION ONLY.	D 15 PP 1Ø-11 D 25; D 37 D 4Ø I 12 P 5 I 76 P 14 I 93 P 24 I 114 P 2	--	--
UNITED KINGDOM 28	NAVY	CIPHER MACHINE	COMBINED CIPHER MACHINE	ULM	--	1944-1945	1944 OKM	NOT BROKEN; WORK STOPPED ON 31 JAN 1945	D 6 D 15 P 6 D 18 P 7 D 41 P 5 D 43 P 2 P 4	--	--
UNITED KINGDOM 29	NAVY	CIPHER	NYKO	TAUNUS	--	?-1942-?	1942 OKM	NO SUCCESS REPORTED; WORKED ON UNTIL BEGINNING OF 1944.	D 6 D 15 P 9 D 18 P 9 I 147 P 17	--	--

UNITED KINGDOM 3Ø	NAVY	SUBSTITUTION CIPHER USING 37-PLACE ALPHABET: 26 LETTERS, FIGURES Ø-9, AND DASH. THERE ARE 32 COLUMNS.	SYKO	RHÖN	--	?-1939-?	1939 OKM
							1943? OKL
							? SIM
								OKM BROKE EASILY. OKL READ ALMOST CURRENTLY. SIM READ.	D 6; D 15
									D 18
									I 1Ø9; I 147
									IF 118
									IF 15Ø6
									IF 1517
									IF 1523
									IF 1519
										--	--

UNITED KINGDOM 31	NAVY	4-LETTER ?-PART CODE WITH 32,ØØØ GROUPS; TWO VALUES TO EACH GROUP.	?	?	--	192?-1939	? OKM	READ CURRENTLY	I 147 P 3	--	--
UNITED KINGDOM 32	NAVY	4-LETTER ?-PART CODE WITH BOOK CHANGING THE 15TH OF EACH MONTH.	FLEET CODE	HAMBURG	--	?-1944-1945-?	1944 OKM ? SIS	READ FROM 15 NOV 1944 TO MAY 1945. READ BY SIS?	D 6; D 44 D 15 P 2 P 8 D 18 P 8 I 12 P 5 I 83 P 2 I 93 P 11 P 13 I 95 P 6 I 114 PP 2-3 IF 15Ø6	--	--
UNITED KINGDOM 33	NAVY	4-LETTER ?-PART CODE, ENCIPHERED.	ANGLO-FRENCH CODE	?	--	?-1944-?	1944 OKM ? SIS	NOT BROKEN BY OKM. ? SIS.	D 15 PP 4-5 IF 15Ø6	--	--
UNITED KINGDOM 34	NAVY	3-LETTER ?-PART CODE, USED BY CONVOYS OFF BRITISH EAST COAST AND IN IRISH SEA.	ECCO	HARZ	--	? - 1943	? OKM	?	D 6 D 41 P 5	--	--

TOP SECRET

CHART NO.

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 35	NAVY	3-LETTER ?-PART CODE, UNENCIPHERED. 4-LETTER, PRONOUNCEABLE INDICATORS: ADCO, AGOG, ALBA, AMID, AGUA. USED FOR INTER-ALLIED TRAFFIC IN LANDING OPERATIONS IN FRANCE.	COMBINED ASSAULT CODE	ALTONA "A"	--	1944 ONLY	1944 OKM	ALBA, AMID, AGUA READ EXTENSIVELY. AGOG COMPROMISED DURING INVASION OF FRANCE.	D 6 D 15 P 2 P 9 D 18 P 8 I 12 P 6 I 93 P 6	--	--
UNITED KINGDOM 36	NAVY	3-LETTER ?-PART CODE, UNENCIPHERED. 4-LETTER, PRONOUNCEABLE INDICATORS: BABY, BANK, BEEF, BIKE, BOLO. USED FOR INTER-ALLIED TRAFFIC IN LANDING OPERATIONS IN MEDITERRANEAN.	COMBINED ASSAULT CODE	ALTONA "B"	--	1944 ONLY	1944 OKM	BIKE, BOLO PARTLY BROKEN	D 6 D 15 P 2 P 9 D 18 P 8 D 44 P 5 I 12 P 6 I 93 P 6	--	--
UNITED KINGDOM 37	NAVY	?-PART CODE.	ODAM OR ØDAM	?	--	? - ?	? OKM	BROKEN, PARTLY THROUGH CAPTURED MATERIALS.	I 14Ø P 2	--	--
UNITED KINGDOM 38	NAVY	UNTIL 3Ø SEPT 1944, 2-LETTER ?-PART CODE CHANGING DAILY. FROM 1 OCT 1944, 3-FIGURE ?-PART CODE, CHANGING DAILY.	COFOX	HUNSRÜCK; SÜNTEL	--	?-1944-?	1944 OKM	READ CONTINUOUSLY.	D 6 D 15 PP 6-7 D 18 P 8 I 12 P 5 I 95 P 6	--	--
UNITED KINGDOM 39	NAVY	5-FIGURE CODE UNTIL 2Ø AUG 194Ø; 4-FIGURE CODE AFTER 2Ø AUG 194Ø. USED UNENCIPHERED UNTIL SPANISH WAR, THEN ENCIPHERED WITH ADDITIVE.	ADMINISTRATIVE CODE	?	--	1934 - ?	1934 OKM	READ AFTER 6 MONTHS OF WORK. ADDITIVE BROKEN DURING SPANISH WAR. BOOK CAPTURED AT BERGEN, BUT ALREADY RECOVERED.	I 12 P 2 I 147 P 3 P 1Ø T 47Ø	--	--
UNITED KINGDOM 4Ø	NAVY	4-FIGURE ?-PART CODE. FROM 1 DEC 1943 ENCIPHERED WITH STENCIL SUBTRACTOR.	NAVAL CODE NO.2	MÜNCHEN BRAUN--FOR PATROL VESSELS, ETC.; MÜNCHEN BLAU--PERSONNEL AND GENERAL.	--	1937-1945?	1938 OKM	BROKEN IN 1938. IN 1941 COMPROMISED BOOK AT TOBRUK. READ IN 1942, BUT NOT AFTER INTRODUCTION OF STENCIL SUBTRACTOR IN 1943.	D 6; D 4Ø D 25; D 41 D 18 PP 5-6 I 12 P 2 P 3 P 5 I 93 PP 6, 21, 22, 25 I 95 P 5 I 147 P 1Ø IF 118F P 1	--	--
UNITED KINGDOM 41	NAVY	4-FIGURE ?-PART CODE ENCIPHERED WITH BOOK ADDITIVE. USED BY BOTH THE UNITED KINGDOM AND THE UNITED STATES.	NAVAL CIPHER NO. 3	FRANKFURT	COMBINED CIPHER NO. 3	1941-1943	1941 OKM; PRIOR TO 1943 SIS	READ UNTIL JUNE 1943	D 6; D 41 I 12 PP 4-5 IF 118F P 1	--	--
UNITED KINGDOM 42	NAVY	4-FIGURE ?-PART CODE ENCIPHERED BY BOOK ADDITIVE.	NAVAL CIPHER NO. 4	KÖLN	--	PRIOR TO 1938 - 1945	1938 OKM	1938, BROKEN. 194Ø, READ. FROM 1943 ON, NOT READ.	D 6; D 4Ø D 41 D 18 PP 5-6 I 12 P 2 P 5 I 93 P 26 I 95 P 5 I 147 P 4 PP 15-18	--	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 43	NAVY	4-FIGURE ?-PART CODE UNTIL FEB 1944, THEN TWO 4-LETTER CODES, A AND B. ONE WAS USED FOR INDIVIDUAL DIRECTION-FINDING BEARINGS, CHANGED SEMI-MONTHLY. THE OTHER WAS USED FOR CONSOLIDATED DIRECTION-FINDING REPORTS, CHANGED MONTHLY.	?	KOLBERG A AND B	--	?-1944-?	1944 OKM	READ	D 6 D 18 P 9	--	--
UNITED KINGDOM 44	NAVY	1-PART CODE UNTIL 1 JULY 1944; 2-PART CODE THEREAFTER.	FOXO	HUNSRÜCK; SÜNTEL	--	?-1944-?	1944 OKM	READ UNTIL 1 JULY 1944 AND FROM NOV 1944 TO END OF YEAR.	D 6; D 44 D 15 P 2 P 8 D 18 P 9 I 12 P 5 I 140 P 2	--	--
UNITED KINGDOM 45	NAVY	1-PART CODE, CHANGING DAILY, UNTIL 1 APRIL 1944: 2-PART THEREAFTER, CHANGING DAILY.	LOXO	HUNSRÜCK; SÜNTEL	--	?-1944-?	1944 OKM	READ	D 6; D 44 D 15 PP 7-8 D 18 PP 8-9 I 12 P 5 I 140 P 2	--	--
UNITED KINGDOM 46	NAVY	1-PART CODE UNTIL APRIL 1944, 2-PART THEREAFTER VOCABULARY IDENTICAL WITH COFOX.	MEDOX	HUNSRÜCK; SÜNTEL	--	?-1944-?	1943 OKM	READ UNTIL AUTUMN 1944, WHEN WORK STOPPED. BOOK FOR MARCH-APRIL 1944 COMPROMISED. APRIL 1944. READ AGAIN 1945.	D 6 D 15 P 7 D 18 P 8 D 44 P 2 I 12 P 5 I 95 P 7	--	--
UNITED KINGDOM 47	NAVY	?-PART CODE	TRAXO	HUNSRÜCK; SÜNTEL	--	?-1944-?	1944 OKM	BROKEN CONTINUOUSLY,* READ UNTIL SUPERSEDED.	D 6; D 44 D 15 P 2 P 8 I 95 P 6	--	--
UNITED KINGDOM 48	NAVY	ONE-TIME PAD ENCIFHERMENT SYSTEM.	ONE-TIME PADS	ONE-TIME PADS	--	?-1944-?	1944 OKM ? OKW	NOT READ. PADS CAPTURED IN AEGEAN IN MARCH 1944.	D 15 P 4 I 31 P 6 I 93 P 6	--	--
UNITED KINGDOM 49	NAVY	ADDITIVE SYSTEM: CONTAINED 100 PAGES OF 30 LINES OF ADDITIVE. HALF WAS FOR ADDRESSES, HALF FOR TEXT. VALID FOR ABOUT 10 DAYS.	LONG SUBTRACTOR	?	--	? - 1944	? OKM	?	D 40 PP 12-13	--	--
UNITED KINGDOM 50	CONSULAR AND NAVAL	5-LETTER ?-PART CODE USED FOR ADDRESSES IN NAVAL SHORE CODE, ALSO USED FOR CONSULAR SERVICE. HAD A NAVAL SUPPLEMENT.	GOVERNMENT TELEGRAPH CODE	ALFEN		?-1940-1944-?	1940 OKM	READ CURRENTLY IN 1940. BASIC BOOK COMPROMISED 1940. NAVAL SUPPLEMENT COMPROMISED BERGEN CONSULATE 1940.	D 6 D 15 P 10 D 18 P 9 I 93 PP 17-18 I 147 P 3	--	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 51	CONSULAR AND NAVAL	4-FIGURE ?-PART CODE USED IN TRAFFIC BETWEEN SHORE STATIONS INCLUDING CONSULATES.	NAVAL SHORE CODE	STETTIN	--	?-1944-?	1944 OKM	ABOUT 2ØØ RELATIVE CODE-GROUPS OBTAINED NO ABSOLUTE VALUES.	D 6 D 15 P 1Ø D 41 PP 5-6 I 93 P 12	--	--
UNITED KINGDOM 52	NAVAL ATTACHE	4-FIGURE ?-PART CODE ENCIFHERED WITH ADDITIVE. DISCRIMINANTS VCVCV OR CVCVC.	INTERDEPARTMENTAL CIFHER	BREMEN	--	? - 194Ø-1942	1938 OKM 194Ø OKL 194Ø FA 194Ø OKW	OKM HAD NOT RECOVERED BASIC BOOK; COMPROMISED 194Ø IN NORWAY.	D 6 I 12 P 5 I 22 P 12 I 31 P 11 I 111 P 3 I 119 P 4 I 147 PP 1Ø-11, 12 I 152 P 9 I 172 P 2 P 4 IF 118A P 9	--	--
UNITED KINGDOM 53	MERCHANT NAVY	5-FIGURE 5-LETTER CODE, ENCIFHERED BY SUBSTITUTION OR UNENCIFHERED. LATER ENCIFHERED WITH ONE-TIME PADS.	BENTLEY CODE	TATRA	--	? - 1944	1944 OKM 1944 OKL	OKM READ. OKL READ EASILY.	D 6 D 15 P 9 D 18 P 9 I 93 P 12 P 17 I 119 P 5 I 152 PP 9-1Ø	--	--
UNITED KINGDOM 54	MERCHANT NAVY	4-LETTER OR 5-LETTER 2-PART CODE, UNENCIPHERED OR ENCIPHERED BY SUBSTITUTION.	MERCHANT NAVY CODE	MERCHANT NAVY CODE	--	194Ø - ?	194Ø OKM 194Ø OKL	OKM CAPTURED SEVERAL COPIES IN NORWAY, READ TRAFFIC SOON THEREATTER. OKL READ FROM EARLY IN WAR.	I 93 P 28 I 121 P 11 I 147 P 1Ø D 63	--	--
UNITED KINGDOM 55	MERCHANT NAVY	4-LETTER 4-FIGURE ?-PART CODE. ENCIFHERED WITH TABLES AND PADS.	MERCHANT SHIPS CODE; MERSIGS	GALLIEN	--	1942?-CURRENT	1942 OKM ? SIS	BOOK CAPTURED. OKM READ CURRENTLY 1 JAN 1944 TO END OF WAR. SIS READ. 2 TABLES RECONSTRUCTED.	D 6; D 43 D 15 P 5 D 18 P 7 D 41 P 5 I 12 P 5 P 7 I 95 P 5 IF 15Ø6	--	--

UNITED KINGDOM 56	AIR FORCE	3-FIGURE ?-PART CODE, ABOUT 1,ØØØ GROUPS. ENCIPHERED WITH "SYKO MACHINE.	AIR FORCE CODE	"AIR FORCE CODE"	--	? - ?	? SIS
							? OKL
								SIS READ; OKL READ "LIKE CLEAR TEXT"	I 1Ø9 P 4Ø
									IF 1513 P 2
									IF 118F F 2
										--	--

UNITED KINGDOM 57	DIPLOMATIC	?-PART CODE. INDICATOR ABABY OR ABABI.	?	?	--	?-194Ø-?	194Ø SIM	READ	IF 1524	--	--
UNITED KINGDOM 58	DIPLOMATIC	?-PART CODE.	?	ENGLISH DIP CODE W. 1938	--	? - ?	? SIS	READ. 1ØØ% COMPROMISED.	IF 15Ø6	--	--
UNITED KINGDOM 59	DIPLOMATIC	DETAILS OF SYSTEM UNKNOWN..	?	?	--	? - ?	? SIM	PARTLY RECONSTRUCTED	IF 1517	--	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM 6Ø	MILITARY	CIPHER. SAME TYPE AS SYKO. USED FOR TRAINING IN THE UNITED KINGDCM.	?	ANNA	--	? - ?	? SIM	READ	IF 1517	--	--

UNITED KINGDOM 61	MILITARY	5-LETTEP ?-PART CODE OF ABOUT 1ØØ VALUES. PREARRANGED VOCABULARY. CODE VALUES SLIDE AGAINST VOCABULARY DEPENDING ON MESSAGE INDICATOR.	CODEX	CODEX	--	? - ?	1942 SIM
							1944 OKH
								READ ONLY INFREQUENTLY BY SIM. SOLVED BY OKH.	IF 1528
									IF 5 P 8
									IF 1Ø7 P 8
										--	--

UNITED KINGDOM 62	MILITARY	2-LETTER CODE MADE OF COORDINATES OF A 676 SQUARE. DAILY CHANGING KEY.	?		--	? - ?	? SIM	READ	IF 1517	--	--
UNITED KINGDOM 64	MILITARY	4-FIGURE ?-PART CODE, ENCIPHERED.	?	?	--	? - ?	? SIM	READ	IF 1518	--	--
UNITED KINGDOM 65	AIR - LAND	3-LETTER ?-PART CODE USED FOR CROSS-CHANNEL TRAFFIC.	?	?	--	? - ?	1944 SID	?	IF 1527	--	--

UNITED KINGDOM 66	R A F	CODE FOR COMMUNICATION BETWEEN PLANES AND DROME-"ENCIPHERED BY SYKO."	?	"X"	--	? - ?	? SIS, SIM	READ	IF 1513
									IF 1523
										--	--

UNITED KINGDOM 67	AIR FORCE	CODE	?	AIRFORCE CODE C.O. 75 2	--	? - ?	? SIS	READ. COMPROMISED.	IF 15Ø6	--	--
UNITED KINGDOM 68	NAVY-AIR	TACTICAL CODE.	?	FOX	--	? - ?	? SIS	READ	IF 1527	--	--
UNITED KINGDOM 69	NAVY	TWO-LETTER THREE-LETTEP ABBREVIATION CODE.	?	SELF EVIDENCE	--	? - ?	? SIM	READ. COMPROMISED.	IF 1523	--	--
UNITED KINGDOM 7Ø	NAVY	4-FIGURE ?-PART CODE WITH 1Ø,ØØØ GROUPS. KEY ENCIPHERMENT.	?	ANGLO-AMERICAN	--	? - ?	1942 SIS AND GERMANS	READ	IF 1527	--	--
UNITED KINGDOM 71	NAVY	4-FIGURE ?-PART CODE. USED NON-REPETITIVE CIPHER KEY.	?	?	--	1941-1943	1941 SIS	READ DEPTHS. I.OT READ AFTER 1942 BECAUSE OF INDICATOR CHANGE.	IF 1527	--	--
UNITED KINGDOM 72	NAVY	ENCIPHERED CODE. 3Ø,ØØØ OR 1ØØ,ØØØ GROUPS. ENCIPHERMENT BY VOLUME 1ØØ PAGES WITH 3Ø LINES OF 5 DIGITS. GOOD FOR 3 MONTHS.	?	?	--	? - ?	? SIS	READ	IF 15Ø6	--	--
UNITED KINGDOM 73	NAVY	TACTICAL CODES WITH DAILY-CHANGING ENCIPHERING TABLES.	?	?	--	? - ?	? SIS	READ	IF 2Ø9	--	--
UNITED KINGDOM 74	NAVAL AIRCRAFT	CODE	?	NAVAL AIR CRAFT CODE NO. 2 S.P. Ø2192 2	--	? - ?	? SIS	READ. COMPROMISED.	IF 15Ø6	--	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

TOP SECRET

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED KINGDOM	75	NAVAL INTELLIGENCE	CIPHER	?	NAVAL INTELLIGENCE NO. 1 S.P. Ø23Ø7; PBLOK	--	? - ?	? SIS	READ. 1ØØ% COMPROMISED.	IF 15Ø6	--	--
UNITED KINGDOM	76	?	5-FIGURE 1-PART CODE. SIMILAR TO U.S. GREY.	?	?	--	? - ?	? SIM	READ	IF 1518	--	--
UNITED KINGDOM	77	?	4-LETTER 2-PART CODE, UNENCIPHERED.	?	?	--	? - ?	? SIM	READ	IF 1518	--	--
UNITED KINGDOM	78	DIPLOMATIC	1-PART CODE.	?	"INDIAN WORD CODE"	--	1939-194Ø	? FA	READ	I 172 P 3	--	--
UNITED KINGDOM	79	DIPLOMATIC	SUBSTITUTION TABLES FOR ENCIPHERING GOVERNMENT TELEGRAPH CODE IN EIRE TRAFFIC. 26 RANDOM ALPHABETS.	?	?	--	?-1942-?	1942 PERS Z S 1943 FA	PERS Z S READ UNTIL 1943. FA READ BERLIN AND MADRID LINKS.	I 172 PP 3-4	--	--
UNITED KINGDOM	8Ø	FOREIGN OFFICE	?-PART CODE	R CODE 1941	?	--	? - ?	? PERS Z S	BROKEN IN 6 MONTHS, 6,ØØØ GROUPS IDENTIFIED.	I 172 P 3	--	--
UNITED KINGDOM	81	AIR FORCE	AIR-GROUND CODE	"CONFIDENTIAL AIR CODE"	?	--	? - ?	? GERMANS	COMPROMISED	IF 118G PP 3-4	--	--
UNITED KINGDOM	82	?	METEOROLOGICAL "CIPHER FORMED OF 5-FIGURE GROUPS. LETTERS BEING ENCIPHERED IN THE RECOGNITION GROUP. TWO TYPES: WITH A VOWEL AT THE BEGINNING, AND WITH A CONSONANT."	?	?	--	?-1942-?	1942 OKL	8Ø% DECIPHERED	IF 118A P 5 F 1Ø	--	--
UNITED KINGDOM	83	?	DETAILS OF SYSTEM UNKNOWN.	?	AIRCRAFT MOVEMENT CODE	--	?-1942-?	1942 OKL 1943 SIS?	READ 9Ø%	IF 118A P 5 PP 9-1Ø IF 118F P 2	--	--

TOP SECRET

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED STATES 1	DIPLOMATIC	5-LETTER 1-PART CODE OF ABOUT 72,ØØØ GROUPS OF CVCVC PATTERN. UNENCIPHERED.	--	B-1; GREEN	--	? - ?	1916 PERS Z S	READ. ORIGINALLY SOLVED BY "SUSSEX NOTE" WHICH PROVIDED ABOUT 1,ØØØ GROUP CRIB. SOME 2Ø,ØØØ GROUPS RECOVERED BY 1919	DF 15	--	--
UNITED STATES 2	DIPLOMATIC	5-LETTER CODE. USED BY COL. HOUSE IN TRAFFIC TO WASHINGTON.	--	B-2; COL. HOUSE'S GREEN & BLUE CODE	--	1916-192Ø	? PERS Z S	NOT READ.	DF 15	--	--

UNITED STATES 3	DIPLOMATIC	5-LETTER 1-PART CODE OF ABOUT 59,ØØØ GROUPS. UNENCIPHERED. STILL IN USE IN 1942.	--	B-3; GRAY CODE	--	1918-1943	1919 PERS Z S
							1919 SIM
								READ CURRENTLY AFTER 1919. SOLVED ON BASIS OF PLAIN TEXT OBTAINED FROM EMBASSY IN STOCKHOLM.	DF 15;
									IF 1518
										--	--

UNITED STATES 4	DIPLOMATIC	5-LETTER 1-PART CODE WITH GROUP PATTERN CVCCV. ABOUT 14,4ØØ GROUPS.	--	B-5	--	1919 - ?	1919 PERS Z S	READ BY CRYPTANALYTIC COMPROMISE.	DF 15	--	--
UNITED STATES 5	DIPLOMATIC	5-LETTER 2-PART CODE, ENCIPHERED.	--	B-6A; A-1; ACI	--	192Ø-1944	1924 PERS Z S 1941 OKW	8Ø% RECONSTRUCTED IN 1939. 1ØØ% COMPROMISED IN 1941.	I 22; DF 15	--	--
UNITED STATES 6	DIPLOMATIC	5-LETTER 2-PART CODE, ENCIPHERED.	--	B-6B; B-1	--	192Ø-1942-1944?	194Ø PERS Z S	PRESUMABLY NOT READ	I 22; DF 15	--	--
UNITED STATES 7	DIPLOMATIC	5-LETTER 2-PART CODE, UNENCIPHERED.	--	B-7; C-1	--	192Ø-1942?	1937 PERS Z S	READ	DF 15; I 22 T 371; T 372 D 3C	--	--
UNITED STATES 8	DIPLOMATIC	5-LETTER 2-PART CODE OF "ABOUT 125,Ø58 GROUPS."	--	B-8; AM-8; BROWN	--	? - 1938?	1938 PERS Z S 1941 OKW ? FA?	READ CURRENTLY AFTER 1933. 1ØØ% COMPROMISED IN 1941.	DF 15; I 22 TF 1Ø; IF 15 I 143:	--	--

UNITED STATES 9	DIPLOMATIC	5-LETTER CODE IN 3 VOLUMES. "MESSAGES WERE ENCODED IN 3 PARTS, ONE PART FROM EACH VOLUME."	--	BROWN	--	? - ?	? SIM	READ. COMPROMISED.	IF 1518
									IF 1524
										--	--

UNITED STATES 1Ø	DIPLOMATIC	5-FIGURE 1-PART CODE OF ABOUT 8,ØØØ GROUPS. UNENCIPHERED.	--	Z-1; BLUE CODE	--	?-(1916)-?	1916 PERS Z S	READ. COMPROMISED BY "SUSSEX NOTE"	DF 15	--	--
UNITED STATES 11	DIPLOMATIC	5-FIGURE 1-PART CODE OF ABOUT 72,ØØØ GROUPS. UNENCIPHERED. USED MAINLY BY CHARGE D'AFFAIRES AT CONSTANTINOPLE WITH WASHINGTON, BERLIN, VIENNA, ETC.	--	Z-2	--	? - ?	? PERS Z S	READ. SOLVED BY NOTING STATISTICAL RESEMBLANCE TO B-1 WHICH WAS READ.	DF 15	--	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED STATES	12	DIPLOMATIC	5-FIGURE 1-PART CODE OF ABOUT 47,ØØØ GROUPS. UNENCIPHERED.	--	Z-3; RED	--	? - ?	? PERS Z S	READ. LATER COMPROMISED AND PHOTOGRAPHED AT FRANKFORT AM MAIN	DF 15	--	--
UNITED STATES	13	DIPLOMATIC	5-FIGURE 1-PART CODE OF ABOUT 24,ØØØ GROUPS. UNENCIPHERED.	--	Z-7	--	1918 - ?	1919 PERS Z S	PARTIALLY SOLVED	DF 15	--	--
UNITED STATES	14	DIPLOMATIC	STRIP CIPHER, NO STRIP ELIMINATION, GENERATRIX SPLIT 15-15.	--	Ø-2	--	1942-1944?	1942 PERS Z S 1942 OKW, POSSIBLY OKH ? FA	READ CURRENTLY 1943-1944	I 2; I 22 I 25; I 31 I 54; I 84 I 89; I 176 I 79; I 13 I 39; I 46 I 58; IF 51 IF 175; TF 1Ø I 25; I 54	--	--
UNITED STATES	15	DIPLOMATIC	DOUBLE TRANSPOSITION SYSTEM USED BY "COORDINATOR OF INFORMATION, WASHINGTON."	--	DOUBLE TRANSPOSITION	--	? - ?	? PERS Z S	PRESUMABLY NOT READ.	I 22	--	--
UNITED STATES	16	MILITARY ATTACHE	5-LETTER CODE, ENCIPHERED WITH 1Ø TABLES OF 2Ø RANDOM ALPHABETS, VOWEL FOR VOWEL, CONSONANT FOR CONSONANT.	--	?	--	?-1942-?	1942 SIM	READ. PHOTOSTAT COPIES OF CODE BOOK RECEIVED FROM HUNGARY. TABLES RECONSTRUCTED BY SIM.	IF 1524	--	--
UNITED STATES	17	MILITARY ATTACHE	5-LETTER CODE, ENCIPHERED.		MI-3; WAR DEPARTMENT CONFIDENTIAL CODE NO. 2	--	?-1942-?	1942 PERS Z S	1ØØ% COMPROMISED	DF 15	--	--
UNITED STATES	18	MILITARY ATTACHE	5-LETTER CODE, UNENCIPHERED.	--	MI-1	--	?-1942-?	1942 PERS Z S	1ØØ% COMPROMISED	DF 15	--	--
UNITED STATES	19	MILITARY ATTACHE	DOUBLE TRANSPOSITION, USING INCOMPLETE RECTANGLES.	--	MILITARY ATTACHE'S EMERGENCY CIPHER	--	?-1942-?	1942 SIM	READ	IF 1519 I 31	--	(PROBABLY RECOVERED BY ANAGRAMMING)
UNITED STATES	2Ø	ARMY	CIPHER MACHINE	--	AM 2; AMERICAN "BIG" MACHINE	--	1941 - ?	? OKL ? OKH? ? OKM?	NOT READ	I 74; I 112 I 113; I 1Ø9 I 119; D 7	--	--
UNITED STATES	21	ARMY	HAGELIN CIPHER MACHINE.	--	AM-1; M-2Ø9	--	1942 - ?	1943 OKH 1943 OKM 1944 OKL? ? OKW ? PERS Z S	1Ø%-2Ø% OF ARMY TRAFFIC INTERCEPTED WAS READ	I 23; I 46 I 45; I 6Ø I 76; I 89 I 142; I 175 I 31; I 35 I 93; I 93 I 6; I 1Ø9 I 119; IF 1Ø7 IF 127; I 112 I 22; I 5Ø I 95; I 147	--	--

TOP SECRET

CHART NO. 1-2

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED STATES 22	ARMY	5-LETTER 1-PART CODE, UNENCIPHERED.	--	WAR TELEGRAPH CODE 1919	--	? - ?	1942? PERS Z S	READ: COMPROMISED BY PHOTOSTAT COPY	DF 15 P 3	--	--
UNITED STATES 23	ARMY	5-LETTER 2-PART CODE OF ABOUT 14Ø,ØØØ GROUPS. UNENCIPHERED.	--	TELWA	--	1943 - ?	1944 OKL	READ 1Ø% IN 1944, CURRENTLY IN 1945	I 112; IF 175	--	--
UNITED STATES 24	ARMY	4-LETTER OR 4-FIGURE 2-PART CODE.	--	D.F.C.	--	194Ø-1944?	1944 OKH	READ OCCASIONALLY. COMPROMISED.	I 76; IF 1Ø7 IF 127	--	--
UNITED STATES 25	ARMY	DOUBLE TRANSPOSITION.	--	DOUBLE TRANSPOSITION	--	?-1945-?	1945 OKH	READ OCCASIONALLY.	I 8Ø; IF 1Ø7 I 22; IF 175	--	--
UNITED STATES 26	ARMY-AIR	STRIP CIPHER, NO STRIP ELIMINATION.	--	"CENEB"	--	? - ?	1942 OKL	READ UNTIL STRIP ELIMINATION WAS INTRODUCED IN 1943.	I 112; I 119 IF 175	--	--

UNITED STATES 27	ARMY-AIR	POLYALPHABETIC SUBSTITUTION USING 25 DISCS.	--	"STRIP"; "URSAL"; "COAL"	--	?-1942-?	1942 OKH
							1942 OKL
								READ	I 112; I 113
									I 142; I 119
									IF 1Ø7;
									IF 175
										--	--

UNITED STATES 28	ARMY-AIR	DIGRAPHIC CODE CHART WITH CHANGEABLE COORDINATES.	--	SLIDEX	--	? - 1945	? OKH ? OKL	READ CURRENTLY WITH 1-3 HOURS LAG.	I 76; I 8Ø I 1Ø9; I 174 IF 1Ø7; IF 127	--	--
UNITED STATES 29	AIR	ENCIPHERED SPEECH DEVICE.	--	"MUSTANG TIGERSTEDT"	--	? - ?	1945 OKW	DEVICE CAPTURED FROM MUSTANG PLANE. THEORETICAL SOLUTION ONLY.	I 17; I 31 I 44; I 92 I 96; I 1Ø4 I 127; D 68 I 57; I 2Ø I 71; I 38 I 186; I 19Ø	--	--
UNITED STATES 3Ø	AIR	CIPHER MACHINE.	--	AM 2; AMERICAN "BIG" MACHINE	--	? - ?	? OKL ? OKH? ? OKM?	NOT READ.	I 74; I 1Ø9 I 112; I 113 I 119; D 7	--	--
UNITED STATES 31	AIR	HAGELIN CIPHER DEVICE	--	AM-1; M 2Ø9	--	1942 - ?	SEE UNITED STATES 21	1Ø%-2Ø%			
UNITED STATES 32	AIR	2-LETTER CODE. DAILY CHANGE OF CODE.	--	BOMBER CODE	--	?-1944-?	1944 OKL	READ CURRENTLY	I 1Ø9	--	--
UNITED STATES 33	COMBINED UNITED STATES-GREAT BRITAIN JOINT ARMY-AIR-NAVY	CIPHER MACHINE.	--	"COMBINED CIPHER MACHINE"	--	1944 - ?	1944 OKM	NOT READ	DF 3; D 15 D 17; D 18 D 43; I 93	--	--

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN		SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
				COUNTRY OF ORIGIN	AXIS	U.S.A.						
UNITED STATES	34	ARMY-AIR-NAVY	HAGELIN CIPHER MACHINE.	--	AM-1; M-2ø9	--	1942 - ?	(SEE UNITED STATES 21)	READ	I 23; I 46 I 48; I 6ø I 76; I 8ø I 142; I 175 I 31; I 35 I 33; I 93 I 5; I 1ø9 I 119; I 112 IF 1ø7; IF 127	--	--
UNITED STATES	35	ARMY-NAVY	3-LETTER 2-PART CODE, UNENCIPHERED. FOR JOINT ARMY-NAVY ASSAULT OPERATIONS. 4-LETTER PRONOUNCEABLE INDICATOR.	--	"COMBINED" ASSAULT CODE	--	1944 - ?	1944 OKM	READ "EXTENSIVELY." ALSO COMPROMISED BY CAPTURE.	D 15; D 18 D 44	--	--
UNITED STATES	36	NAVY	CIPHER MACHINE.	--	AM-2?; "BIG" MACHINE	--	? - ?	? OKL ? OKH? ? OKM?	NOT READ	I 74; I 1ø9 I 112; I 113 I 119; D 7	--	--
UNITED STATES	37	NAVY	HAGELIN CIPHER MACHINE	--	AM-1; M-2ø9	--	1942 - ?	(SEE UNITED STATES 21)	READ--ONLY A FEW DAY'S TRAFFIC, DUE TO LACK OF DEPTH	I 6; I 35 I 92; I 95	--	--
UNITED STATES	38	NAVY	STRIP CIPHER	--	"DUPYH"	--	?-1942-?	1942 OKM	READ. COMPROMISED STRIPS AND SETTINGS RECEIVED FROM JAPANESE.	I 12; I 93	--	--

~~TOP SECRET~~

~~TOP SECRET~~

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
URUGUAY 1	DIPLOMATIC	4-LETTER 1-PART CODE WITH 2,142 GROUPS. INTERSPERSED PLAIN TEXT AND PLAIN TEXT ENCIPHERMENT. 1ØØ-PLACE TABLES USED TO SUBSTITUTE 2-FIGURE GROUPS FOR LETTERS OR SYLLABLES.	?	?	(URA)	(? - CURRENT)	? PERS Z S	COMPLETELY READ	D 16, REPORT 2, P 5	(ALMOST COMPLETELY READABLE.)	--
URUGUAY 2	DIPLOMATIC	5-FIGURE OR 4-FIGURE CODE.	?	?	?	? - ?	? SIM	1ØØ% COMPROMISED	IF 1517	(UNIDENTIFIED)	--
URUGUAY 3	DIPLOMATIC	?-PART CODE WITH DIGRAPHIC FIGURE ENCIPHERMENT.	?	?	?	? - 1927 - ?	? PERS Z S	?	D 16, REPORT 1, P 4	(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET~~

73

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
VATICAN 1	?	4-FIGURL ?-PART CODE ENCIPHERED WITH A TABLE.	?	VAT. T. B. 2	--	?-1938-1939-?	1939 PERS Z S 1939 RLM/FA	TABLES SOLVED. RECOVERED ABOUT 15% OF VALUES.	T 93	--	--

VATICAN 2	?	3-LETTER 1-PART CODE. FIRST TWO ELEMENTS INDICATE PAGE AND LAST ELEMENT INDICATES GROUP. LETTERS "Y" AND "Z" USED AS DUDS OR AS SPELLER INDICATORS.	?	"NULLE YZ"	--	?-1943-?	1943 SIM	4ØØ-5ØØ GROUPS RECOVERED.	IF 1517 P 5
									IF 1526 P 11
										---	--

VATICAN 3	?	3-LETTER 1-PART CODE. FIRST TWO ELEMENTS INDICATE PAGE AND LAST ELEMENT INDICATES GROUP. LETTER "E" USED AS DUD OR AS SPELLER INDICATOR.	?	"NULLA E"	--	?-1944-?	1944 SID, SIM	READ	IF 1526 P 1Ø
									IF 1517
										--	--

VATICAN 4	?	3-LETTER ?-PART CODE.	?	VATIKAN CODE II 441	--	? - ?	? ?	RECOVERED 3Ø%-5Ø%	T 2195	--	--
VENEZUELA 1	DIPLOMATIC	4-LETTER 1-PART CODE. 12,ØØØ GROUPS. INTERSPERSED ENCIPHERED PLAIN TEXT.	?	?	(VZB)	(?-1941-CURRENT)	1941 PERS Z S	?	D 16, REPORT 2, P 5 T 3Ø1Ø	(95% READABLE)	--
VENEZULA 2	?	4-FIGURE ?-PART CODE.	?	?	?	? - ?	? ?	RECOVERED LESS THAN 3%	T 3Ø14	(UNKNOWN)	--
VENEZUELA 3	DIPLOMATIC	POLYALPHABETIC SUBSTITUTION CIPHER WITH 5 TO 1Ø ALPHABETS.	?	?	(VZA)	(?-1941-CURRENT)	1941 PERS Z S	READ	D 16, REPORT 2, P 5	(1ØØ% READABLE)	--

~~TOP SECRET~~

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
YUGOSLAVIA- 1 CROATIA	DIPLOMATIC	5-LETTER 1-PART CODE ENCIPHERED BY SUBSTITUTION. USED BY THE FOREIGN OFFICE. DATE GIVEN AT END OF MESSAGE PRECEDED BY S OR SVT.	?	C 1	?	?-1944-?	1944 SID	ENCIPHERMENT SYSTEM KNOWN. PERHAPS READ.	T 16Ø4	(UNKNOWN)	--
YUGOSLAVIA 2	(DIPLOMATIC)	(4-LETTER 2-PART CODE UNENCIPHERED.)	?	?	(YOA)	(1935-CURRENT)	1944 OKW	READ	T 797	(GCCS BROKE CODE. ASA NOW READING 1ØØ%. VERY LIGHT TRAFFIC.)	--
YUGOSLAVIA- 3 CROATIA	DIPLOMATIC	5-FIGURE 1-PART CODE. APPROXIMATELY 3Ø,ØØØ GROUPS. CODE GROUPS SPLIT INTO SINGLE DIGITS AND DIGRAPHS, EACH SEPARATELY ENCIPHERED.	?	?	?	?-1943-1944-?	1943 SIM	COMPROMISED. READ JUNE 1944 --SEPT 1944.	IF 1525 PP 5-6	(UNKNOWN)	--
YUGOSLAVIA- 4 MICHAILOVITCH AND TITO	DIPLOMATIC AND CONSULAR	5-FIGURE ?-PART CODE. ABOUT 3Ø,ØØØ-4Ø,ØØØ GROUPS. LATER REPAGINATED. ENCIPHER TABLES USED IN TWO DIFFERENT WAYS. (SIMILAR TO ITEM 2. VARIATION OF YOA ENCIPHERMENT.)	?	?	?	1934-1944-?	1944 SIM AND PREDECESSOR	PLAIN CODE COMPROMISED. ENCIPHERMENTS NOT READ.	IF 1525 PP 2, 5, 6	(UNKNOWN)	--
YUGOSLAVIA 5	DIPLOMATIC AND MILITARY ATTACHE	5-FIGURE PARTIALLY 1-PART CODE. APPROXIMATELY 3Ø,ØØØ GROUPS. PAGES RENUMBERED PERIODICALLY. CLEAR TEXT IN SERBIAN. ENCIPHERED AFTER 1921.	?	?	?	1918-1934	? SIM AND PREDECESSOR	PROBABLY READ.	IF 1525 PP 2, 3	(UNKNOWN)	--
YUGOSLAVIA- 6 SERBIA	DIPLOMATIC?	5-FIGURE ?-PART CODE. ENCIPHERED BY SUBSTITUTION	?	?	?	193Ø - ?	1929 OR 193Ø PERS Z S	?	I 22 P 2	(UNKNOWN)	--
YUGOSLAVIA 7	DIPLOMATIC?	5-FIGURE ?-PART CODE. ENCIPHERED BY DIGRAPHIC SUBSTITUTION WITH TABLES CONSISTING OF 1ØØ DIGRAPHS.	?	?	?	1938-1943-?	1938, 1943 PERS Z S	READ	I 22 P 9	(UNKNOWN)	--
YUGOSLAVIA 8	DIPLOMATIC?	5-FIGURE PROBABLY 1-PART CODE.	?	STOCKHOLM ØØ1-249	?	? - ?	? PERS Z S	APPROXIMATELY 15% RECOVERED	T 2138	(UNKNOWN)	--
YUGOSLAVIA 9	DIPLOMATIC?	5-FIGURE 1-PART CODE.	?	S D III	?	? - ?	? PERS Z S	RECOVERED LESS THAN 3%	T 2119	(UNKNOWN)	--
YUGOSLAVIA 1Ø	DIPLOMATIC	5-FIGURE 1-PART CODE.	?	37 IX D LESART: 345-12	?	? - ?	? PERS Z S	APPROXIMATELY 35% RECOVERED	T 2238	(UNKNOWN)	--
YUGOSLAVIA 11	DIPLOMATIC	4-FIGURE ?-PART CODE. PROBABLY REPAGINATED TO 5-FIGURE.	?	SERBIEN I	?	?-1924-?	? PERS Z S	WORKED ON	T 2117	(UNIDENTIFIED)	--
YUGOSLAVIA 12 CROATIA	DIPLOMATIC	?-FIGURE ?-PART CODE. "CHILDISH" ENCIPHERMENT.	?	?	?	? - ?	PRIOR TO 1941 SIM	COMPROMISED	IF 1517 P 4	(UNIDENTIFIED)	--
YUGOSLAVIA 13 CROATIA	DIPLOMATIC?	PROBABLY CONSISTED OF A SQUARE 1Ø X 1Ø WITH KEYS FOR EVERY MESSAGE.	?	?	?	? - ?	1942 SIM	READ	IF 1524 P 4	(UNKNOWN)	--
YUGOSLAVIA 14	MILITARY ATTACHE	2-PART CODE.	?	22? AM BOOK	?	1921-1927	1923? SIM	READ FOR 5 YEARS.	IF 1525 P 4	(UNKNOWN)	--
YUGOSLAVIA 15	MILITARY ATTACHE	SIMILAR TO ITEM 12, BUT MORE COMPLICATED PAGE NUMBERING WHICH CHANGED YEARLY. ENCIPHERMENT SIMILAR TO LATER SYSTEM OF FOREIGN OFFICE AND DIPLOMATIC MISSIONS BUT OF SIMPLER CONSTRUCTION.	?	?	?	1927 - ?	? SIM	?	IF 1525 P 4	(UNKNOWN)	--

TOP SECRET

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS

AS LEARNED FROM TICOM SOURCES

(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
YUGOSLAVIA- 16 CROATIA	ARMY	ENIGMA K -- 3 WHEELS AND NO STECKER.	?	?	?	1941-1942-?	1941 OR 1942 OKW	WIRINGS COMPROMISED 1941 OR 1942. READ 1ØØ%.	I 92 P 2 I 58 P 3	(NOT KNOWN TO HAVE BEEN USED.)	--
YUGOSLAVIA- 17 TITO	ARMY	FIELD CODE OF THE 26 X 26 SQUARE TYPE. CHANGEABLE ALPHABET COORDINATES.	?	?	?	? - ?	AFTER APRIL 1941 SIM	BROKEN AND RECONSTRUCTED	IF 1517 P 5	(UNKNOWN)	--
YUGOSLAVIA 18	ARMY	CODE OF THE 26 X 26 SQUARE TYPE. SIMILAR TO ITEM 17. TABLES CHANGED EVERY TWO OR THREE MONTHS.	?	?	?	?-1941-?	BEFORE 1941 SIM	READ	IF 1519 P 3	(UNKNOWN)	--
YUGOSLAVIA 19	ARMY	FIELD CODES OF THE 1Ø X 1Ø SQUARE TYPE.	?	?	?	? - ?	? SIM	?	IF 1525 P 6	(UNKNOWN)	--

YUGOSLAVIA- 2Ø CROATIA	ARMY	DIGRAPHIC SUBSTITUTION, 2-SQUARE CHECKERBOARD. USED IN THE FIELD.	?	?	?	1941-1943	AFTER APRIL 1941 SIM	EASILY READ	IF 1517 P 4
									IF 152Ø P 5
									IF 1512 P 4?
										(UNKNOWN)	--

YUGOSLAVIA 21	ARMY	DOUBLE PLAYFAIR.	?	?	?	? - ?	? SIM	?	IF 1525 P 6	(UNKNOWN)	--
YUGOSLAVIA- 22 CROATIA	AIR	REVERSED PLAIN TEXT IN UNALTERED SEQUENCE.	?	?	?	?-194Ø-1943-?	? SIM	?	IF 1525 P 6	(UNKNOWN)	--
YUGOSLAVIA- 23 MICHAILOVITCH	MILITARY	?-LETTER CODE OF THE 26 X 26 SQUARE TYPE. SPACES CONTAINED DIGRAPHS, TRIGRAPHS, AND WORDS IN FULL.	?	?	?	? - ?	AFTER JUNE 1943 SIM	READ	IF 152Ø P 4	(UNKNOWN)	--
YUGOSLAVIA 24	ARMY-NAVY	4-FIGURE 1-PART CODE.	?	?	?	? - ?	? OKW	COMPROMISED 1ØØ%	T 962	(UNKNOWN)	--

YUGOSLAVIA- 25 MICHAILOVITCH	MILITARY	DOUBLE TRANSPOSITION CIPHER SYSTEM WITH SAME KEY FOR BOTH RECTANGLES. RECTANGLE WIDTH USUALLY 12 OR 13. NO CALL SIGNS USED. KEYS WERE ANNOUNCED THEN FOLLOWED COVER NAMES OF ADDRESSES.	?	JRC	(YOB)	(1943-1944)	? OKH
							? SIM
							? PERS Z S
								READ BY GERMANS AND ITALIANS	I 69 P 23
									D 3Ø PP 1-11
									IF 152Ø P 4
									IF 1525 P 6
										(TRAFFIC RECEIVED. WORKED ON FOR 1-2 MONTHS 1944. NO SUCCESS.)	--

YUGOSLAVIA- 26 TITO	MILITARY	DOUBLE TRANSPOSITION.	?	?	?	? - ?	? OKH	READ	I 113 P 5	(UNKNOWN)	--
YUGOSLAVIA- 27 MICHAILOVITCH	MILITARY	SIMPLE TRANSPOSITION CIPHER ON A PATTERN OF AN INCOMPLETE RECTANGLE, WITH KEY VARYING FROM 13-21. USED IN THE FIELD.	?	?	?	? - ?	1944 SID	PROBABLY READ	IF 1525 P 6	(UNKNOWN)	--
YUGOSLAVIA- 28 MICHAILOVITCH	MILITARY	POLYALPHABETIC SUBSTITUTION CIPHER WITH 5? ALPHABETS.	?	?	?	? - ?	? SIM	READ	IF 152Ø P 4	(UNKNOWN)	--
YUGOSLAVIA- 29 TITO	MILITARY	POLYALPHABETIC SUBSTITUTION, 1 OR 2 DIGITS PER LETTER, WITH 3, 4, 5, 6, 9, 11, OR 19 ALPHABETS. KEY CHANGED EVERY 5 DAYS. USED BY DIVISIONS AND BRIGADES.	?	?	?	?-1944-?	? OKH	?	I 69 P 5 I 52 P 5	(UNKNOWN)	--
YUGOSLAVIA- 3Ø TITO	MILITARY	2-DIGIT SUBSTITUTION BY MEANS OF 1Ø X 1Ø ENCIPHERING SQUARE FORMED FROM A 1Ø-LETTER KEYWORD WRITTEN IN VERTICALLY.	?	?	?	? - ?	? OKH	?	I 69 PP 22,23	(UNKNOWN)	--

TOP SECRET

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
YUGOSLAVIA- 31 TITO	MILITARY	2-DIGIT SUBSTITUTION BY MEANS OF 8 x 8 ENCIPHERING SQUARE WITH 8-LETTER KEYWORD WRITTEN IN HORIZONTALLY. PROBABLY USED BY 11TH DIVISION OF 5TH CORPS.	?	?	?	? - ?	? OKH	?	I 69 P 23	(UNKNOWN)	--
YUGOSLAVIA- 32 TITO	MILITARY AND (DIPLOMATIC)	MONOALPHABETIC SUBSTITUTION, 2 DIGITS PER LETTER, AND ALSO AUXILIARY 3-DIGIT CODE, ALL SUPERENCIPHERED WITH NUMERICAL RUNNING ADDITIVE CONVERTED FROM THE TEXT OF A BOOK. USED ABOVE DIVISION.	NOVA ŠIFRA	?	?	1944-1945	? OKH	NOT BROKEN BUT COULD HAVE BEEN WITH MORE TRAFFIC	I 69 PP 16-2Ø	(IN EFFECT THIS IS A NON-RANDOM ONE-TIME PAD ENCIPHERMENT AND BECAUSE IT IS NON-RANDOM IT IS THEORETICALLY SOLVABLE. ASA IS NOT WORKING ON THIS PROBLEM.)	--
YUGOSLAVIA- 33 TITO	MILITARY?	BELIEVED TO BE SIMILAR TO ITEM 32. MESSAGES TO MOSCOW HAD A SPECIAL GROUP 66666, SOMETIMES 11111 66666 EITHER AT THE BEGINNING OR AT THE END OF THE MESSAGE. FIRST GROUP OF THE ACTUAL MESSAGE USUALLY REPEATED AFTER ADDITION OF A CERTAIN NUMBER.	?	?	?	?-1944-?	? OKH	NOT SOLVED	I 69 P 3Ø	(UNKNOWN)	--
YUGOSLAVIA- 34 TITO	MILITARY	MONOALPHABETIC SUBSTITUTION--LETTER FOR LETTER OR 2 DIGITS PER LETTER. USED BY BRIGADE AND UNITS.	?	?	?	?-1944-?	? OKH	READ	I 69 P 2 I 52 P 5	(UNKNOWN)	--
YUGOSLAVIA- 35 TITO	MILITARY	MONOALPHABETIC SUBSTITUTION, 2 DIGITS WITH 5-DIGIT REPEATING ADDITIVE. USED BELOW DIVISION LEVEL.	?	?	?	?-1944-?	? OKH	?	I 69 PP 2-3	(UNKNOWN)	--
YUGOSLAVIA- 36 TITO	MILITARY	MONOALPHABETIC SUBSTITUTION, 2 DIGITS PER LETTER, WITH NULLS INSERTED IN EVERY 5TH AND 6TH GROUPS AND MULTIPLES THEREOF, AND WITH 15-DIGIT REPEATING ADDITIVE. KEY CHANGED EVERY 7 TO 14 DAYS. USED BELOW DIVISION.	?	?	?	?-1944-?	? OKH	?	I 69 PP 4-5	(UNKNOWN)	--
YUGOSLAVIA- 37 MICHAILOVITCH	MILITARY	MONOALPHABETIC SUBSTITUTION, 1 OR 2 DIGITS FOR SINGLE LETTERS, WITH SHORT REPEATING ADDITIVE. BASED ON A KEYWORD.	?	?	?	?-1943-1944-?	? OKH	READ	I 51 P 3 I 52 P 5	(UNKNOWN)	--
YUGOSLAVIA- 38 TITO	MILITARY	MONOALPHABETIC SUBSTITUTION, 2 DIGITS PER LETTER, ENCIPHERED WITH REPEATING ADDITIVE FORMED MATHEMATICALLY FROM AN ADDITIVE SQUARE OF 3ØØ DIGITS.	?	?	?	?-1944-?	? OKH	?	I 69 P 2Ø	(UNKNOWN)	--
YUGOSLAVIA- 39 TITO	MILITARY	MIXED SUBSTITUTION ENCIPHERED BY MEANS OF ADDITIVESFROM A FIGURE TABLE.	?	?	?	? - ?	? OKH	?	I 52 P 5	(UNKNOWN)	--
YUGOSLAVIA- 4Ø TITO	MILITARY	VARIABLE SUBSTITUTION WITH SHORT REPEATING ADDITIVE. CIPHER CHANGED EVERY MONTH. USED ABOVE DIVISION, LATER BY UNITS.	?	?	?	?-1944-?	? OKH	READ	I 68 PP 3-15	(UNKNOWN)	--
YUGOSLAVIA- 41 TITO	MILITARY	VARIABLE SUBSTITUTION WITH ENCIPHERING TABLE.	?	?	?	?-1944-?	? OKH	?	I 69, ITEM 13	(UNKNOWN)	--
YUGOSLAVIA-42 TITO	MILITARY	18ØØ GROUP CODE IN 3Ø x 6Ø RECTANGLE SUPERENCIPHERED BY "ENCIPHERING ROWS."	?	?	?	? - ?	? OKL	READ EXTENSIVELY	I 121 P 9	(UNKNOWN)	--
YUGOSLAVIA 43	?	5-LETTER ?-PART CODE.	?	?	?	? - ?	? GERMANS	?	T 2122	(UNKNOWN)	--

RESULTS OF EUROPEAN AXIS CRYPTANALYSIS
AS LEARNED FROM TICOM SOURCES
(WITH ANNOTATIONS FROM ARMY SECURITY AGENCY SOURCES IN PARENTHESES)

~~TOP SECRET~~

COUNTRY OF ORIGIN	SERVICE	DESCRIPTION OF SYSTEM	NAME OF SYSTEM			DATES OF USE	WHEN ATTACKED AND BY WHOM	RESULTS	TICOM REFERENCE	STATUS OF THE SYSTEM AT ASA	REMARKS
			COUNTRY OF ORIGIN	AXIS	U.S.A.						
YUGOSLAVIA 44	?	5-FIGURE PROBABLY 1-PART CODE.	?	STOCKHOLM 25Ø-499	?	? - ?	? GERMANS	APPROXIMATELY 2Ø% RECOVERED	T 2139	(UNKNOWN)	--
YUGOSLAVIA 45	?	5-FIGURE CODE PROBABLY 1-PART.	?	?	?	? - ?	? GERMANS	RECOVERED LESS THAN 2Ø%	T 2124	(UNKNOWN)	--
YUGOSLAVIA 46	?	5-FIGURE ?-PART CODE WITH ABOUT 3Ø,ØØØ-4Ø,ØØØ GROUPS. CLEAR TEXT IN SERBIAN.	?	?	?	1934 - ?	? SIM	COMPROMISED	IF 1525 P 2	(UNKNOWN)	--
YUGOSLAVIA-SERBIA 47	?	5-FIGURE PROBABLY 1-PART CODE.	?	S D IV	?	? - ?	? GERMANS	APPROXIMATELY 25% RECOVERED	T 2123	(UNKNOWN)	--
YUGOSLAVIA 48	?	5-FIGURE 1-PART CODE.	?	?	?	1941 - ?	? ?	1ØØ% COMPROMISED	T 2576	(UNKNOWN)	--
YUGOSLAVIA 49	?	4-FIGURE PROBABLY 1-PART CODE.	?	?	?	? - ?	? GERMANS	APPROXIMATELY 15% RECOVERED	T 2126	(UNKNOWN)	--
YUGOSLAVIA 5Ø	?	4-FIGURE PROBABLY 1-PART CODE.	?	S D V. II	?	? - ?	? GERMANS	APPROXIMATELY 15% RECOVERED	T 2118	(UNKNOWN)	--
YUGOSLAVIA 51	?	DETAILS OF SYSTEM UNKNOWN.	?	S D V. I	?	? - ?	? GERMANS	WORKED ON	T 2123	(UNKNOWN)	--
YUGOSLAVIA 52	?	DETAILS OF SYSTEM UNKNOWN.	?	HOF CODE	?	? - ?	? GERMANS	?	T 2123	(UNKNOWN)	--
YUGOSLAVIA-SERBIA 53	?	DETAILS OF SYSTEM UNKNOWN.	?	S D VI	?	?-1933-?	? GERMANS	WORKED ON	T 2123	(UNKNOWN)	--
YUGOSLAVIA-CROATIA 54	?	CIPHER TRANSPOSITION WITH INCOMPLETE RECTANGLES.	?	?	?	? - ?	AFTER APRIL 1941 SIM	RECONSTRUCTED	IF 1517 P 4	(UNKNOWN)	--
YUGOSLAVIA-SERBIA 55	MILITARY	"TABLE OF 28 X 28, ABOUT 5ØØ WORDS. TRANSMITTED IN 5-LETTER GROUPS. DAILY KEY."	?	?	?	? - ?	? SIM	"HAS BEEN RECONSTRUCTED."	IF 118C, P 4	(UNKNOWN)	--
YUGOSLAVIA-SERBIA 56	MILITARY	SIMPLE TRANSPOSITION WITH VARIABLE LENGTH NUMERICAL KEY. ALL MESSAGES BEGAN WITH BRX CITIRI. INCOMPLETE RECTANGLES.	?	?	?	? - ?	? SIM	READABLE	IF 118C, P 4	(UNKNOWN)	--

~~TOP SECRET~~

~~TOP SECRET CREAM~~

~~TOP SECRET CREAM~~