Some Reminiscences

BY BRIGADIER JOHN H. TILTMAN

~~*Top Secret Trine*~~

This article is liable to be a rather disjointed affair. I have given four other papers to the CMI during the past five years, each built round its own central theme. But into the present paper I have tried to put everything else which, in my view, would still be of interest to others. If it has a central theme, it is that there are still cipher systems in use which are potentially quite vulnerable but which, in the diagnostic stage, require wide cryptanalytic experience.

The justification for the scale on which signal intelligence is practiced is that it is a weapon of defense, and that, in addition to the full scale scrutiny of the sophisticated systems of potential enemies, we still cannot afford to neglect the communications of the less important states. The intelligence derived from the study of such communications is only cheap if it is carried out as expeditiously as possible, and the cryptographic systems of such states frequently make up in complexity what they lack in sophistication and in these cases it frequently needs wide experience at successful cryptanalysis to discover the clues to solution.

My treatment of the subject is personal and in most cases I have had to rely entirely on my memory. I have had to dig back into past history for some odd cases to show how I got my experience.

With some misgivings I am now going to include some passages from the farewell address which I gave at GCHQ on my retirement from British Government service in the fall of 1964.

"Out of 45 years' connection with this office, I suppose I have spent upwards of 30 breaking into previously unexploited ciphers from scratch. I have often tried to analyze my own approach to diagnosis although it seems to me unlikely that any of my subjective conclusions will be of much help to others. Speed of operation and speed of thinking are obviously factors contributing to success, and speed is to a great extent dependent on variety of experience and particularly on the experience of personal successes of the kind which breed confidence (even if unjustified) and optimism. My powers of concentration are not good—this makes me an inattentive listener. It seems to me that most of my useful thinking goes on just below the level of full consciousness. I have always envied the power of concentration of people like Josh Cooper and Hugh Alexander who

appear to be able to read or listen to a long and complicated technical argument, to absorb the whole of it and record it mentally for future use."

I have recently been reading again the story of Michael Ventris' solution of the Mycenaean "Linear B" inscriptions. Most readers will probably know the story, but, for the benefit of those who don't, in about 1953 Ventris, a young British architect, announced his solution of the quite large number of inscriptions found mostly in Crete and at Pylos in Greece and named Linear B by the original finder of the Cretan ones, Sir Arthur Evans. Ventris' solution, if correct, proved that the underlying language was an early form of Greek (some 800 years earlier than the Classical Greek of literature). The vast majority of classical scholars have accepted his solution *in toto*, but there has been considerable controversy, a few scholars openly rejecting it. One recent elaborate study of his solution refers to him as an "amateur," expresses surprise at the speed he showed in reaching his conclusion before the "professionals," and criticises his description of his method of arriving at solution as "less than frank." I personally think it extremely likely that Ventris simply didn't know how he arrived at his first recoveries—he had soaked in the inscriptions for years and carried with him in his head a mental picture of the combinations of signs; and the ideas that came to him that led to solution were formulated quite subconsciously.

To return to my quotation. "I have always been rather a lone hand, preferring whenever possible to do my own preliminary analysis, registration and indexing. I prefer not to embark on machine runs any more complicated than the simplest sorting and listing, unless there is some very good reasons to believe that they will be profitable." By way of comment on that sentence, I ought to have said that a special exception should be made in the case of runs of the type of the Rob Roy Stethoscope, which, of course, saves a lot of time in those cases where repetitious and non-random features within a message may provide an immediate clue.

"But I am usually impatient at the first approach to a new problem and on these occasions invariably have to back-pedal later so as to make proper use of back history, collateral, T. A., etc. I don't, however, believe in being too cautious. I am prepared to follow a tenuous lead without knowing whether it is statistically justified, in the hope that I will know when to stop following it, if it appears to be leading into the ground.

"I have no knowledge of higher mathematics and my grasp of probability is instinctive and quite unsound, but I am not too proud to ask for help and, when I have done so, have not often been misled.

"A cryptanalyst cannot afford to be afraid of making mistakes. I

have made a fool of myself many times and I think I have usually profited. I have therefore always felt justified in refusing to accept anyone else's conclusions without careful scrutiny.

"I believe most experienced cryptanalysts would agree with me that cryptanalysis, at any rate in its diagnostic aspect, is much closer to art than to science, and this is what makes the personal factor so important." Hugh Alexander has told me that he considers I am much more like a detective than a cryptanalyst.

"I am not in any sense of the word a linguist and have always found languages hard to acquire, but I have never been afraid of an unknown language and believe that a research cryptanalyst is the better equipped if he develops a working knowledge of comparative linguistics and an ear for the sound patterns of unfamiliar languages. But I am aware that this is not a rule of universal application—comparatively few cryptanalysts nowadays have the opportunity of working in more than one or two languages.

"A cryptanalyst should take every opportunity of acquiring a general working knowledge of branches of Signal Intelligence other than his own. From 1921 thru 1929 I was a member of a section of the General Staff at Army Headquarters in Simla, India, consisting of never more than 5 persons. We were employed almost entirely on one task, to read as currently as possible the Russian diplomatic cipher traffic between Moscow, Kabul in Afghanistan and Tashkent in Turkestan. From about 1925 onwards I found myself very frequently involved in all aspects of the work—directing the interception and encouraging the operators at our intercept stations on the North West Frontier of India, doing all the rudimentary traffic analysis that was necessary, diagnosing the cipher systems when the frequent changes occurred, stripping the long additive keys, recovering the codebooks, translating the messages and arguing their significance with the Intelligence Branch of the General Staff. I realize that I was exceptionally lucky to have this opportunity and that very few others have had the chance of acquiring this kind of general working experience. Between 1921 and 1924 I paid three visits to the corresponding unit in Baghdad and on several occasions, sitting amongst the operators in the set-room of the Baghdad intercept station, worked directly on the red forms fresh off the sets, to the benefit not only of my own experience but also to the morale of the operators.

"I have benefitted greatly from being forced, often much against my will, to write detailed reports and general appreciations. I have also, at frequent intervals between 1924 and 1948, been forced to produce practical ciphers of varying degrees of security for British use. This is a field in which sloppy thinking finds one out more than in any other and I believe it to be a considerable factor in training

the imagination for diagnosis of complicated problems. It is obvious that the livelihood of a cryptanalyst depends almost entirely on the over-ingenuity of the designers of foreign ciphers."

I shall come later in the lecture to the description of two of the ciphers I have produced. Nearly all my ciphers went into use before there was any organization for studying their technical security. During most of World War II I held the traditional title of Chief Cryptographer. (By the way, I am told that one of the senior German cryptanalysts under interrogation in 1945 said he understood that the British Chief Cryptographer was paid more than the Archbishop of Canterbury). As a result of this high-sounding title I was expected to be personally responsible for the technical security of all British cipher systems.

At this point I just want to tell one story. In 1924 I produced a field cipher for use by the Army in India, and in Fig. 1* I have made up an example to show how it worked. (The text is just a piece of narrative text chosen at random.) There was a key consisting of the rearrangement of the 10 digits—this was changed daily and it was to be written vertically and repeated cyclically as well as horizontally. In each line the number of cells corresponding to the digit of the key at its left was crossed out and the message written in line by line into the remaining cells and then the letters were taken out in columns according to the horizontal key starting with the digit 1, giving the result as shown at the right. The last line was to be completed with null letters as far as the erasure of cells according to the key allowed. Though at the time I was very inexperienced, I gave a good deal of thought to the cipher and to the instructions for its use and convinced myself that it was original, practical and sufficiently secure for its purpose, and there was no one else to check its security. Some considerable time after it had gone into use and when I was thinking of something entirely unconnected with it, I suddenly became conscious of the flaw.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

I am now going to give an abbreviated description of my contact with Japanese ciphers beginning in 1933. One system I have not included is the very complicated cipher wished by the Japanese Government on the Japanese commercial firms in 1944. I carried

*All figures and tables appear at the end of the article.

out all the steps to final solution at GCHQ, but the cipher was also independently solved in ASA and a full description of it is on record.

[redacted] EO 1.4.(b) EO 1.4.(c) EO 1.4.(d)

In 1933 I solved the Japanese Military Attaché System which had been in use since 1927. There was a small basic code-chart of, I think, 240 units which meant that a large part of the plain text had to be spelt-out in syllables. I don't remember the details of the system except that the code-chart had to be reconstructed and 40 different sets of line and column coordinates recovered. There were at the time two very distinguished Japanese scholars in the office, who had each retired as British Consul General in Japan. One of them partially reconstructed the code-chart for me from the material in one of the 40 keys, and I set about recovering the other keys. Shortly afterwards the other expert came and said he had heard I had some interesting work in progress and that he would like to help—so I gave him the material in one of the keys in which I had recovered most of the syllabic values, numbers and so forth. He returned it to me 3 weeks later unchanged, saying my solution was "plausible." This should have warned me that I was treading on hallowed ground.

At this point I feel I must inflict a digression on the special nature of the Japanese language as seen from the cryptanalyst's point of view. Twenty years ago a considerable number of people in both the American and British offices had of necessity acquired some knowledge of Japanese, but there must now be many readers who have not been exposed to this language which in its written form is not like other languages. Written Japanese is based on Chinese characters, but the result is in many respects much more complicated than Chinese. The enormous variety of Chinese characters are ideographs representing basic concepts and having monosyllabic sounds. The Japanese, whose native language had originally nothing in common with Chinese, first committed their language to writing between the 7th and 9th centuries A. D. by introducing Chinese characters wholesale. The characters were absorbed in two waves separated by a considerable interval of time during which there was quite a change of sound. As a result, a Japanese character normally now has at least two differently sounding Chinese readings and these sounds are very different from the present-day Chinese readings of the characters. In addition, a Japanese character also usually has one or more native Japanese readings in no way related to the Chinese sounds, only to their meaning. Fig. 3 shows a page of Rose Innes' *Dictionary of Chinese-Japanese Characters*. This is a limited dictionary for English-speaking students of Japanese giving the commoner readings of about 5000 characters and the commoner compounds of two or more characters. What would correspond in Western languages to

alphabetic order is in Chinese and Japanese "stroke-order." A character is treated as a combination of one of 214 radicals and a so-called phonetic, and the characters are listed first under the number of strokes in the radical and then the number of strokes in the phonetic. The counting of strokes and the arrangement are traditional in both languages, and the process of finding a character is far more complicated than it sounds. In addition, the Japanese were obliged to introduce a syllabary (known in its two forms as Hirapana and Katakana) as a sort of commentary to make the meaning of the Chinese characters clear where Japanese syntax requires it and for spelling of foreign names. (Fig. 3A)

Written Japanese, therefore, is a mixture of Kana syllables with Chinese characters each of which can be read in a number of different ways according to context. Fig. 4 shows a typical passage of printed Japanese text. In the right hand column, i.e., the first column of text, I have written the Romanised transliteration opposite the Kana (Hirapana characters). I should add here that there is also a conventional Romanised form of Japanese known as Romaji. Critics of the enormously complicated nature of Japanese written in characters have tried to have it replaced entirely by Romaji but have met with much opposition on the ground that it introduces ambiguities that the use of characters doesn't. But in favor of Romaji it should be said that all the early Japanese ciphers were based on it, especially the two high-grade diplomatic machines which enciphered from Romaji letter by letter, and it is the opinion of Japanese scholars who have worked on the solution of such ciphers that, except in the special case of reference to Chinese proper names, cases of possible ambiguity were very rare indeed.

You will realize that putting Japanese plain text into cipher involves some special problems, especially when a code based on characters is in use.

The page of Rose Innes I give in Fig. 3 was chosen specially to show what the Japanese can do with their language when they really try. The large character in the middle of the right hand column is the 150th of the 214 radicals and has, in addition to the readings given here, the reading "GAI." There is an historical example dated about 1716 A. D. of a Japanese artist who signed his work with this same character 4 times running and expected his patrons to read his name "Tanigai Yatsuya."

I learned what little I know of the written form of Japanese the hard way! We had a British Army intercept station at Hongkong which from about 1935 forwarded to us considerable quantities of Japanese military intercept. Amongst the traffic was a number of messages sent in 4-figure groups, each message having a sentence or

two of plain language Japanese in romanised form (Romaji) in the preamble. It was clear from the repetitions and the homogeneity of the cipher texts that I had to deal with an unreciphered code, and I started code-breaking in the traditional manner by first isolating numbers, etc. I identified some of the numbers and found that they fell into their correct places in the stroke-order of their characters—stroke-order was something I had to find out for myself at this time. Thus I was able to treat the material as a one-part code with the groups in dictionary order, fixing the values for military formations, ranks, etc. It was only after proceeding quite far that a friend of mine, a Chinese interpreter in military intelligence in the War Office, convinced me that I was breaking, not a Japanese code, but the Chinese Telegraph Code! This was (and presumably still is) the index of rather less than 10,000 Chinese characters used by everyone for sending telegrams. It provides 4-figure equivalents in numerical order for the characters in stroke-order. There are 100 pages each containing 10 lines and 10 columns. The index goes through the first 80 pages in stroke-order, the remaining 20 pages being a supplement of infrequently used characters. Figure 5 is the page containing the 75th radical. I myself have never been able to memorise more than a very small number of the very simplest characters. I suffer from a sort of mental block which wipes out the memory of a character as soon as I take my eyes off it. But at one time I knew the values of quite a large proportion of the 4-figure equivalents in CTC.

Also in about 1935 I had to work on a system which was obviously a one-part code in which the cipher units were 3 kana groups. All the messages seemed to be very long and the most puzzling feature was that after the first few groups which were very sterotyped there appeared to be about 80 groups saying the same thing in a different order. The material turned out to be the intercommunications of 6 Japanese field signal intelligence stations on the China coast exchanging their recoveries of the private ciphers of the various Chinese warlords, all recipherments of the CTC. The normal practice in these ciphers was to renumber the pages as dinomes and sometimes the line and column coordinates (in digital form) on the pages. In some cases the line and column coordinates were different for all 80 pages—then the messages were really long! When the repagination didn't conform to a regular pattern, the message was interrupted to give between brackets the plaintext number of any page whose cipher value had not been recovered—this, I remember, usually happened with page 08 of CTC which contains no commonly used characters. At the end of each message the name of the user of the cipher recovered was given in CTC, each character of the name being expressed in two cipher groups having dinome plaintext equivalents.

My time for the three years, 1935 thru 1937, was almost entirely taken up with research on the intercepts from Hongkong. The major part of the traffic was in a succession of military systems used for transmission of intelligence reports from China, especially detailed as to the characteristics of key personalities. One of the Chinese warlords frequently mentioned was General LI TSUNG JEN, who in 1965 was much in the news—having in his old age just defected from Nationalist to Red China. His name, LI TSUNG JEN, became in its Japanese reading RISOJIN. The small basic code-charts used at the time necessitated the spelling of most of the plain text in Kana syllables, and each character of a Chinese name had to be precisely described either by giving the native Japanese reading for the character or its CTC equivalent, or even in some desperate cases, an elaborate description of the way in which a rare character was put together.

During this period the cipher systems used seemed to be changed quite drastically about every 9 months, and I had a hard time keeping up with the changes. I had no Japanese interpreter attached to me and the other members of my military section were otherwise engaged, part of the time on Italian ciphers during the Abyssinian War. There was an underlying thread of cryptographic continuity in all the systems, these being irregular switches from one substitution to another within messages. In one of them a switch took place immediately after every occurrence in the plain text of a particular syllable, the substitutions following a cycle which differed from day to day. In another the switch took place roughly at the end of each sentence and in this case warning switch groups had to be inserted. [redacted] This system seemed to have been mechanised in some way as the 12 x 20 code-chart was divided into two halves, the left half going through a cycle of 16 sets of coordinates and the right half through 17. It was in this cipher that I first came across [redacted] which remained the Japanese practice from that time until the end of World War II. This is the practice [redacted]

EO 1.4.(b) EO 1.4.(c) EO 1.4.(d)

From the 1st of December 1937 these systems rapidly gave way before the digital additive system which became general throughout World War II. The first cipher which was intercepted in sufficient quantity for attack had a 2-part 4-figure code-book in which the cipher groups were limited to multiples of 3, and the additive recipher

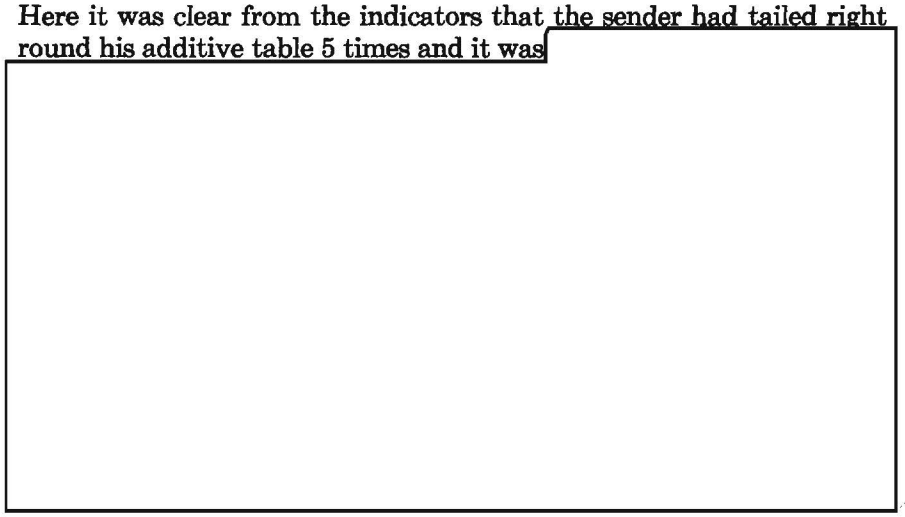
consisted of 10,000 4-figure groups arranged on 100 pages each containing 10 lines and 10 columns. For indicating purposes, each page carried its own pair of mixed digital sequences to act as column and line coordinates. Both the starting and ending points in the additive were indicated in each message and these were reciphered each by one of 100 4-figure additive groups controlled by a particular dinome of the first cipher group for the starting point indicator and the last cipher group for the ending point.

I succeeded in establishing the method of indication when our military and air sections were at our war station, Bletchley Park, during the Munich crisis in the fall of 1938. By the end of the year it seemed to me that we were sufficiently advanced to shift the responsibility for Japanese cryptanalysis to the Far East. In addition to the Navy, Army and Air Force intercept units in Hongkong there was a naval cryptanalytic unit, and in the summer of 1937 I had gone to Hongkong in an attempt to unload the solution and exploitation of military systems. This attempt failed, but at the beginning of 1939 I went again to Hongkong, this time taking with me Pat Man-Johnson and Geoffrey Stevens, both of them known to many of my readers. From this time this particular responsibility was out of my hands.

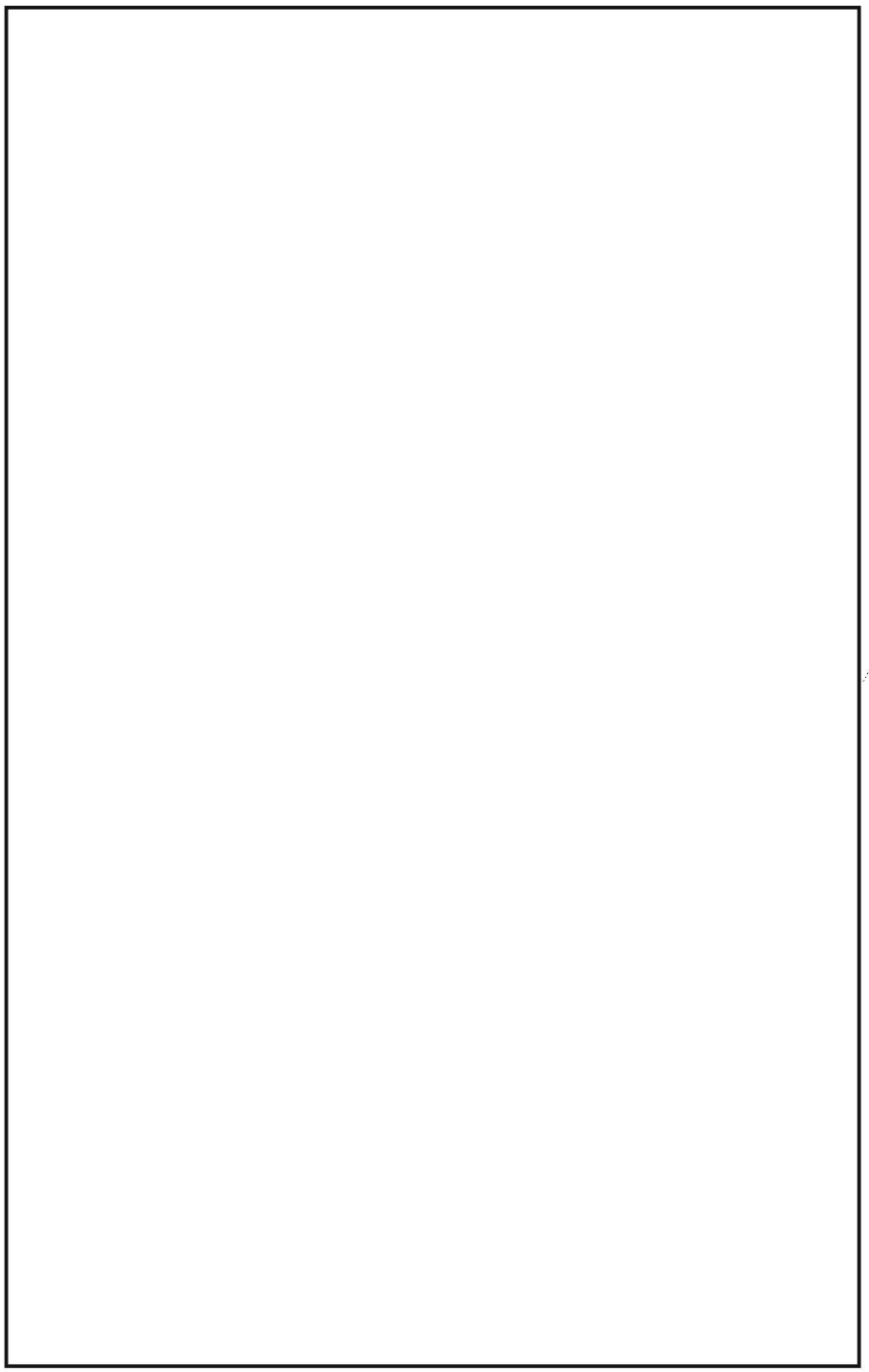
But I was not through with Japanese yet. After Pearl Harbour it rapidly became apparent that we would need many more Japanese interpreters for military purposes than were available, and I obtained permission from the War Office to start an experimental six months' course in written Japanese. For this purpose I was advised to recruit classical scholars of from 18 to 20 years of age from Oxford and Cambridge, and for a short but glorious period I achieved considerable personal popularity at both universities because I was the only person who wanted classical scholars because of their attainments in Latin and Greek. The courses went on for three years and were on the whole very successful. My opposite number, J. E. S. Cooper, who was head of the Air Section at GCHQ throughout the war, tried a rather more tricky experiment. What the Royal Air Force needed was interpreters who could read R/T air-to-ground and air-to-air conversations and for this purpose he started an intensive 11 weeks' course at which the students were bombarded incessantly with Japanese phonograph records ringing the changes on a very limited vocabulary. The course was directed, not by a Japanese linguist, but by a phonetics expert. I remember taking a U. S. Army Japanese interpreter, Col. Svensson, round the course. Stunned by the volume of sound in every room, Svensson mildly asked the Director whether all the students made the grade and the reply he received was: "After

the fifth week they're either carried away screaming or they're nipponified."

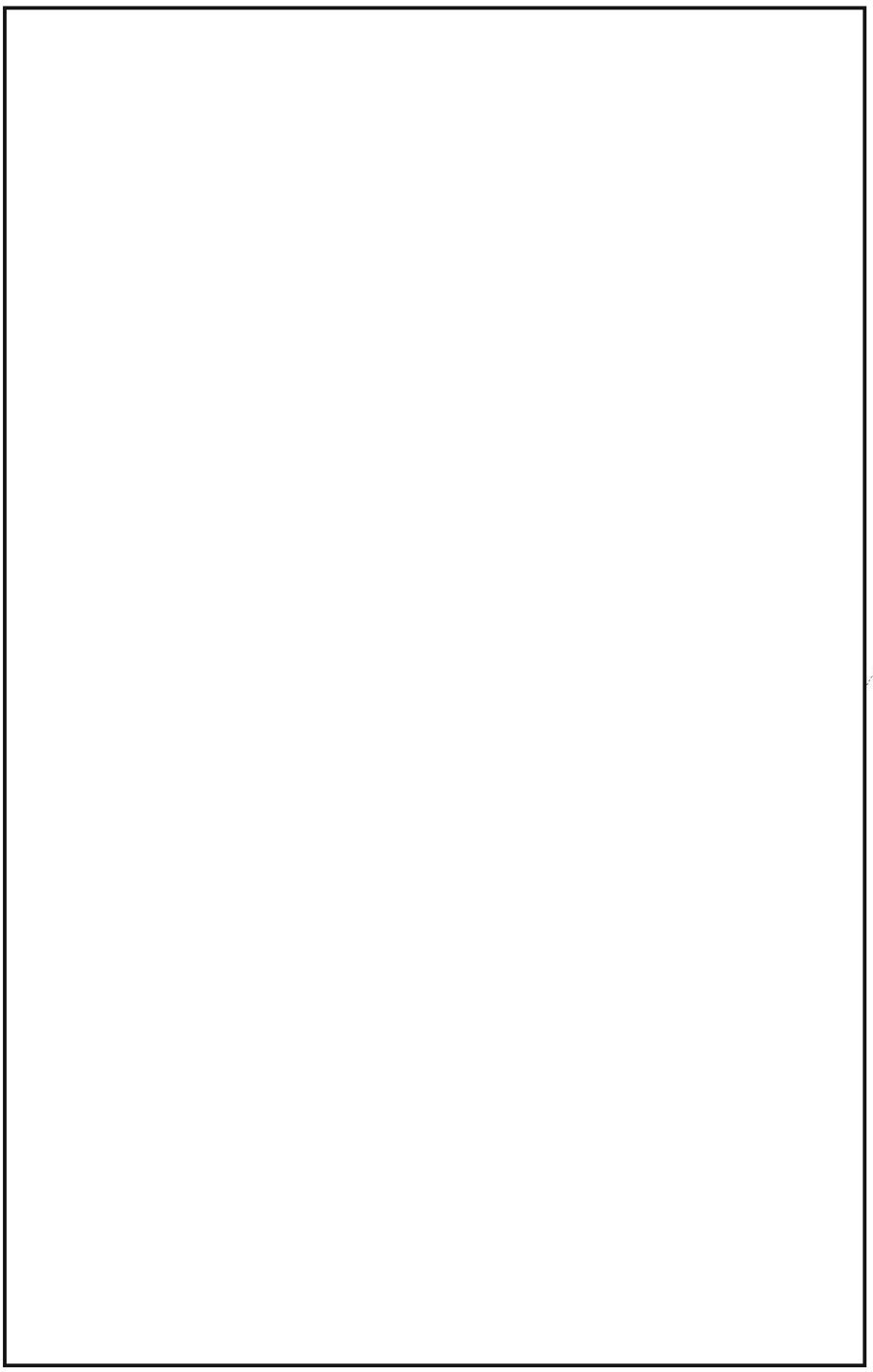
I have thought it desirable to dwell at some length on my pre-war and wartime Japanese experiences because hardly any of it is on record. It remains to say something about the Japanese Military Attaché cipher used throughout World War II. I took some part in the diagnosis of this system, and I believe I was the first actually to read messages in it. For some reason the workups of the initial break-in to the system are lost. About the end of 1941 I had to rescue the material from a party of French cryptanalysts who had remained with us after the fall of France. I had given it to them as a task when I and my research section were fully occupied with German problems, and they had diagnosed it wrongly as a combined substitution and transposition system and had got the intercepts into a hopeless tangle. By the time I first came to Washington in March 1942 I and my section had partially recovered the indicating system and had diagnosed the cipher as a literal additive system with indicators which gave the starting and ending points for messages rather in the manner of the military 4-figure system previously described. It became clear that the normal practice was to tail successive messages rigorously through the additive tables, i.e., to start reciphering each message with the additive group following the last group of the preceding message. It was clear that pages of the additive contained 400 letters but I believe I was the first to prove that the pages of key contained 80 5-letter groups and not 100 4-letter groups as had been expected on the analogy of the 4-figure military systems. Some time after returning to Bletchley I set to work on a large number of messages emanating from some unplaced station in the middle of Europe. Here it was clear from the indicators that the sender had tailed right round his additive table 5 times and it was



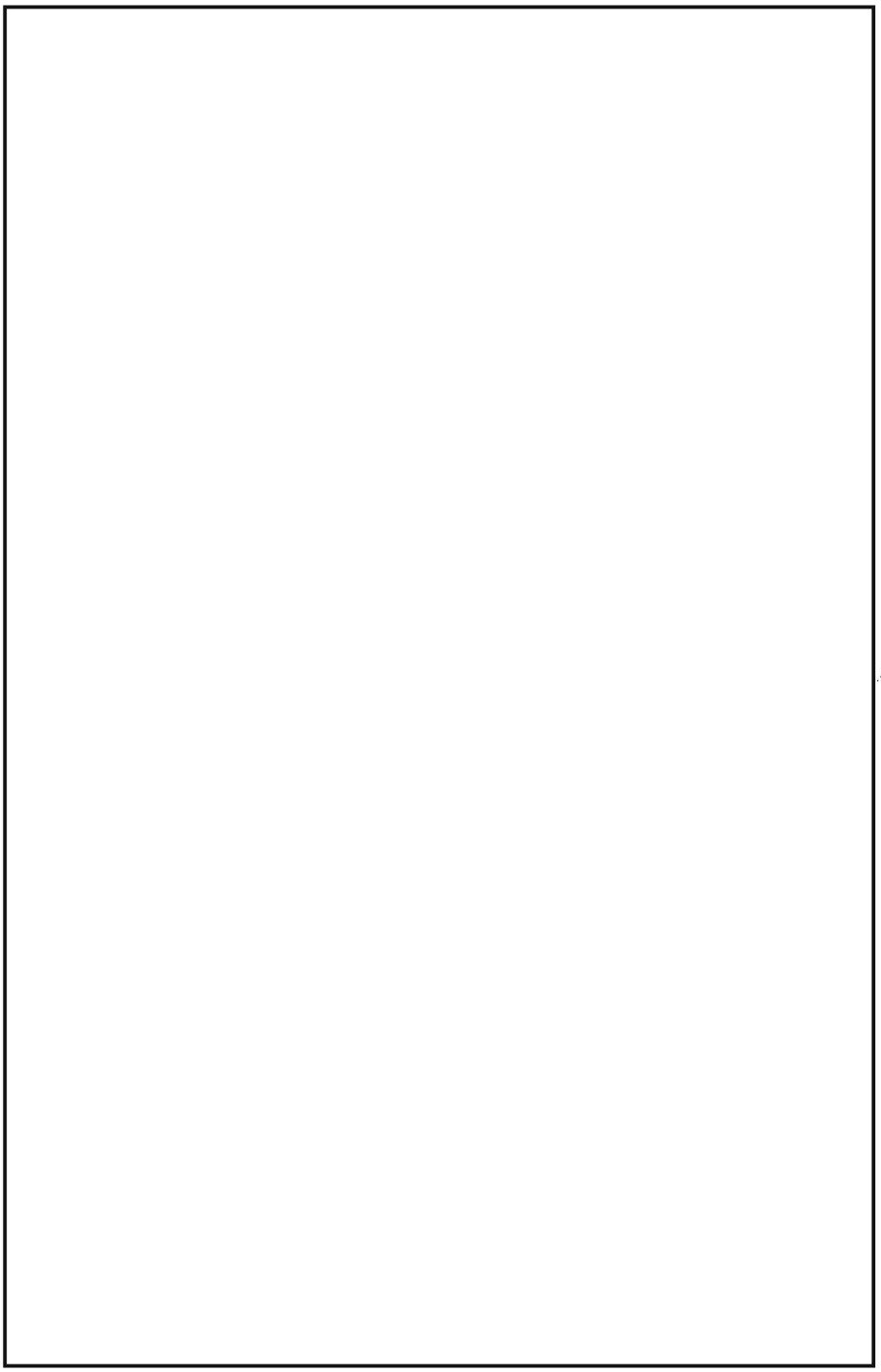
EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



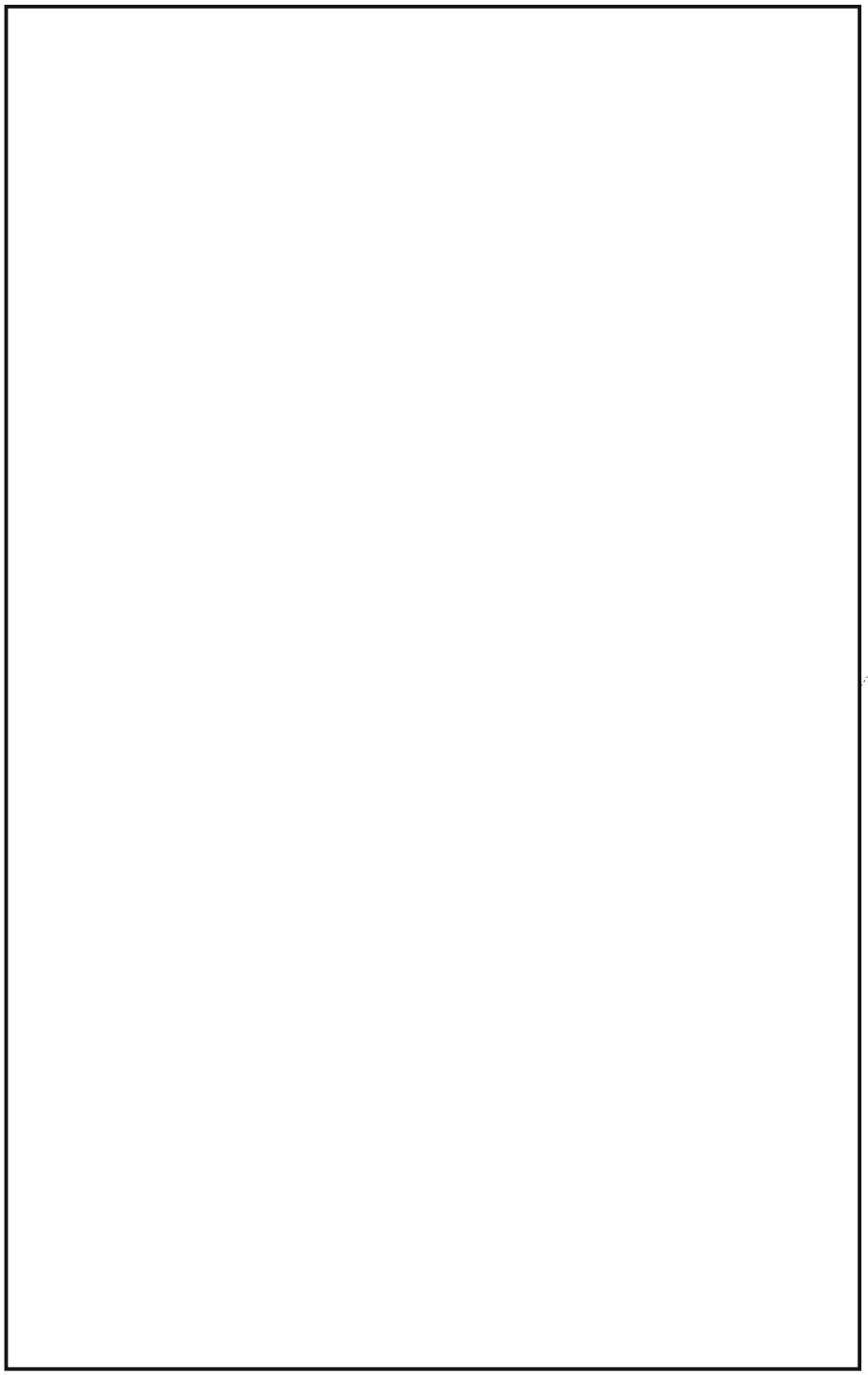
EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



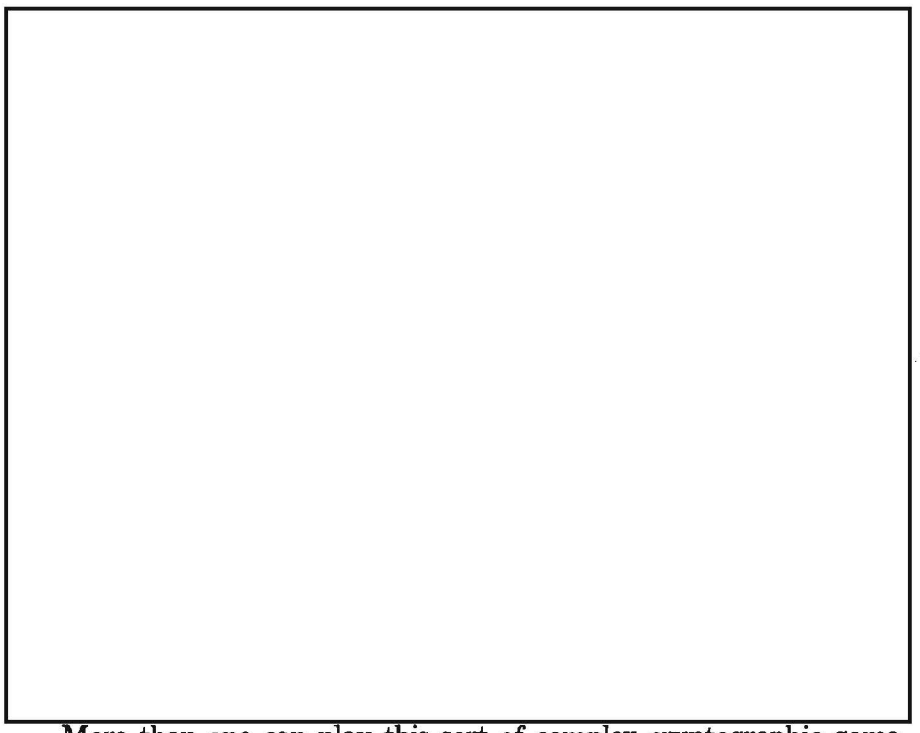
EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



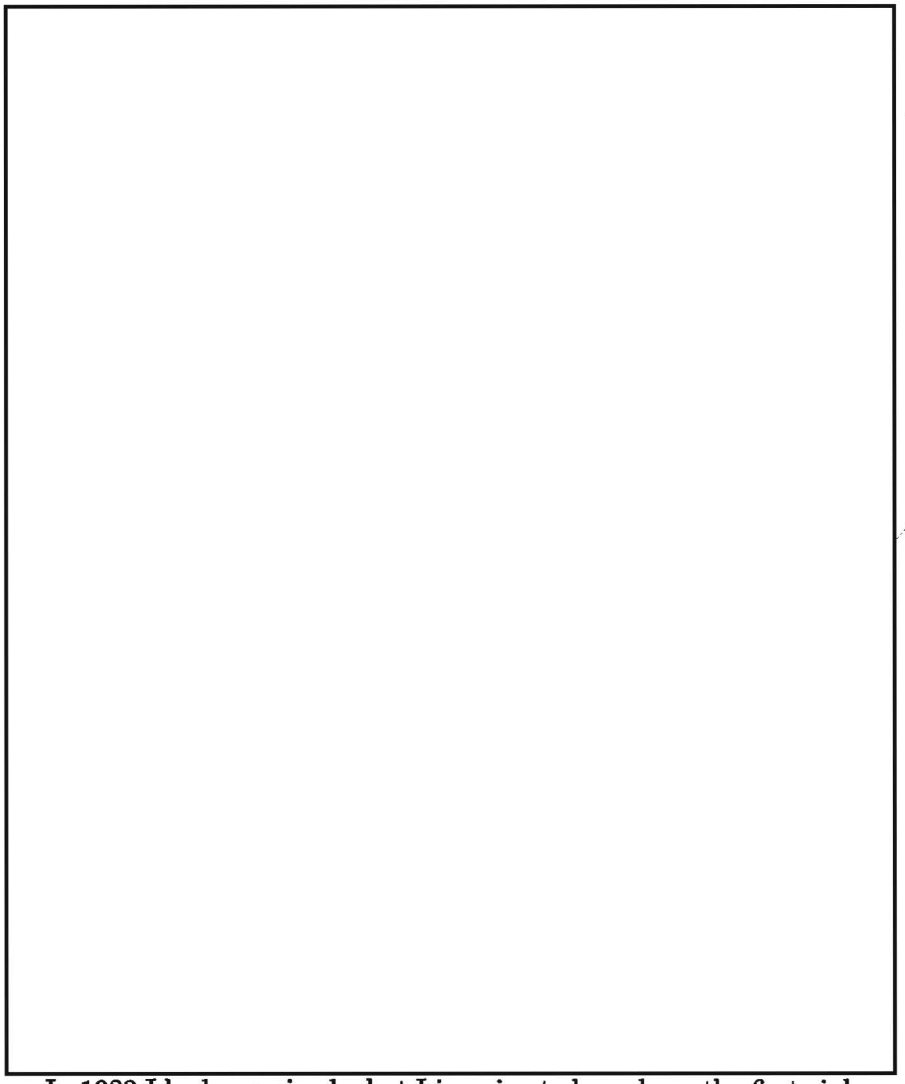
More than one can play this sort of complex cryptographic game as I would like to show by recalling one of the cipher systems I designed. Sometime in 1944 the War Office put up to me for security assessment a field cipher they had produced for use within divisions. I believe what the designer had in mind was an improvement on the old American "Strip" system. I didn't like their idea much and redesigned it. My design was called "Linex," and it was issued in the form I laid down and extensively used in the field. I was rather surprised at its acceptance as I thought it extremely cumbersome. Fig. 12 displays the top of one of the pages of the book of alphabets issued as part of the cryptographic materials. There are 25 such pages in the book lettered A to Z (omitting the letter I), and in each there are 42 mixed alphabets each repeated twice on a line; on each page, 25 of the 30 top lines are lettered. There are, in addition, 10 cursors; one of them described for indicating purposes by either S or T is shown laid under the fourth line D on page T. Supposing that the "true" indicator for a message is TDSZ—then the operator goes to page T and lays cursor S under line D. He also marks the letter Z in the alphabet at the top of the cursor. To start enciphering, the operator slides the cursor until the marked letter Z lies under the first letter to be enciphered and enciphers it by the letter lying in the cut-away square on the right hand side of the cusror. He then slides

the cursor down one line and enciphers the second letter in the same way. The ten cursors, some indicated by 2 variant letters and some by 3, have cut-away squares in the 10 different possible positions and each has its own mixed alphabet at the top. The true indicator is derived from a disguised indicator by use of a Playfair 5 x 5 square giving two digraph equivalents according to normal Playfair rules, the first digraph giving the starting page and line and the second the cursor to be used and the letter to be marked in its alphabet. The Playfair squares were prepared separately for each division by the division concerned, and the disguised indicators were chosen from a list of 4-letter groups supplied by division to each holder of the cipher, marked off and not used again.

To start with, there are 250 ways in which a message can be enciphered, and message to message repeats can only occur when two messages are enciphered in the same way. A tremendous amount of material would have to accumulate in order to provide workable message-to-message overlaps.

when I got the first solution in 1942 of the usage of the commercial Enigma for the German railroad control. I had a to work on, but I only succeeded because the underlying plain texts were of a very stereotyped nature and because the alphabets were subject to the limitation of Enigma-type rotor machines, i.e., that a plaintext letter can only be represented by a different letter in cipher. I feel confident that very little if anything could have been read in our use of Linex.

EO
1.4.(b)
EO
1.4.(b)
EO
1.4.(d)



In 1933 I had conceived what I imagine to have been the first cipher employing a grille additive. Fig. 14 shows a sketch of the device drawn from memory—the prototype I lashed up has not survived. It was based on a cylinder inscribed with 48 lines of random digits. Over this cylinder a moveable sleeve was fitted. The sleeve carried 24 lines of 4-figure windows, 5 windows to a line arranged at random, the lines corresponding to alternate lines of the basic cylinder. It could be clamped to any one message against the cylinder in 5 consecutive lateral and 48 vertical positions, i.e., 120 in all, and encryption by addition could start at any of the 24 lines and proceed for a limit of 120 groups. Further, the internal cylinder was divided into

8 cylindrical segments of different length and these segments could be locked on the shaft in any order and the lines of digits aligned with one another at any setting. The segments of the cylinder were inscribed with red letters for setting purposes. An effective disguise for the starting points and settings was not worked out at the time. My intention had been to provide very large numbers of different additive series set by memorisable keywords. As it turned out, my suggestion was, I think, in advance of its time, and neither my office nor I realised the possibilities of a grille additive system.

[redacted]

EO
1.4.(b)
EO
1.4.(c)
EO
1.4.(d)

[redacted]

足 身 車 辛 辰 辵 邑 酉 釆 里 　　　　7 Str. Rad. 一四九

一四 11200 護 Go. *Mamo(ru)* to protect; defend.
送 *Gosō* to escort; send under guard.
衛 *Goei* to guard; protect.
謨 *Gomu* gum; rubber.
11197 譴 Ken. *Shika(ru)* to scold; to reprimand.
責 *Kenseki* censure.

一五 11207 讀 Doku; toku; tō punctuation. *Yo(mu)* to read.
方 *Yomikata* the way of reading; reading.
本 *Tokuhon* reader (book).
合 *Yomiawa(seru)* to read and compare or verify.
者 *Dokusha* reader (person).
書 *Tokusho* reading.
破 *Dokuha* read through.
書三昧 *Dokusho-sammai* constant reading.
會 *Dokukai* reading (of a bill).
誦 *Dokushō* recitation.
難 *Yominikui* hard to read.
11219 讃 See 11229 讚 149,19.

一六 11220 讐 Shū to avenge. *Ada*: *kataki* enemy.
討 *Katakiuchi* revenge.

一七 11222 讓 Jō. *Yuzu(ru)* to defer; be inferior; transfer.
合 *Yuzuriai* compromise: mutual concessions.
歩 *Jōho* concession.
受 *Yuzuriuke* transfer; receive.
渡 *Yuzuriwata(su)* to transfer; hand over.
與 *Jōyo* concession; transfer.
11224 讒 Zan to slander; to accuse.
言 *Zangen* slander; calumny.
誣 *Zambu* a false charge.
謗 *Zambō* slander; calumny.

一九 11229 讚 San eulogy. *Ho(meru)* to praise: *tasu(keru)* to assist.
岐 *Sanuki* p. n.
美 *Sambi* praise; commendation.
美歌 *Sambika* a hymn.
嘆 *Santan* admiration.
辭 *Sanji* a eulogy.

一五〇 **谷**

11234 谷 Koku. *Tani* valley: *kiwama(ru)* to be in a fix. (*Ya*). (*Yatsu*).
川 *Tanigawa* mountain stream.
間 *Tanima* a ravine.

二 卻 See 却 26,5.

三 11274 郤 Geki. *Sukima* crevice: *hima* leisure. 【色】

425

Fig. 3.

ELEMENTARY *KANA* SYMBOLS

(*Kata-kana* above; *Hira-gana* below).

Note that *i* and *e* are repeated in the Y column, and that *w* is repeated in the W column.

パ	バ	ダ	ザ	ガ	ワ	ラ	ヤ	マ	ハ	ナ	タ	サ	カ	ア
ぱ	ば	だ	ざ	が	わ	ら	や	ま	は	な	た	さ	か	あ
pa	ba	da	za	ga	wa	ra	ya	ma	ha	na	ta	sa	ka	a
ピ	ビ	ヂ	ジ	ギ	キ	リ	イ	ミ	ヒ	ニ	チ	シ	キ	イ
ぴ	び	ぢ	じ	ぎ	ゐ	り	い	み	ひ	に	ち	し	き	い
pi	bi	ji	ji	gi	(w)i	ri	(y)i	mi	hi	ni	chi	shi	ki	i
プ	ブ	ヅ	ズ	グ	ウ	ル	ユ	ム	フ	ヌ	ツ	ス	ク	ウ
ぷ	ぶ	づ	ず	ぐ	う	る	ゆ	む	ふ	ぬ	つ	す	く	う
pu	bu	zu	zu	gu	(w)u	ru	yu	mu	fu	nu	tsu	su	ku	u
ペ	ベ	デ	ゼ	ゲ	エ	レ	エ	メ	ヘ	ネ	テ	セ	ケ	エ
ぺ	べ	で	ぜ	げ	ゑ	れ	え	め	へ	ね	て	せ	け	え
pe	be	de	ze	ge	w)e	re	(y)e	me	he	ne	te	se	ke	e
ポ	ボ	ド	ゾ	ゴ	ヲ	ロ	ヨ	モ	ホ	ノ	ト	ソ	コ	オ
ぽ	ぼ	ど	ぞ	ご	を	ろ	よ	も	ほ	の	と	そ	こ	お
po	bo	do	zo	go	(w)o	ro	yo	mo	ho	no	to	so	ko	o

ン (*Kata-kana*), ん (*Hira-gana*) n (end of syllable).

Fig. 3A.

跋

國語に關する書庫にして最完備せるは、東京帝國
年四月同文科大學助手に任ぜられ、此書庫の一椅子
博士上田萬年先生指導の下に國語の研究に從事する
に及び、數多き字書各特色を有すと雖、國語辭書と
ひ、殊に倭名抄・字鏡集・倭玉篇乃至節用集の如き、

Fig. 4.

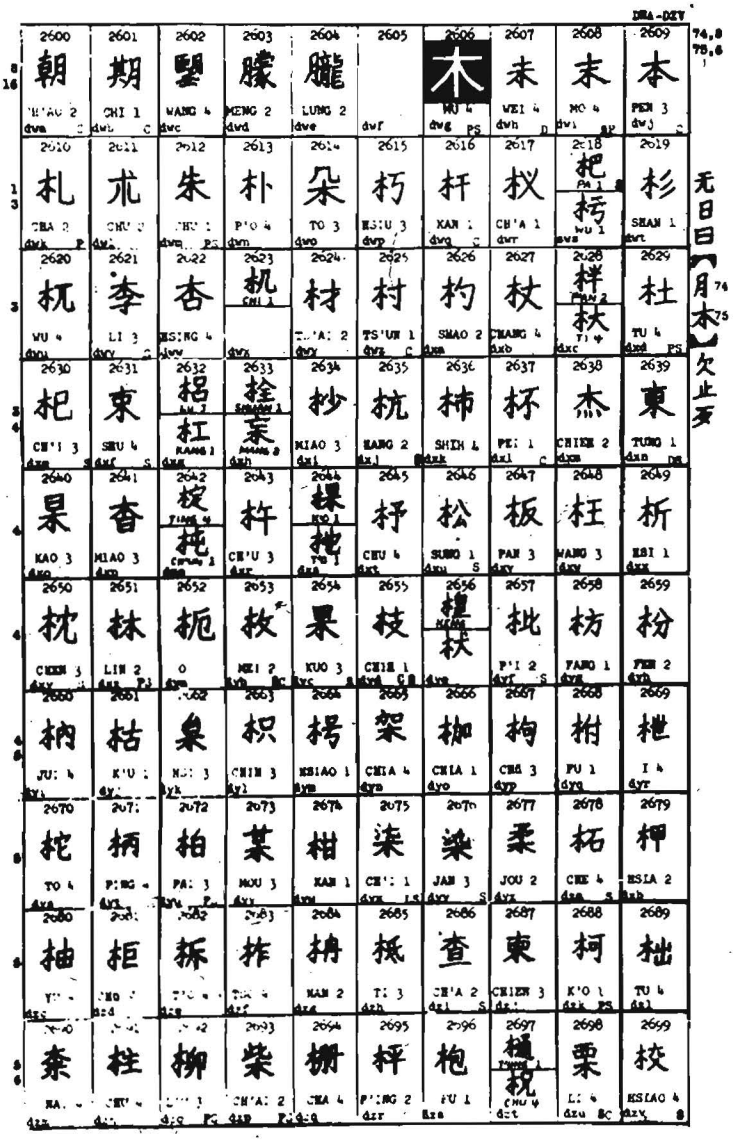
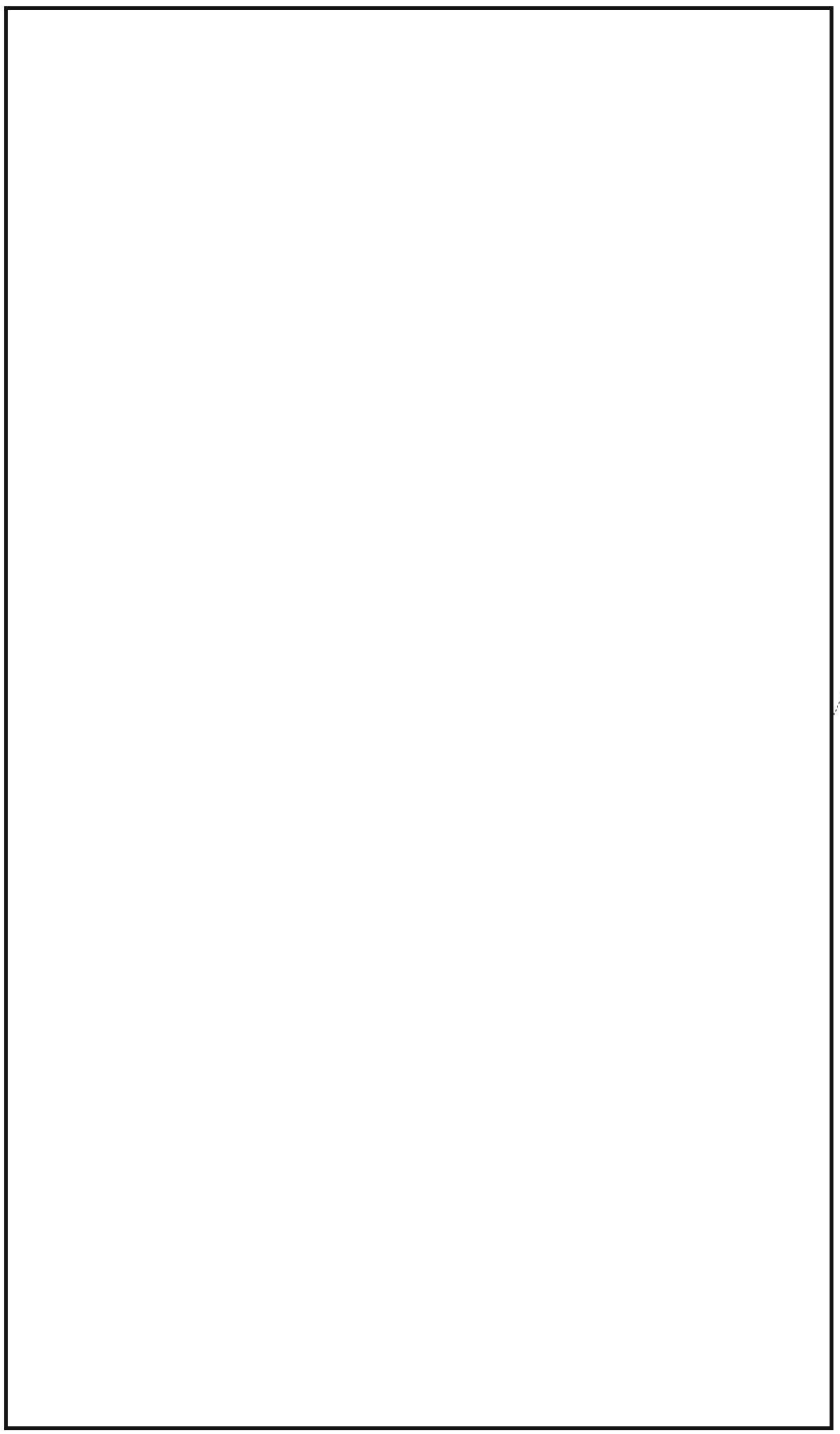
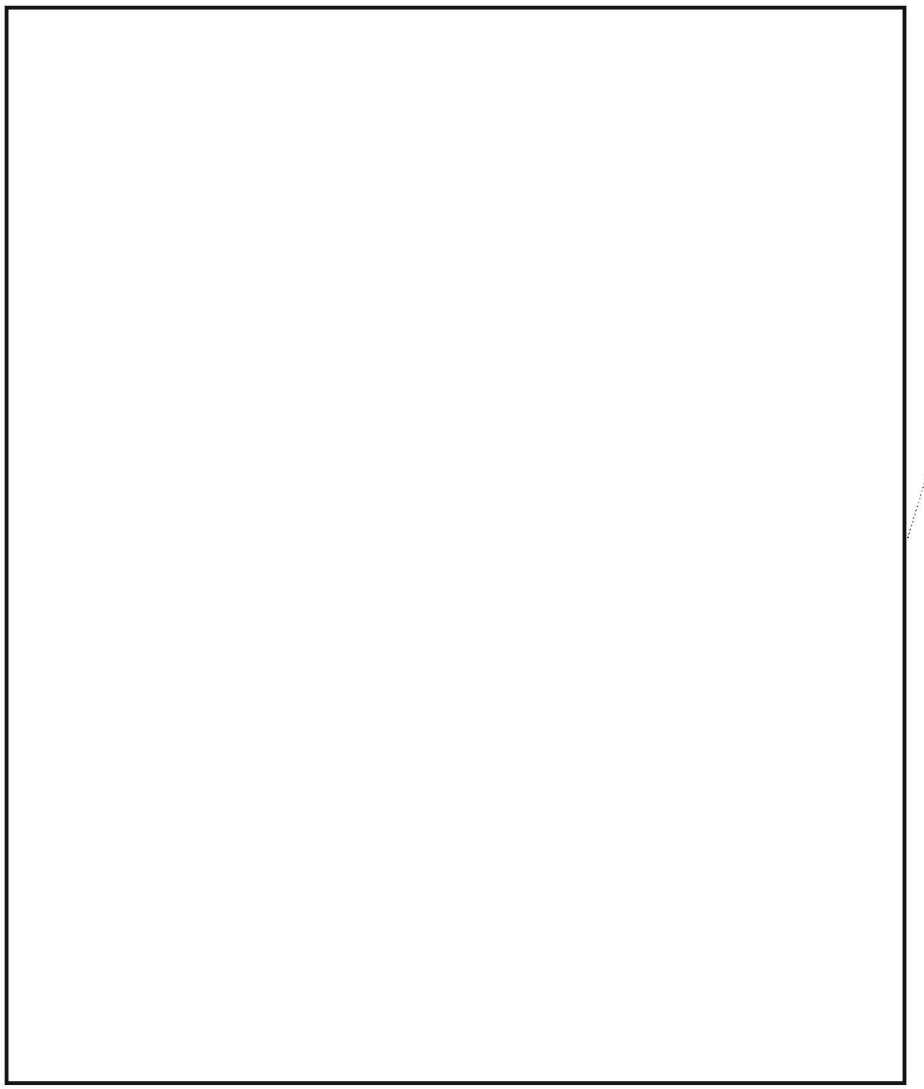


Fig. 5.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

~~TOP SECRET TRINE~~

DOCID: 3838686

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

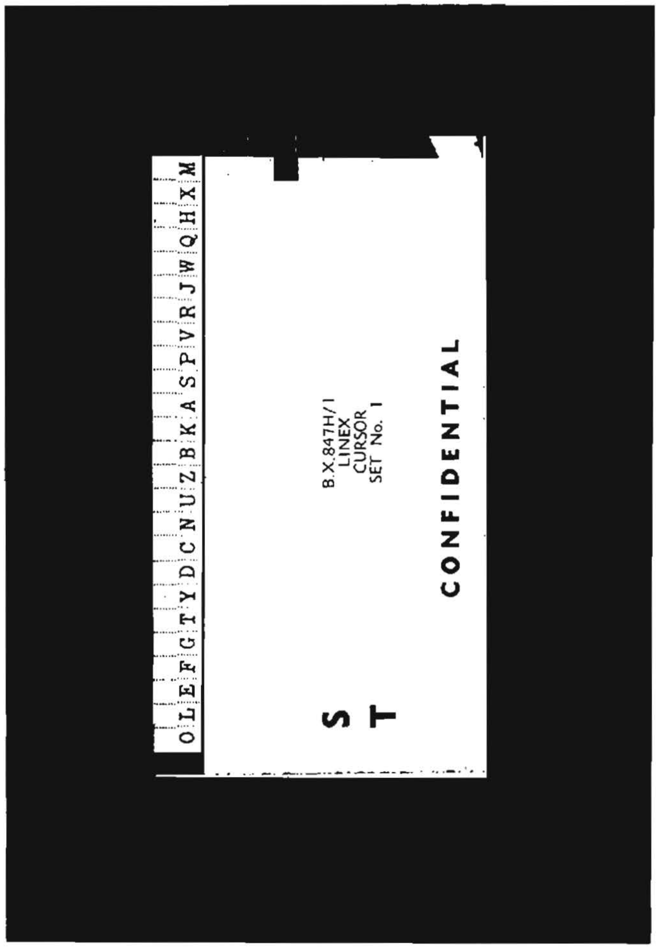
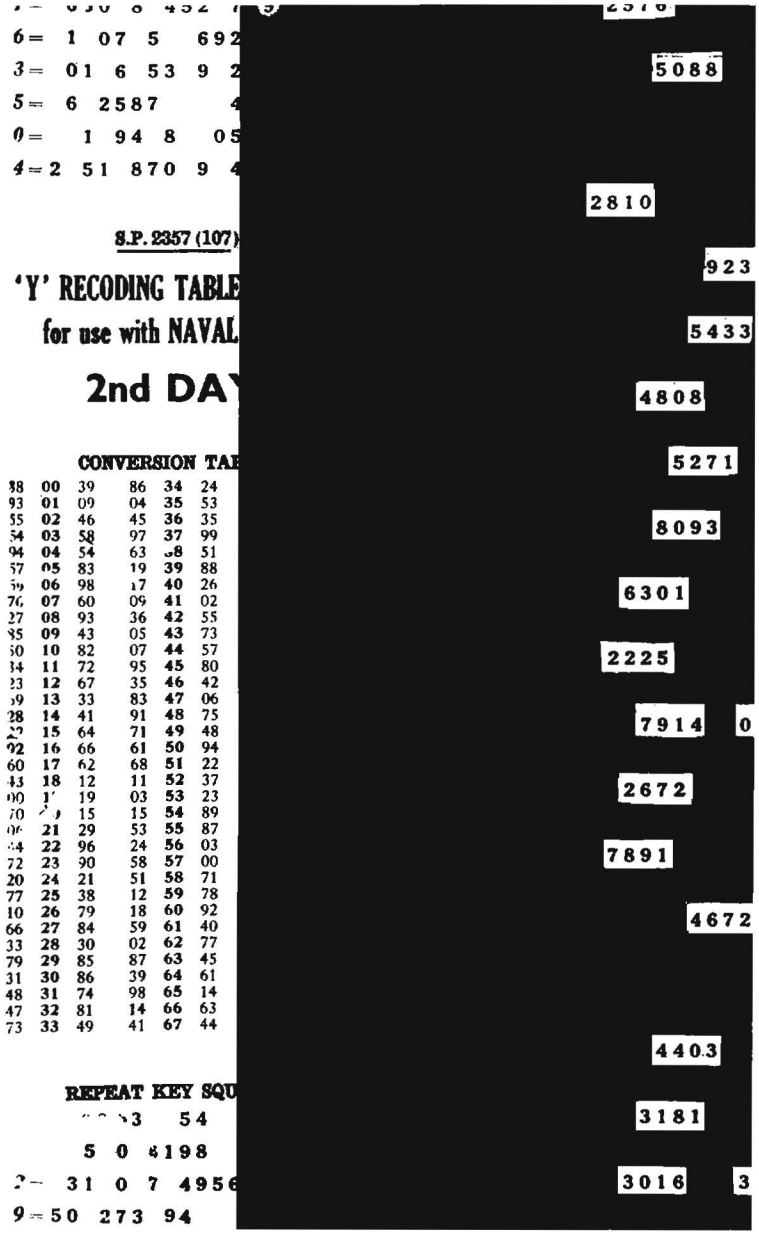

O L E F G T Y D C N U Z B K A S P V R J W Q H X M
S
T
B.X.847H/1
LINEX
CURSOR
SET No. 1
CONFIDENTIAL

Fig. 12.



6= 1 07 5 692

3= 01 6 53 9 2

5= 6 2587 4

0= 1 94 8 05

4=2 51 870 9 4

S.P. 2357 (107)

'Y' RECODING TABLE

for use with NAVAL

2nd DAY

CONVERSION TAB

38	00	39	86	34	24
93	01	09	04	35	53
55	02	46	45	36	35
54	03	58	97	37	99
94	04	54	63	38	51
57	05	83	19	39	88
59	06	98	17	40	26
76	07	60	09	41	02
27	08	93	36	42	55
85	09	43	05	43	73
30	10	82	07	44	57
34	11	72	95	45	80
23	12	67	35	46	42
29	13	33	83	47	06
28	14	41	91	48	75
22	15	64	71	49	48
92	16	66	61	50	94
60	17	62	68	51	22
43	18	12	11	52	37
00	19	19	03	53	23
70	20	15	15	54	89
06	21	29	53	55	87
44	22	96	24	56	03
72	23	90	58	57	00
20	24	21	51	58	71
77	25	38	12	59	78
10	26	79	18	60	92
66	27	84	59	61	40
33	28	30	02	62	77
79	29	85	87	63	45
31	30	86	39	64	61
48	31	74	98	65	14
47	32	81	14	66	63
73	33	49	41	67	44

REPEAT KEY SQU

3 54

5 0 8198

2= 31 0 7 4956

9=50 273 94

2576

5088

2810

923

5433

4808

5271

8093

6301

2225

7914 0

2672

7891

4672

4403

3181

3016 3

Fig. 13.

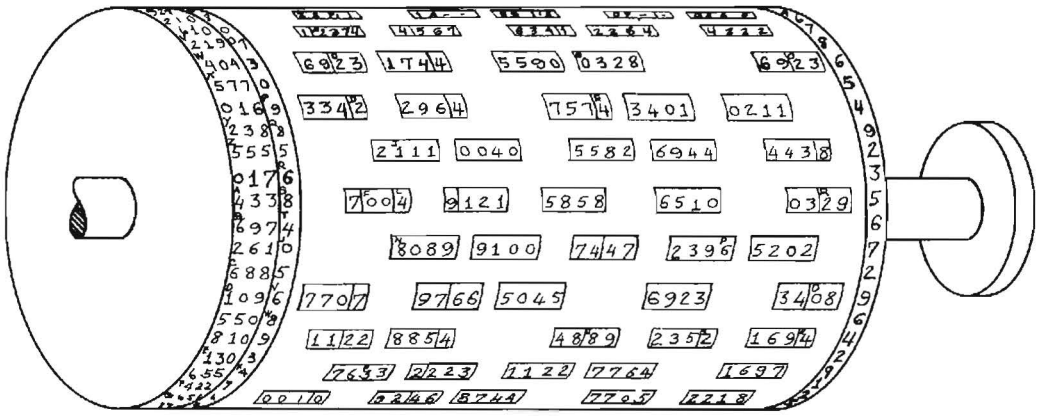


Fig. 14.