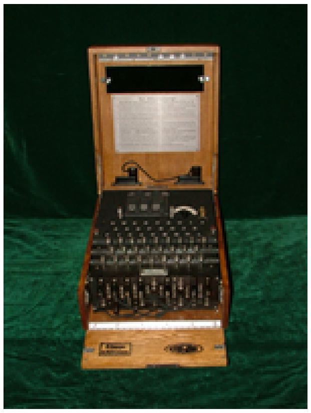
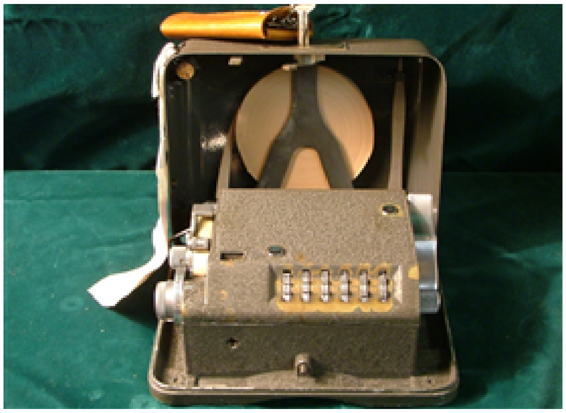
NATIONAL CRYPTOLOGIC MUSEUM



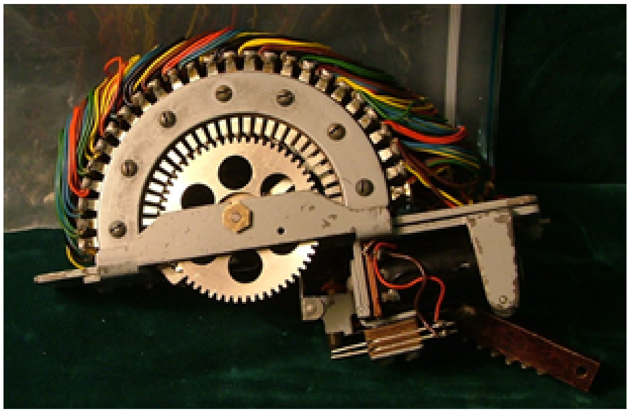
Enigma

Originally invented by Arthur Scherbius in the 1920's, the Enigma machine was adopted and adapted by the German military to send encrypted messages during WWII. This electromechanical device would use 3-4 wired rotors to scramble messages.



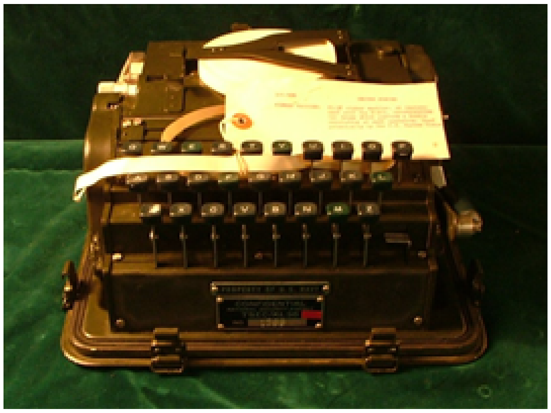
Hagelin C-38

The C-38 was designed and built by Boris Hagelin and his company AB Cryptoteknik in 1938. The design was sold to the US Military in 1940 where is was renamed the M-209 (Army) and CSP-1500 (Navy). These devices proved to be the most used tactical field cipher machines for the US Military.



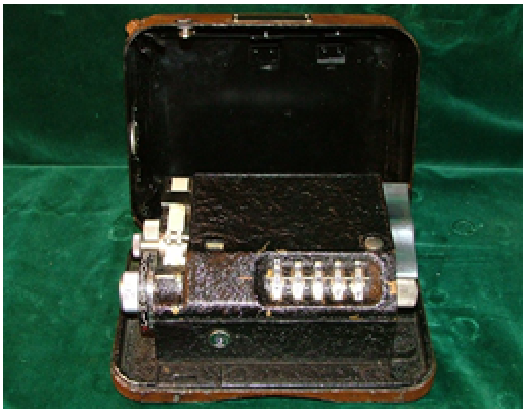
Selector Switch, Japanese PURPLE

The Japanese Purple selector switch found in the wreckage of the Berlin Embassy.



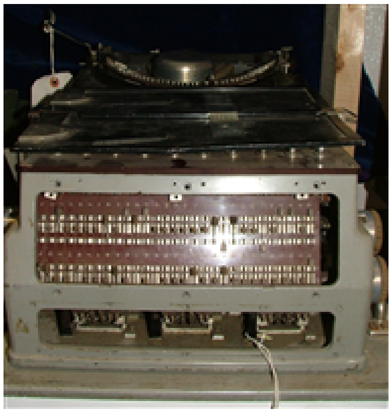
KL-36

This cipher machine was developed by the US Navy and incorporated into the Armed Forces Security Agency. It is an improved version of the M-209 with two sets of revolving rotors.



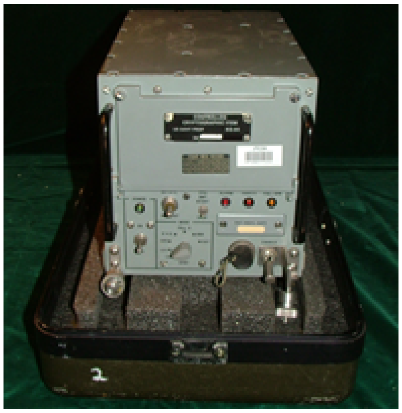
Hagelin C-36

The Hagelin C-36 cipher machine was developed in the 1930’s by Boris Hagelin. The six rotor mechanical cipher machine was one of the early pin and lug ciphers that used a pinwheel to move the rotors. The C-36 was predominantly used by the French Army.



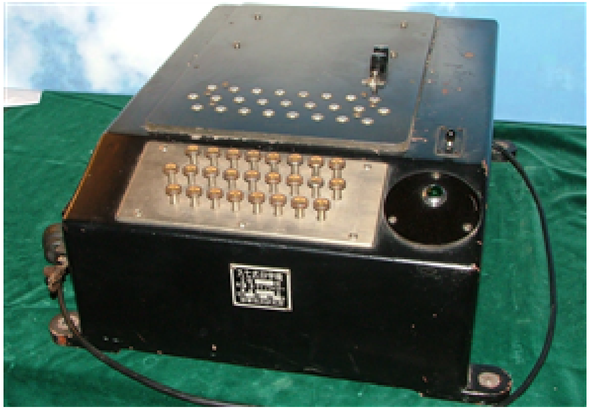
Japanese GREEN Cipher Machine

Japanese electromechanical wired rotor cipher machine, codenamed GREEN by U.S. cryptanalysts. It enciphered kana characters and digits into two-digit numbers varying from 00-99.



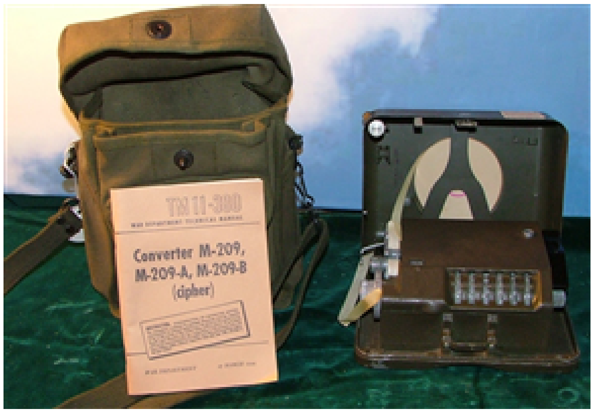
KG-84

This Dedicated Loop Encryption Device provides encryption and decryption for teletype and digital data traffic on dedicated links to various Input/Output devices. It is designed for use in tactical, protected, and fixed environments.



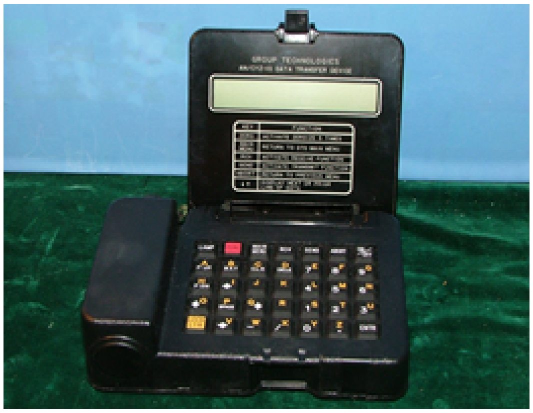
Japanese JADE Cipher Machine

The Japanese JADE cipher machine, the Japanese World War II cipher used by the Imperial Navy from late 1942 until 1944. The Japanese Navy used the JADE machines for high-level encryption of the katakana syllabary.



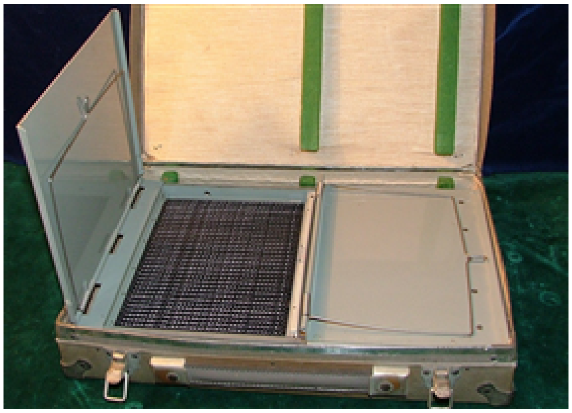
US Army M-209

Mechanical pin and lug cipher machine developed and sold to the US by Boris Hagelin. The device was rebranded the M-209 for the US Army. It was used for low level tactical field messages.



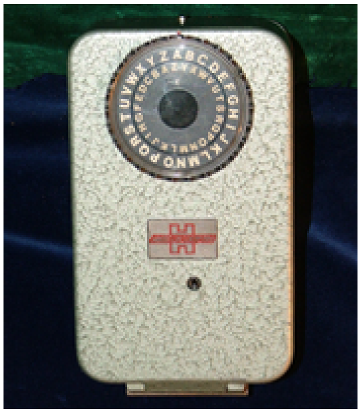
AN/CYZ-10

Developed in the 1990s by NSA and used by the US military and its NATO allies, the portable AN/CYZ-10 was a transfer device used for the distribution of cryptographic data to tactical radios. Nicknamed the Crazy-10, it was compatible with multiple crypto devices and capable of storing up to 1000 different crypto keys.



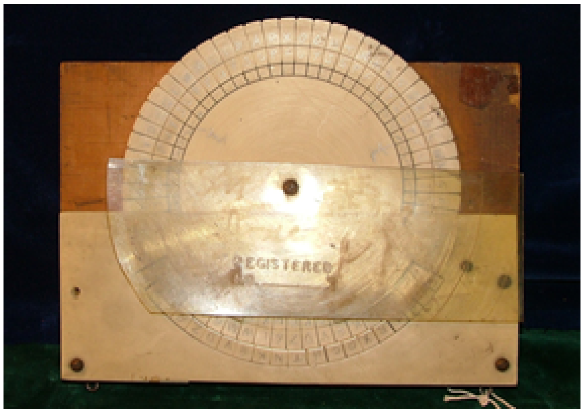
British SYKO Cipher

This mechanical cipher machine was a portable slide cipher introduced in 1939 by Morgan O’Brien and used by the British Royal Air Force.



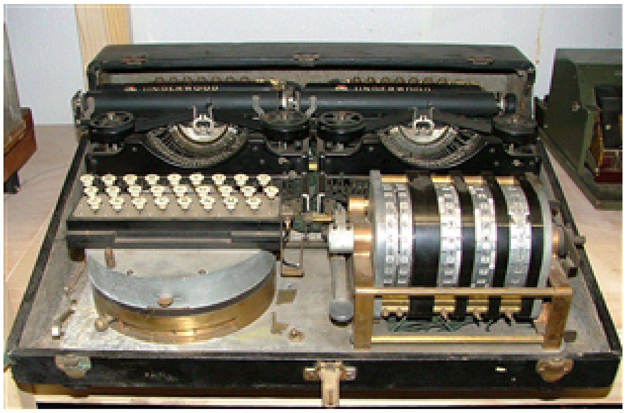
Hagelin CD-57

This handheld mechanical cipher machine was introduced by Crypto AG in 1957. The CD-57 was primarily used for tactical field messages and was popular with European militaries.



US RED Analog, Manual

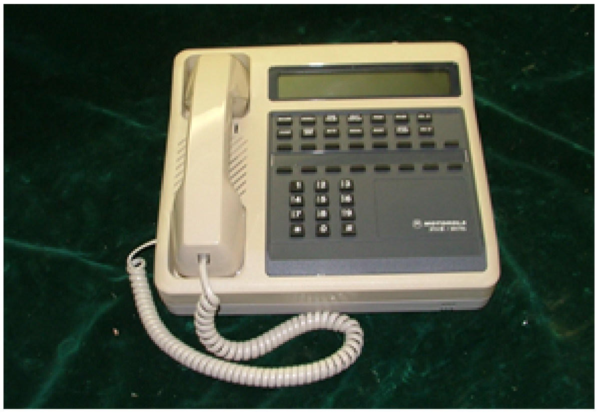
Analog of Japanese "RED" machine built by Frank B. Rowlett. Duplicated the cryptography of the much larger Japanese "RED" machine. Hand operated, used to decrypt Japanese diplomatic traffic in the mid 1930s.



Hebern Code Machine

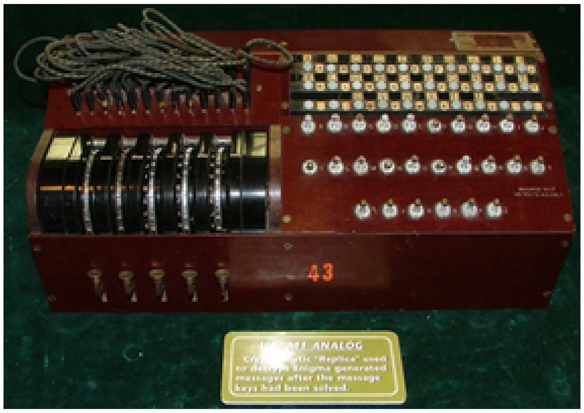
Hebern invented the Electric Code Machine in 1918. It was the first wired rotor cipher device in the US. The Code Machine worked in conjunction with an electric typewriter with the wired rotor acting as a scrambling device to change the signal from each typed letter to a different letter. This created an enciphered message.

While the overall sales of Hebern's machines were unsuccessful, they did find a limited market in the US Navy. This Hebern Electric Code Machine (HCM) was purchased and used by the Navy through the beginning of WWII.



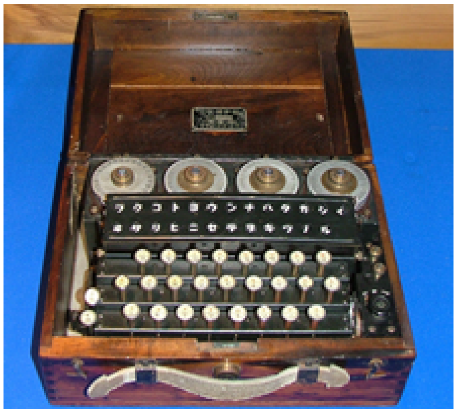
STU-III

The STU-III, developed in the mid-1980s, was the most sophisticated secure telephone system in the world at the time and was used by US government, contractors, and allies. It plugged into a standard telephone wall jack and could make calls to any ordinary phone user.
When a call was placed to another STU-III unit, and both used the Crypto Ignition Key, a call could "go secure" in seconds.



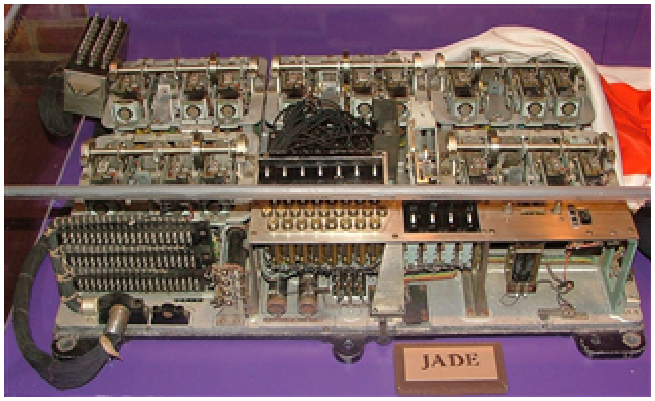
US M-1 Enigma Analog

U.S. M-1 Analog, machine no. 17. Cryptanalytic analog used to decrypt Enigma generated messages after the message keys had been solved. Used five SIGABA type rotors.



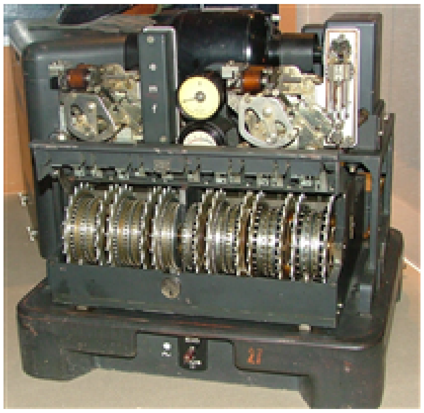
Japanese Rotor Machine

The Japanese cipher machine developed based on principles of the German Enigma containing both a light board and rotors for enciphering and deciphering.



Japanese JADE Cipher Machine

The Japanese JADE cipher machine, the Japanese World War II cipher used by the Imperial Navy from late 1942 until 1944. The Japanese Navy used the JADE machines for high-level encryption of the katakana syllabary.



German Schlusselzusatz-40/42 | TUNNY

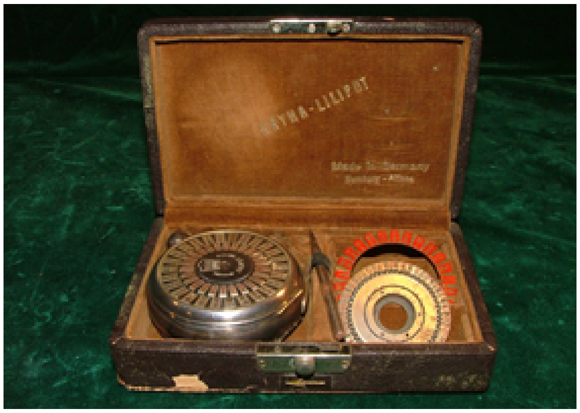
The Spark

Manufactured by the German firm Lorenz, the Schlusselzusatz 40 (SZ40) was used by the German Army for high-level communications. It encrypted and decrypted messages and could handle large volumes of traffic at high speed. It was far more complex, and thus far more difficult to break, than the German Enigma machine.

Lorenz cipher machine (codenamed Tunny), Germany, WWII

Disk Cipher

Early West European communications security device. This cipher device was used by the ministry of the interior of Denmark to secure its communications from 1910 - 1914. Two concentric brass rings hold ivory alphabetic pieces.

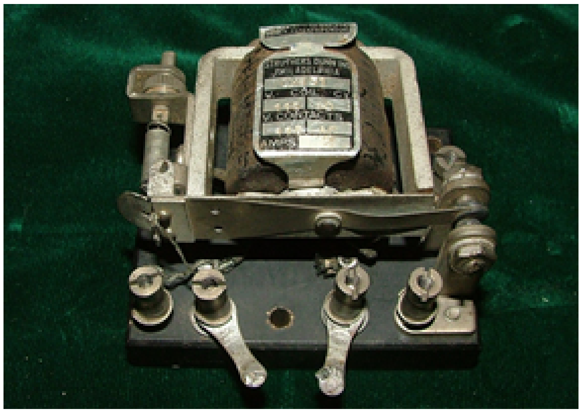


German KRYHA Liliput

This handheld cipher was one of three models invented by Alexander von Kryha in the 1920's. The Kryha-Liliput is the smallest and slowest of the three devices.

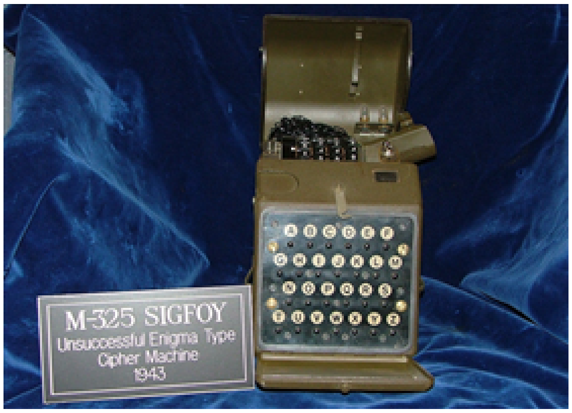
MAGIC Briefcase

Pouch used from late 1945-46 in G-2 at the Pentagon to courier MAGIC documents to authorized recipients.



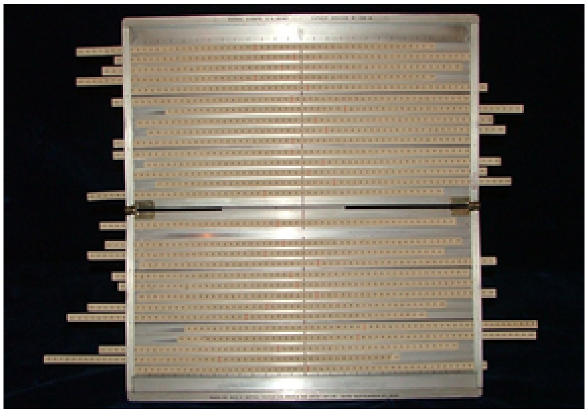
Failed Relay, PURPLE Analog

Original failed master relay switch salvaged from Purple Analog No. 1 by Frank Rowlett. While checking the power supply circuits during the first decrypt attempt, Leo Rosen discovered the master relay contacts had fused together. Frank Rowett found another relay and Rosen did some fast math calculations and decided to wire a condenser across the contacts of the replacement relay before installing it. Once the new relay was in place the machine performed perfectly until the end of the war.



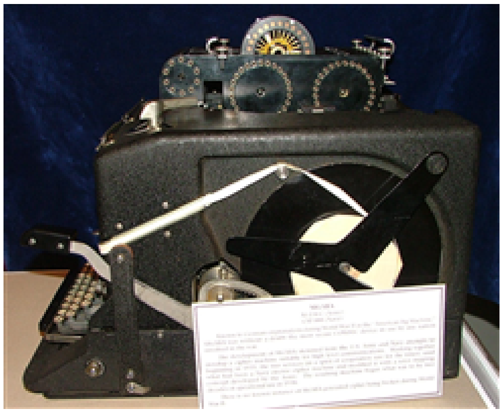
US Army M-325

M-325 SIGFOY was an Enigma type device designed by William Friedman in 1936. It was intended for use by the U.S. Army during WWII but it was never adopted. Between 1944 and 1946, more than 1,100 machines were deployed within the United States Foreign Service. Its use was discontinued in 1946 because of faults in operation.



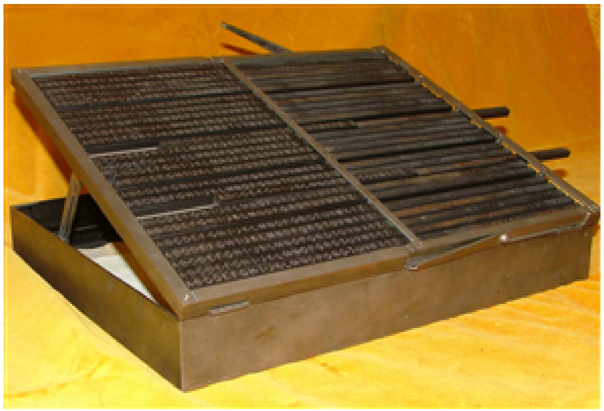
US Army M-138

The M-138 strip cipher was invented in 1916 by Parker Hitt of the US Army but was not adopted for use with secure communications until 1935. The M-138 originally had only twenty-five strip channels.



US Army M-134-C | ECM Mark II

U.S. SIGABA Cipher Machine developed by US Army's Frank Rowlett and built by the US Navy. It uses random stepping motion of 15 wired rotors contained in a detachable rotor basket. The rotor motion is governed by five-level punched tape. It was the high level cipher machine used by the US during and after WWII. There is no known instance of SIGABA enciphered messages being broken.

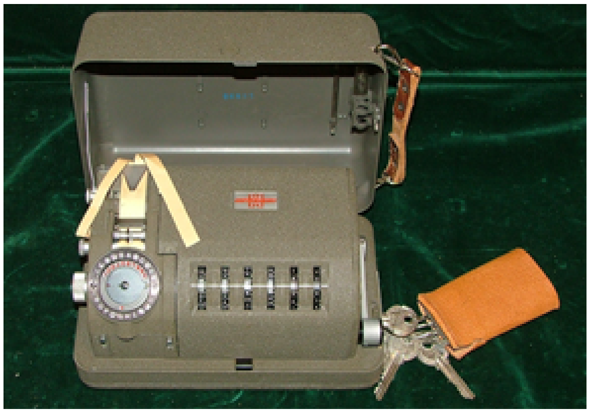


US Navy Cipher Box Mark I

The first cipher device used by the US Navy. Introduced in 1917 by Lieutenant Commander Russell Wilson, this metal slide cipher box had lettered plastic slides that were used to encrypt messages.

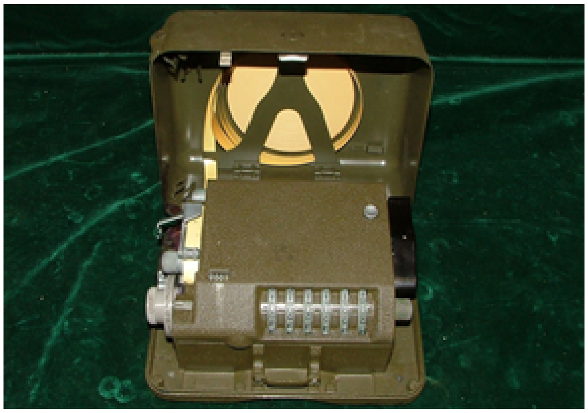
Slidex

This paper based hand held cipher was used by the British during WWII for tactical field messages. Introduced in 1943, the Slidex consisted of a pre-defined matrix of words and numbers to encode messages.



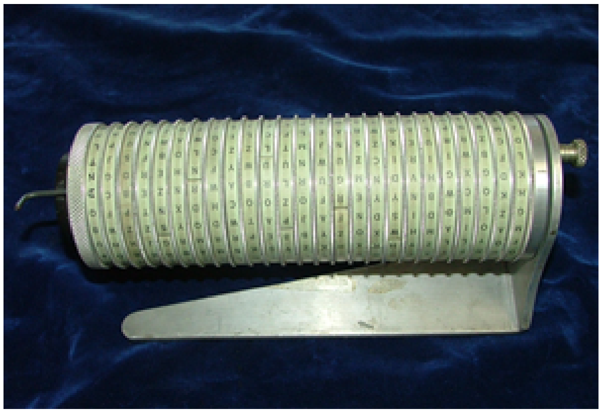
Hagelin C-52

The C-52 is a six-rotor cipher machine with paper tape output meant to be a replacement for the C-38. As some of the rotors had up to 46 settings, it was a much more secure system than the C-38. Portable and hand-operated, it was used to encode/decode diplomatic messages and other high-value traffic.



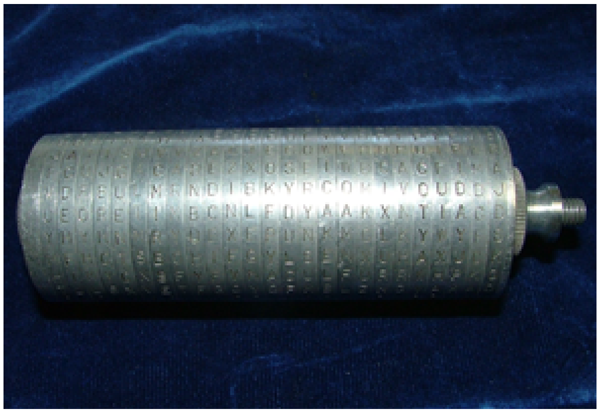
US Navy CSP-1500

The Naval version of the M-209-B, the CSP-1500 is a six-rotor cipher machine with paper tape output. Portable and hand-operated, it was used aboard ships to encode/decode tactical messages.



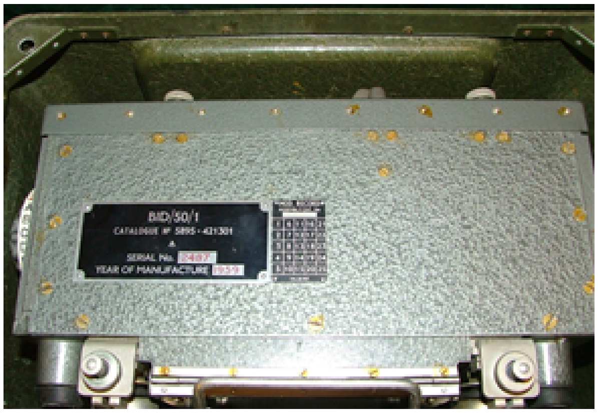
US Army M-136

The US Army M-136 cipher device was designed by the U.S. Army Signal Corps and is functionally similar to the M-94. However, it was not put into use and no instructions were ever made for it. It contains 25 wheels, covered with light green randomly lettered paper strips, metal construction, sits on a v-shaped base and has a black knob on the end.



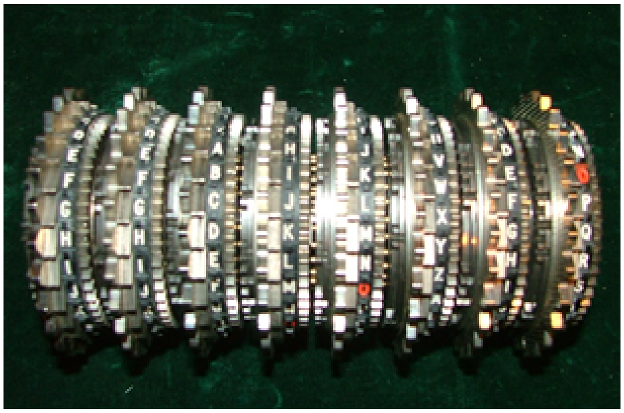
US Army M-94

U.S. Army M-94 Cylinder cipher, 1922-1945, 25 wheels. Invented in 1915 by Colonels Parker Hitt and Joseph Mauborgne, adopted by the U.S. Army in 1922. Earliest versions were Bakelite. This aluminum version dates from WWII. Each wheel is contains a randomized alphabet. The relative positioning of the wheels and the ordering of them on the axle constitute secondary and primary cryptovariables. The design is identical in concept to a device depicted in drawings by Thomas Jefferson.



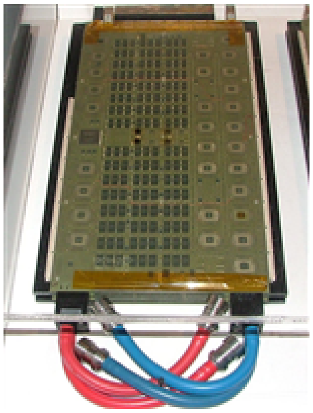
British Portex

This British cipher machine was used by the UK Secret Services during 1940’s and 1950’s. It is a more advanced version of the Enigma with 8 cipher wheels with irregular stepping.



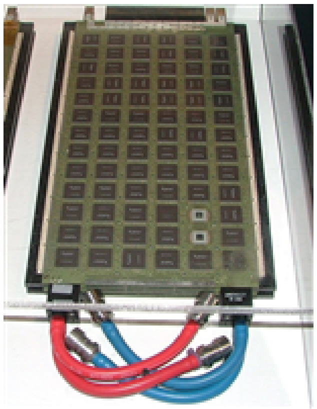
Rotor Storage, Portex

Green Fiberglass Box containing a rotor set for the British Portex Cipher Device.



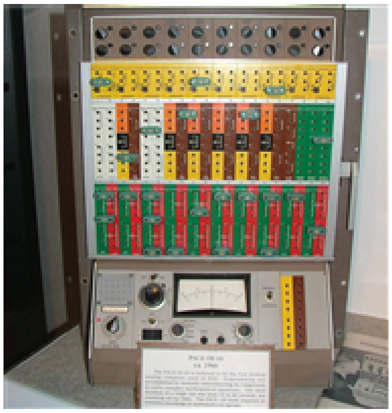
Module, Memory

Cray Y-MP M90 or Ziegler memory module, MEMDRAM16. One of 38 installed in the Ziegler, which had a total of 32 GB of memory.



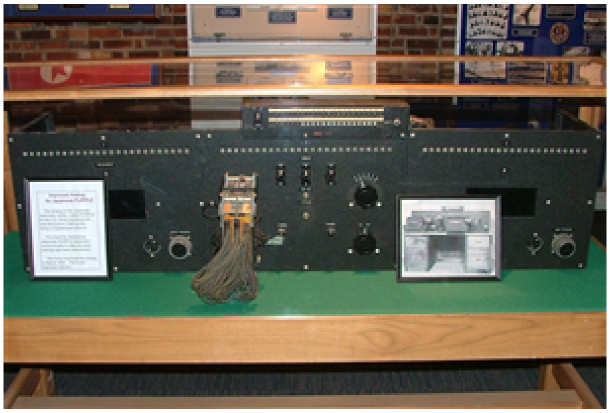
Module, Processor

Cray Y-MP M90 Ziegler processor module. One of eight parallel vector processors mounted on liquid cooled coldplate.



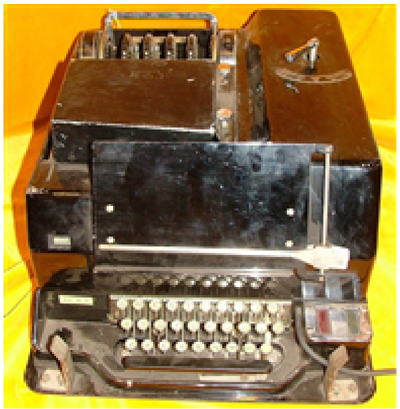
Computer, Analog

Introduced in the 1960’s, the PACE TR-10 is believed to be NSA’s first desktop analog computer. This device was operated manually by interconnecting the various plugs and components into the color coded signal processing sections. This would solve complex mathematical equations.



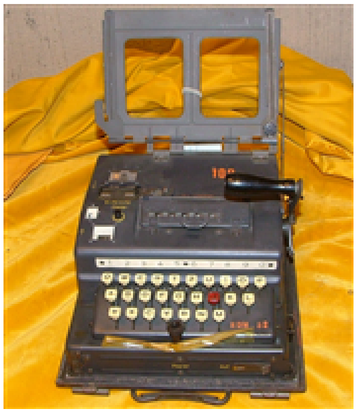
PURPLE Analog

Analogue of Japanese Purple cipher machine. The original version constructed by Cryptanalytic Branch (US Army) in November 1940 for reading messages after wheel settings had been determined. This improved version was constructed in March 1944.



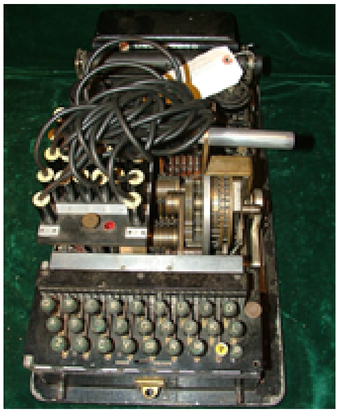
US Navy CSP-1127

The CSP-1127 was a modified ECM Mark I and used in conjunction with a CSP- 693 Teleprinter for state department traffic. It was also considered the HCM Mark III.



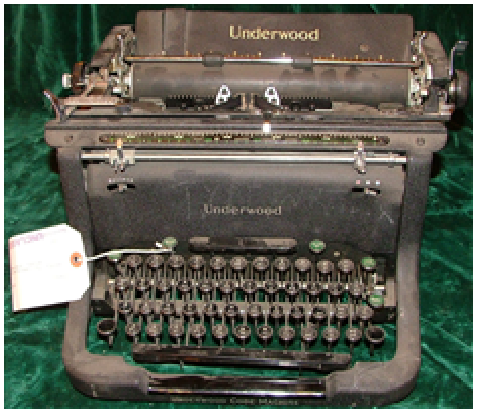
German Schlusselgerat 41

The German Shlusselgerat 41 was introduced by the German Intelligence Organization called the Abwehr in 1944 as a potential secession to the Enigma-G machine. The SG-41 was a mechanical pin-wheel cipher machine very similar to the Hagelin C-38. It's hand crank earned it the nickname the Hitlermuhle or Hitler Mill.



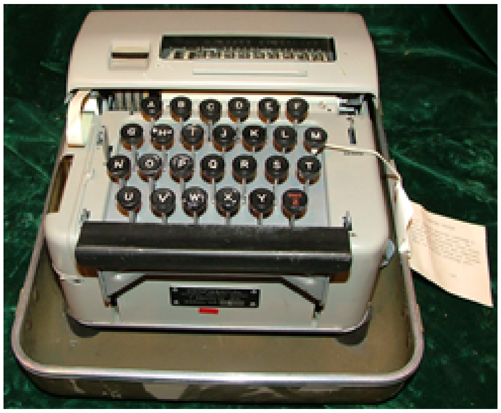
RED Analog

In the late 1930s the Navy Yard model shop constructed the electromechanical RED analog. The machine mimicked the actions of the Japanese Cipher Machine Type A [RED] with its commutators for the sixes [vowels, including Y] and twenties [consonants], the [47-position] breaking wheel that controlled the stepping motion, and the plugboard.



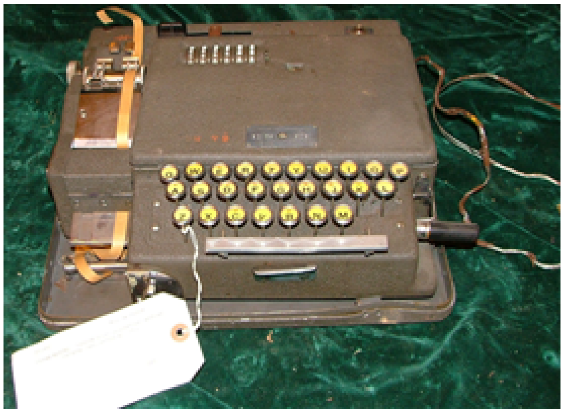
UNDERWOOD CODE MACHINE

This special transliteration device was developed in 1924 by the US Navy's Laurence Safford and built by the Underwood Typewriter company. It was used to aid in the transcription of Japanese intercepts with a keyboard designed with both Roman and Kana included.



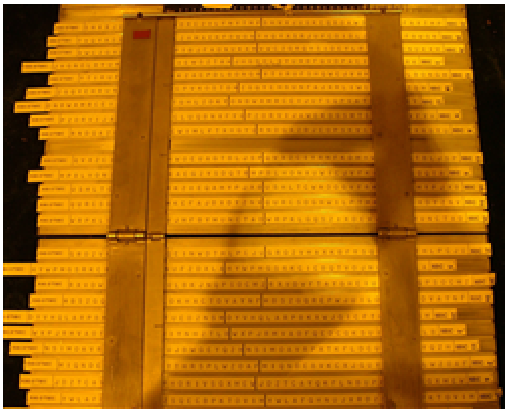
KL-17

This pneumatically powered cipher machine was developed in the 1950’s by US Armed Forces Security Agency. It utilized air powered maze rotors to encipher messages. Never put into production due to sluggish operation.



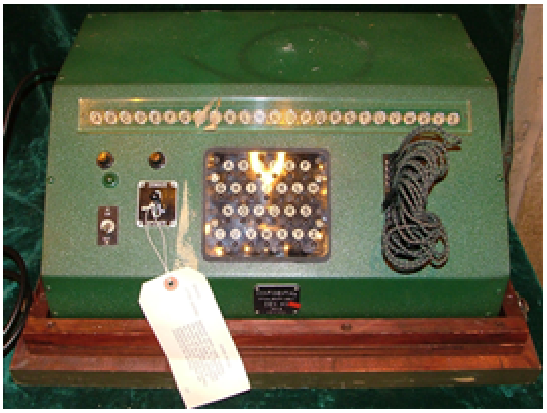
Hagelin BC-38

Electromechanical cipher machine invented by AB Cryptoteknik in 1939. It is an advanced version of the C-38 with a motor and keyboard.



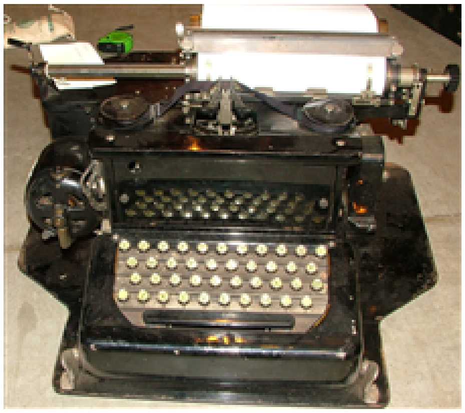
US Navy CSP-845

The Navy equivalent of the Army M-138, the CSP-845 was a manual strip cipher device consisting of a folding aluminum base on which is formed thirty channels or grooves into which alphabet strips may be inserted. When inserted these strips would be aligned in a specific order to cipher and decipher messages.



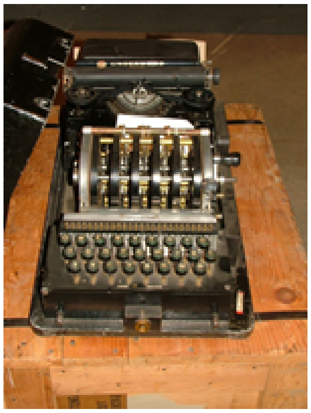
ZEN-40

Developed for use by the “Aggressor” – or the bad guys in American joint maneuvers and training exercises – the Zen 40 was used for the encryption of summaries of secret agent reports. The Machine used telephone-selector switches similar to Japanese Purple.



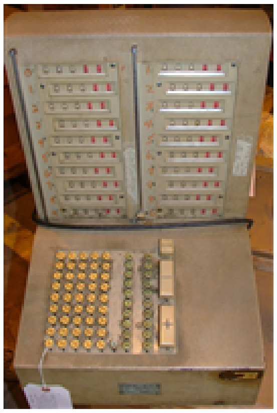
US Navy CSP-693

The CSP-693 was a modified teleprinter used in conjunction with a CSP- 1127 cipher attachment for state department traffic.



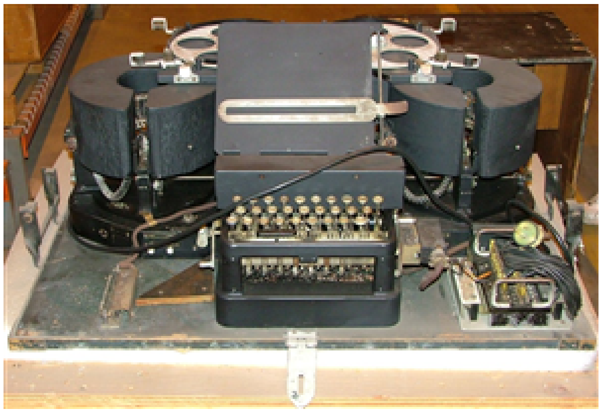
US Navy CSP-903

The US Navy used modified a Hebern Cipher Machine to develop the CSP-903. It is also called the Hebern Code Machine (HCM) Mark I



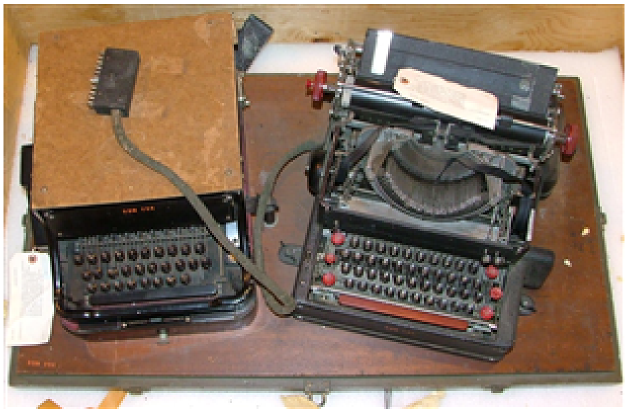
NCR Differencing Machine

Special purpose calculator/differencing machine developed by the U.S. Navy and manufactured by National Cash Register company (NCR). Designed simply to invert (undo) the non-carrying addition of numerical code groups to plain text, a practice used in Japanese Army systems. Non-carrying addition is a basic operation in modular arithmetic, and the inverse operation, which amounts to adding the additive inverse, is called differencing, so this device is otherwise called a differencing machine, or cryptanalytic differencing machine.



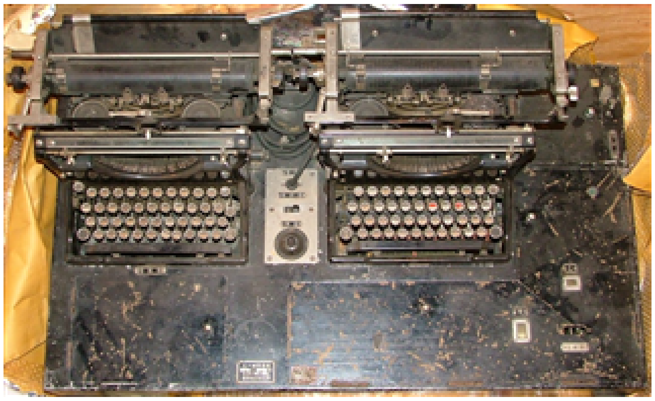
British Typex

The Typex was developed in the UK by O.G.W. Lywood in 1934. It is considered the British Variant of the German Enigma and was used for high level communications.



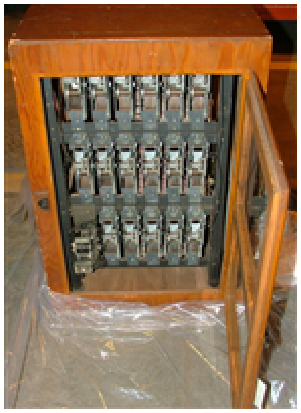
PURPLE Analog

These are the input and output typewriters for PURPLE analog. The PURPLE analog machine was developed by the US Army Signals Intelligence Service in 1940 to help expedite breaking the Japanese PURPLE Cipher Machine. Eight of these machines were built for the US. Four went to Washington DC, two went to the US Army, and two went to the US Navy.



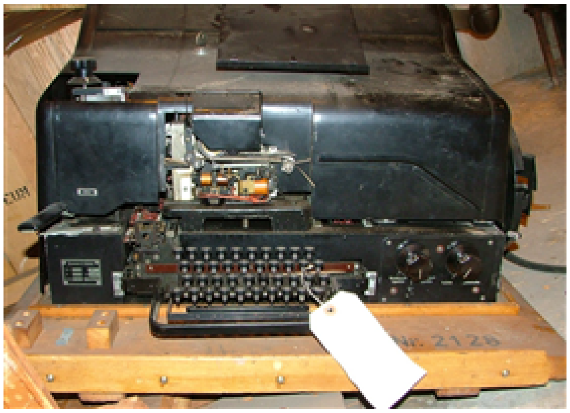
Japanese RED Cipher Machine

This is the System 91 Typewriter or Japanese RED Machine as code named by US cryptographers. Introduced between 1930-32, the RED Machine was used for Japanese diplomatic communications and by Japanese naval attaches before and during WWII.



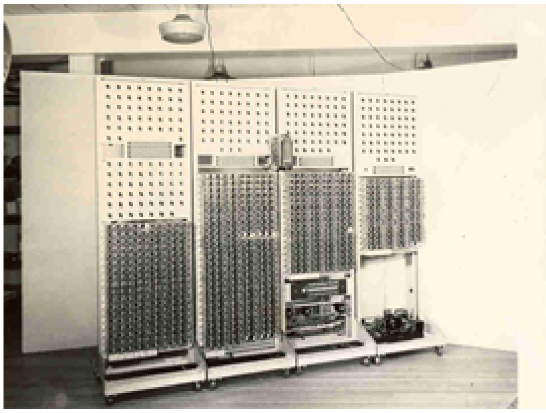
PURPLE Analog

The PURPLE Analog machine was developed by the US Army Signals Intelligence Service in 1940 to help expedite breaking Japanese PURPLE cipher machine. Eight of these machines were built for the US. Four went to Washington DC, two went to the US Army, and two went to the US Navy.



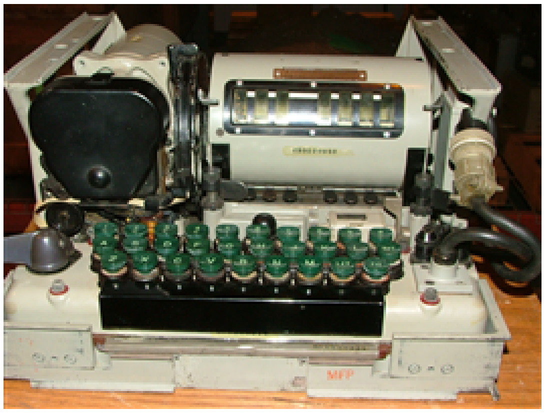
STURGEON

The T-52 Geheimschreiber was an electromechanical cipher machine was used for teleprinter signals. Nicknamed Sturgeon by code breakers at Bletchley Park, the T-52 was Invented by Siemen & Halske in the 1930's and used throughout WWII.



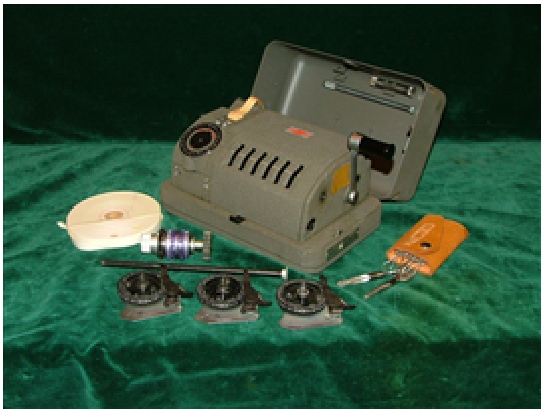
DRAGON

The US Built Dragon was a cryptanalytic device built by the Signal Security Agency (SSA) in 1944 to facilitate the British Colossus in breaking the Schlusselzusatz SZ40 Cipher machine during WWII.



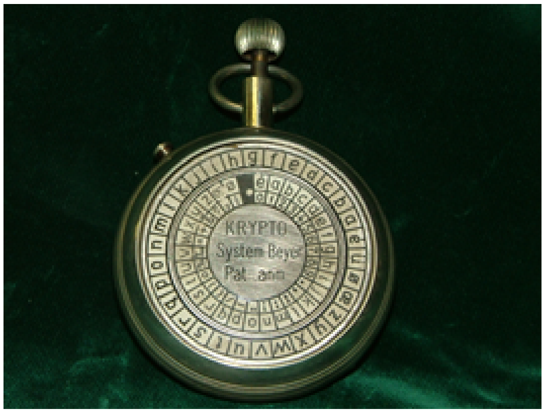
KL-7

This offline electromechanical cipher machine was developed jointly by the US Army and Navy. It was the first cipher device issued under the Armed Forces Security Agency (Precursor to the National Security Agency) in 1952. It used 8 electrical rotors to encrypt messages.



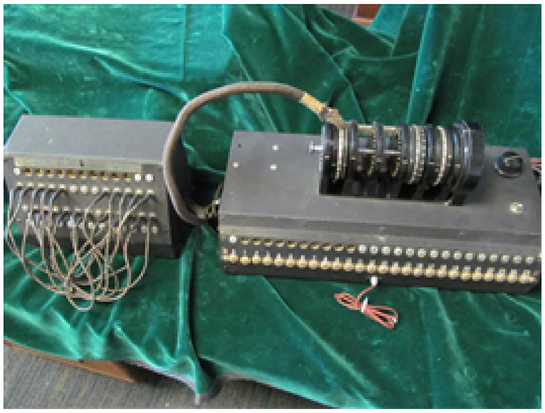
Hagelin CX-52

This mechanical lug-and-pin cipher device was invented by Boris Hagelin in the 1950’s as a successor to the C-38. As some of the rotors had up to 46 settings, it was a much more secure system than its predecessor. Portable and hand-operated, it was used to encode/decode diplomatic messages and other high-value traffic.



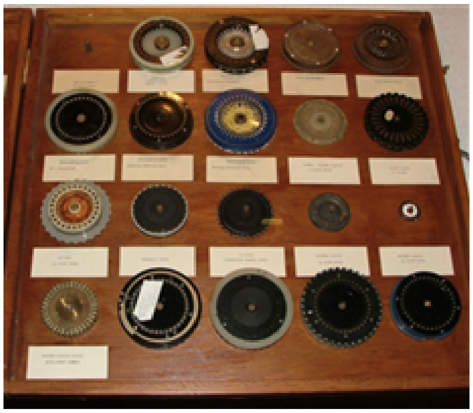
KRYPTO System Beyer

The Krypto System Beyer is a mechanical cipher device the size of a pocket watch. It was invented in Denmark in the 1930s by The Danish Cipher Machine Company, Ltd.



Bombe Checking Machine

After each Bombe run, a WAVE supervisor checked the results on an M-9 machine like this to see if a message actually decrypted to German. Only one solution on one Bombe would have the correct wheel order: a “Jackpot.”



Various Cipher Machine Rotors

Various rotors from many different cipher devices. Prominent rotors in the collection include:
- Enigma
- Sigaba
- KL-7
- Hebern
- Bombe
- Hagelin
- Tunny
- Sturgeon
- Japanese Rotor Machine
- Typex