Chapter 3. Japanese Diplomatic Cyphers: Cryptographic Survey Report Of Special Intelligence Section HQ Australian Military Forces Melbourne 1946[1]

Introduction

Part I: The Codes

1. NU (Date and Number Code)
2. TO (Address Codes)
3. LA Code (JAH)
4. X Code (JAI)
5. CA (Head of Mission) Code (JAJ)
6. YO Code (JAK)

Part II: The Transposition Cyphers

1. FUJI (TSU) Cypher (JAF)
2. GEAM Transposition System (JBB)
3. BA (TOKI) Cypher (JBA)

Part III: The Recyphering Tables

1. Cypher Book No. 1 (JBC)
2. NE (JAM)
3. SOSOS (JBN)
4. 10101 (JBD)
5. JAO
6. 50505 (JBE)

1 National Archives of Australia, Series A6923/2, Item 1.

Part IV: Breaking the Recyphering Tables

1. Letter-Figure Substitution
2. Placing of Messages in Depth
3. Breaking of Additives
4. Indicator Systems

Part V: Miscellaneous Cyphers

1. HINOKI Machine Cypher (JAA)
2. SAKURA Emergency Cypher (JBL)
3. Unidentified Cyphers

Part VI: General Remarks

1. Code-Building
2. Cypher Systems
3. Errors in Encyphering
4. Distribution of Cyphers
5. Cooperation with Linguists

Part VII: Personnel 1942–45

Appendices[2]
A: Best Groups
B: Starts and Ends
C: R7F Low-Power Far Eastern Diplomatic Network
L: Code and Keys for GEAM (JBB)
Q: Unused Emergency Cyphers

2 The following Appendices, though referred to in the text, are missing in the xerox copy of the Report that is deposited with the National Archives of Australia — D: Copy of NU (Date and Number Codes); E: Copy of TO (Address Codes); F: Copy of LA; G: Copy of X; H: Copy of CA: I: Copy of YO; J: Standard Japanese Diplomatic Vocabulary (1620 words); K: Copy of FUJI and Catalogue of Recovered Keys and Cages; L: Code and Keys for GEAM (JBB); M: Complete Information on BA: N: [Title Unknown]; O: [Title Unknown]; P: [Title Unknown]. Presumably these were stripped from the original document some time between its creation and its examination by the Department of Defence for access clearance in 1996. [All footnotes in this report were inserted by Sissons.]

Abbreviations

Three-letter nomenclature for diplomatic cyphers

JAA	HINOKI Machine Cypher
JAF	FUJI (TSU) Transposition Cypher
JAH	LA Code
JAI	X Code
JAJ	CA Code
JAK	YO Code
JAM	NE Recyphering Table
JAO	GEAM Recyphering Table (Repeated Indicator)
JBA	BA Foreign Office Transposition Cypher (TOKI)
JBB	GEAM Transposition Cypher
JBC	Cypher Book No. 1 (Foreign Office)
JBD	10101 Interdepartmental Recyphering Table
JBE	50505 GEAM Recyphering Table
JBL	SAKURA Emergency Cypher
JBN	SOSOS Foreign Office Recyphering Table

Introduction

Work on Japanese diplomatic cyphers was first begun by the Section in December 1941 under the auspices of the Navy. During 1942, the staff consisted of only three cryptographers, but after the Section was taken over by the Army in November of that year, the technical staff was increased to deal with new cyphers. Professor A. D. Trendall of the University of Sydney was in charge of cryptography, assisted by Lieutenant R. S. Bond and Lieutenant E. S. Barnes. Mr. C. H. Archer of the British Consular Service supervised the language and translation section, and on his return to England in December 1944, Mr. R. L. Cowley was sent to replace him.

When the Section began work on Japanese diplomatic cyphers in February 1942, there were in force four codes, LA (also known as JAH), X (JAI), CA (JAJ)

and YO (JAK), and two cyphers, HINOKI machine (JAA) and FUJI/TSU (JAF). All were used in conjunction with the Number (NU) and Address (TO) codes. The four codes, together with NU and TO, had already been broken and copies were supplied to this section. LA, X, NU and TO were virtually complete, but CA and YO required considerable expansion and correction.

During l942, all four codes and virtually all traffic in the FUJI cypher were being read locally, and the breaking of the daily keys for FUJI was the principal task of the section at the time. Traffic in JAA (the highest grade of Japanese diplomatic cypher) was sent direct to London where a copy of the HINOKI machine was held.[3]

Between 1943 and 1945, the Japanese introduced eight new cyphers — two transposition systems and six recyphering tables. The Section was the first to break the new Greater East Asia Ministry transposition cypher (GEAM) introduced in July 1943. The breaking of the Foreign Office transposition cypher (BA) followed soon afterwards, and the Section concentrated on working out the available keys, while London turned to the machining of traffic in the recyphering tables. Once London was able to establish preliminary facts about the recyphering tables, the Section contributed code-equivalents and many pages of the pads, although relying upon recovery by hand without any mechanical aid.

Approximately 90 per cent of traffic received in these cyphers was read.

Intelligence Derived from the Messages

Messages sent in code rarely contained any important information, as the Japanese themselves realized that their codes had little security value.

Low-grade cyphers were chiefly confined to financial and staffing problems within the various embassies, visas, couriers, rations and similar routine matters.

Traffic in high-grade cyphers showed the reaction of the enemy to naval, military and political events abroad, and in addition provided a reliable general picture of the situation within Japan itself.

An idea of the importance of reading diplomatic cyphers may best be gained by mentioning a few examples of information received.

Of considerable local interest was a message despatched by the Japanese representative at Dili which revealed that the enemy was reading the Australian guerrilla code in Timor.

---

3 In the American literature on this subject, JAA is often referred to as the PURPLE cypher and the HINOKI machine as the PURPLE, the Type-97 Injiki, or the Type-B, Machine.

The official Japanese attitude to the general war situation was regularly circulated by Tokyo, with particular reference to their reaction to 'Big Three' conferences or negotiations with the Soviet. The earthquake off Nagasaki and the American bombings of Japan were reported in full, including complete details of damage and casualties.

Posts abroad regularly sent through diplomatic channels reports from their spies and agents. Spy reports on the European and Russian front were frequently received from the Minister at Stockholm; Kabul was the nerve centre of a spy organization throughout India and the reading of their reports enabled us to supply the Indian authorities with information about the movements and activities of these agents. In 1942 one message from Kabul revealed that a Japanese agent was present at a British naval trial, and was supplying full details of carriers and battleships stationed at Bombay. Spy reports, dealing with the internal situation in China, came from an agent at Chungking and were transmitted to Japan from the embassy at Canton. One of these messages disclosed that the French Minister at Chungking was in the pay of the Japanese.

Information about Chandra Bose and his puppet government was obtained from messages sent from Rangoon and other places visited by the Indian National Government.

Posts in occupied Europe constantly sent detailed accounts of the effectiveness of Allied bombings on their respective cities, and long reports upon local politics.

Russo-Japanese relations were always delicate, and from a survey of reports submitted by Ambassador Sato recording his interviews with Molotov and Lozovsky, the gradual hardening of the Russian attitude became apparent.

For several months before the Russian entry into the Far Eastern War, reports were coming through from Japanese couriers via the Vladivostok consulate on the eastward movement of troops and material.

Much material recovered from Japanese diplomatic cyphers was of use to the Ministry for Economic Warfare in London. Reports from Far Eastern posts were mainly of an economic nature, generally trade reports and statements of shortages. Up to the end of 1942 shipping information was often sent in diplomatic cyphers but thereafter this practice was discontinued. However, we were able to follow the progress made by the Japanese in the building of wooden ships in French Indo-China and Siam to alleviate their shipping shortage. In addition air raid reports came frequently from Bangkok, Hanoi and Chiengmai [Chiang Mai]. London displayed a marked interest in the Japanese need for supplies and commodities, particularly Swedish ball bearings and Turkish chrome.

Part I: The Codes

1. NU (Date and Number Code)

2. TO (Address Codes)

3. LA Code (JAH)

4. X Code (JAI)

5. CA (Head of Mission) Code (JAJ)

6. YO Code (JAK)

1. NU (Date and Number Code)

This code was used in conjunction with most Japanese diplomatic codes and cyphers.

The date and serial number of each message were contained in a single five-letter group generally immediately preceding the cypher text. In this group the first three letters designated the serial number, the fourth letter the part number and number of parts, and the fifth the date and the period of day (i.e. morning or afternoon).

The complete alphabet was used in each part of this code (e.g. *ADYIP* indicated No. 304, Part 1 of a two-part message, sent on the morning of the 31st of the month).

Serial Number

There were two separate codes used, one for ordinary (place-to-place) messages and the other for circulars.

In the 'hundreds' place, each letter of the alphabet was assigned a number from 0 to 25 at random. The numbers assigned to the one letter for circular and ordinary messages added up to 25 — e.g. B (ordinary) = 0, B (circular) = 25. For numbers beyond 2,599, two thousand was subtracted before encoding — e.g. 2600 would be encoded as 600. There was little chance of confusion, as few series ever reached such high numbers, and in those which did, several months separated the identically encoded numbers.

For the 'tens' and 'units' places, the figures 0 to 9 were distributed over the alphabet at random, a few letters being left blank in each column. In no case was a letter left without a figure equivalent in the corresponding columns of

both circular and ordinary numbers. This fact sometimes helped in establishing doubtful cases (e.g. If E occurred in the 'units' place, the number had to be a circular because E had no equivalent in the ordinary 'units' code).

In June 1943 the circular and ordinary codes were interchanged. Thus whereas ADY had signified Message 304, it now became Circular Message 304. There was no further change in the code at any stage.

Message Parts

The fourth letter of the date-and-number group designated the parts of messages. Each letter was given an equivalent ranging from 'single-part message' to 'part six of a six-part message'. There were six optional letters for 'single-part message', and one for each part of two-, three-, four-, five- and six-part messages. When a message exceeded six parts, all its parts were externally encoded as single-part messages and numbered internally (i.e. within the cypher text). This practice often proved of real assistance in the breaking of recyphering tables and in the finding of initial 'fits' in BA. Occasionally the several parts of a multi-part message were designated in LA code before the cypher text.

Date

The final figure only of the date (except in the case of 31st) was encoded. Each of the figures 0 to 9, and 31 was allocated two letters at random, one for morning and one for afternoon. The remaining four letters were reserved for special cases (e.g. 'date in text'). Thus B in the final place of the date-and-number group could designate the morning of either 10th, 20th or 30th of the month, the precise date normally being clear from the date of transmission. In the case of delayed messages confusion could arise, but generally traffic records decided any uncertainty.

Reference Code

When a message referred to a previous message an additional five-letter group was inserted between the date-and-number group and the beginning of the cypher text. In this code the first letter indicated the source of the message referred to (e.g. 'my circular', 'your telegram (+2000)'), the second, third and fourth letters provided the number of that message and the fifth letter the part or paragraph thereof. The whole alphabet was employed for each of the five codes involved, alternatives being freely used. The fifth letter of the group was almost always one of the five choices for 'dummy' (used when the whole message was referred to and not merely a section of it).

Foreign Ministry Revised System

On February 15th 1945 the Japanese Ministry of Foreign Affairs made a change in the date-and-number system, although the Greater East Asia Ministry retained the old system. In the revised system the same code was retained for the numbering and reference sections, but an improved date code was brought into force. The original five- letter groups were each expanded to two groups by doubling each letter, and for the date a bigram was substituted, there being a separate bigram for each day of the year. Thus Circular Message 48, Part 2 of 3, on 28th March in the old system would be BZUXT, but now became BBZZU UXXRH. This new system may have been introduced to diminish the chance of error arising from corruption.

The new date code consisted of bigrams formed at random from consonants. No provision was made to differentiate between morning and afternoon. Sufficient traffic was normally available to establish the code on sequence of messages, but it was possible to check most bigrams by means of the JBC indicator system which employs the date of origin. Occasionally the old date code was used, reduplicated, in place of the bigram code. The new date code was established, virtually complete for dates from 15th February 1945 to early September 1945 when cypher traffic ceased.

For copies of the date-and-number code together with the reference code see Appendix D [Missing].

2. TO (Address Codes)

Both the Greater East Asia Ministry and the Foreign Ministry used the same system of addressing messages but each had its own code. These codes were originally supplied to the Section by London and were complete only in as far as the posts with the greatest volume of traffic were concerned. Efforts were directed towards filling in the missing sections by inference from the texts of messages and from number series, but neither code was recovered in its entirety.

Address codes consisted of bigrams and trigrams, the bigrams being instructions for the distribution of the message (e.g. 'This message is addressed to …', 'Please forward to …'); and the trigrams, place-names. To complete a five-letter group at the end of a series of addresses the fillers SIMO were used. Where re-addressing involved numbering a message in a different series, the original number and address always came last, i.e. immediately before the cypher text. Thus in the Greater East Asia Ministry address code, a message from Shanghai Embassy to Tokyo, which Tokyo is forwarding to Hanoi and Saigon as a circular, would leave Tokyo with the following address code groups:- QQFZQ FVBMO (my message to Hanoi, Saigon) (date and number group) NNCZS (message from Shanghai to

me (date and number group). When a message addressed primarily to one post was repeated merely for information to a number of other posts, the primary addressee was normally indicated at the front, and the remainder at the end of the message.

Copies of the address codes will be found in Appendix E [Missing].

3. LA Code (JAH)

This is a simple code consisting of bigrams and tetragrams, indicated by the letters LA at the beginning of the text. Bigrams are of the form, consonant-vowel or vowel-consonant; and tetragrams are special combinations of two bigrams, the first bigram being, SI, TU, VE, WO or XY. All the letters of the alphabet are used except Q; and Y is regarded as both a vowel and a consonant.

The bigrams are patterned according to the order of the *kana* vowels, i.e. A, I, U, E, O and the tetragrams are arranged in blocks of related words.

LA code has little security value and is used extensively for communications the contents of which the Japanese merely wish to keep from post office officials. However, cypher clerks on rare occasions did make the mistake of sending confidential matter in LA code but, on the whole, LA messages contained little of interest and value.

A copy of LA code may be found in Appendix F [Missing].

4. X Code (JAI)

This is an unrestricted alphabetic code of bigrams and tetragrams, indicated by one of the five bigrams IP PA AP AN IK at the commencement of the text. The code book is not patterned and is thus of higher grade than LA. X was not nearly as extensively used as LA — most messages in X coming from Kabul — but its subject matter was usually more interesting.

A copy of X code is attached as Appendix G [Missing].

5. CA (Head of Mission) Code (JAJ)

CA is an unrestricted bigram code held only by the Head of the Mission and is indicated by CA at the head of the text. Its security value is the same as that of X.

The code was usually sent unencyphered, but was occasionally used in conjunction with any one of the current cypher systems.

As only the Head of the Mission was able to decode these messages, the subject matter of CA messages was usually confined to staff problems.

Encyphered CA messages usually contained general statements on policies which Tokyo did not wish to disclose to embassy staffs.

A copy of CA code may be found in Appendix H [Missing].

6. YO Code (JAK)

YO is an unrestricted bigram code indicated by YO at the head of the text.

This code was rarely used, but occasionally appeared encyphered in the same manner as CA. Owing to the small amount of traffic, this code was only partially recovered and is attached as Appendix I [Missing].

Part II: The Transposition Cyphers

1. FUJI (TSU) Cypher (JAF)

2. GEAM Transposition System (JBB)

3. BA (TOKI) Cypher (JBA)

1. FUJI (TSU) Cypher (JAF)

This transposition cypher was current between June 20th 1941 and June 30th 1943, and was the main cypher used by the Japanese for diplomatic communications over this period. The cypher system had already been broken in 1941, and a few basic code groups recovered. Such information as was known was supplied to the Section.

The indicator of FUJI is a five-letter group immediately preceding the cypher text, the first three letters being invariably consonant-vowel-consonant. The initial consonant classifies the message as (a) European, (b) Far Eastern, (c) American, or (d) a Tokyo circular, while the remaining four letters progress in a fixed self-checking cycle. The cypher was designed to be used for a period of one year, all four regions having a separate key for each day, thus giving a total of 1464 keys. At the conclusion of the cypher text a checked five-figure group gives the number of cypher groups (e.g. 13777).

The code is composed of unrestricted bigrams and tetragrams, the total vocabulary of 1576 groups comprising 676 bigrams and 900 tetragrams. This vocabulary is slightly smaller than the standard Japanese diplomatic vocabulary

of 1620 words (v. Appendix J [Missing]). Bigrams are used for *kana*, numerals, punctuation and short commonly used words; tetragrams for paragraphs, place-names, weights and measures, and longer words and phrases. Those bigrams which form the beginnings and ends of tetragrams (e.g. AL, BJ, YM, ZB) are used for dates and spellers.

An encoded message is written into a single transposition form which varies in width from 19 to 25 according to a key supplied by the indicator. The form contains random blanks which are inserted according to the date and which normally change on the 1st, 11th and 21st of each month. The maximum number of blanks is 53, and they are arranged in sets so that no blank is ever isolated. The blanking pattern does not extend below the l2th row of the form.

The Breaking of FUJI Keys

Progress on FUJI was at first slow and difficult. The recoveries supplied to the Section were few and unreliable, and the only keys broken in this country prior to February l942 had been obtained from short messages the contents of which were known or presumed (e.g. messages reporting the departure of such ships as the *Queen Elizabeth* or *Queen Mary* from Sydney Harbour).[4] As FUJI (apart from the HINOKI machine) was the only diplomatic cypher in use at the time, the first task of the Section was to discover a general method for reading all traffic within a few hours of receipt.

The first attack was made on the following lines: An arbitrary width of key was chosen and the cypher text was written out in strips. Efforts were then made to find two strips which when correctly placed side by side produced good basic groups (v. Appendix A). Messages under seventy cypher groups were not worked upon if it could be avoided, because as we had only an elementary knowledge of the code, everything depended upon finding a good 'fit' in the section of the message clear of the blanks. This method of attack was very cumbersome and seldom profitable as the arbitrary width was almost always incorrect, and after a week this method was abandoned.

In March 1942 a member of the British Foreign Office from Singapore who possessed an excellent knowledge of Japanese joined the Section.[5] On the basis of his knowledge of the language a new and more direct attack was made upon the cypher.[6]

---

4 FUJI came into operation on 20 June 1941. The *Queen Mary*'s departures from Sydney after that date during 1941 were 13 June, 29 June, 21 August, 3 September, 15 October, 1 November; the *Queen Elizabeths*'s arrivals were 13 June, 15 October, 15 December.

5 A. R. V. Cooper of the British Government Code and Cypher School.

6 Bond insists that it was Trendall, not Cooper, who devised 'zoning':

> I cannot really accept this paragraph which suggests that it was Cooper who introduced 'zoning'. It was Trendall, and the latent mathematician in him. I was there, and as a minion I did the hack-work. Does this statement mean that the author of the Report was not personally involved in 1942. But the details of zoning on this page are 'spot-on', 100% correct.
>
> (R. S. Bond to D. C. S. Sissons, 15 November 1998)

As the common *kana* symbols *wa*, *wo*, *no*, *ni*, *shi*, and *to* were bound to occur frequently in any message of reasonable length, a search was made for these groups by 'zoning' out the letters of the cypher text which formed these code groups. Owing to a weakness in code construction the common group *wa* had only one equivalent, AG. Consequently AG usually proved a profitable investment for the zoning treatment.

A given letter, say A, was 'zoned' by writing all the 'A's of a message along a line of graph paper and writing, above and below each A the 15 letters which respectively preceded and succeeded it. Although 'zoning' might appear cumbersome the writing out rarely exceeded ten minutes and invariably produced results.

After, say, 'A's and 'G's had been zoned in the above manner they were placed together in turn until a 'fit' was found. To be classified as a 'fit', a column had to contain a high percentage of good groups. Value of groups was the most important factor in determining a fit, but experience alone decided its validity; even though a column might be found containing *shi*, *wa*, *no*, and *to*, if it also contained several rare or unknown groups like AZ or LY there was little chance of its being correct. In addition a correct fit had to be mathematically possible (e.g. letter 178 could not fit with letter 180, however good the resulting groups might be!).

When a fit was found that seemed reliable, the numbers of the letters were studied in an endeavour to establish the width of the key. For example, if a line ending at letter 24 fitted with a line ending at 72, and the message contained 530 letters, the average length of a column was 24 and the key was probably 22 wide. Owing to the bigram and tetragram basis of the code an odd key (i.e. 23 wide) would give a column in which code groups would be formed only on alternate rows. An even key (i.e. 20 wide) would form code groups on every row. At first even keys proved more difficult than odd keys, as columns had to be found separately and then fitted together according to sense; but with odd keys each alternate row had a split group which was of great assistance in fitting on a third line to the original two. For instance if a split group H . Z occurred in a message from South America there was a high chance of this being EHZB, the tetragram for Chile.

If the blanking system for the period was already known, a set of four or five lines was usually sufficient to determine the width of the key and the position of the set in the cage. When this had been done, a very useful device, known as the principle of isolated columns, was used. An isolated line was a section of the cypher text whose beginning and end were determined but which had not yet been fitted. The lengths of all isolated lines were checked off against the calculated lengths of all the lines in the setting. If a certain length occurred

only once, the corresponding isolated line could be immediately written into the form, irrespective of whether it had been fitted to other lines or not. Such isolated lines were extremely useful as 'bridges' in expanding the original fitted lines.

If the cage was not known, all the lines of the message had to be fitted together, the end-point of the message determined by sense, and the number of blanks in each line calculated. The cage was then broken purely on the sense of the message and was, of course, greatly assisted by stereotyped beginnings (v. Appendix B).

Using the method outlined above, by May 1942 we were able to read virtually all FUJI traffic; and all bigrams, except those of very rare occurrence, and most tetragrams had been recovered.

The technique and speed of breaking keys gradually improved to such an extent that 'zoning' could almost be eliminated and the following simpler method was usually adopted: Messages were typed out, numbered, and an 'apartage' marked (i.e. letters were marked which were at a distance of two or four apart, as these distances were easily noted and accounted for both even and odd key-lengths) — e.g. … XZLAN AFKTA … which would be checked with PAQLD GYYOG, giving (since AG = *wa*) two *wa*s. Groups like *wa*, *wo*, *no*, *shi*, *ni* etc were so common in the body of a message that there was a high possibility that they would occur over one another in the same column. If a search for a *wa* over *wa* proved unsuccessful, a *wa* over *no*, or *ni* or *shi* was almost certain to be found. By this method fits came quickly and easily, and from May 1942 onwards it was only in rare instances that the 'hammer' method of zoning had to be adopted to discover an initial fit.

Change 1

On July 1st 1942 the first of three changes in the encyphering of FUJI messages was introduced. In normal times a completely new cypher would probably have been introduced but distribution during wartime to overseas posts prevented the Japanese from changing their cyphers after the usual period. The first change was as follows: The top line of the original cage was removed and the key 'telescoped' (i.e. arranged in the order first, last, second, second-last etc). The instructions for this change were circulated in a SUPER FUJI message (see below) which could not be read, but as soon as a key was broken after July 1st the system was quite apparent.

Change 2

From October lst 1942 messages to and from Europe and South America were encyphered by moving the fifth row of the cage to the top. Far Eastern posts continued to use the system introduced on July 1st 1942. Kabul now used European cages with Far Eastern keys.

Change 3

The third variation in FUJI cypher was introduced on February 1st 1943, when all posts with the exception of the Far East used cages formed by moving the original blanks ten columns to the left. In addition a new key was used, derived from the original key in the following manner: Step 1: To each key number the preceding was added, retaining only the units digit in the sum. Step 2: These digits were then numbered in ascending order from the left to provide the new key.

E.g. Original Key:

11	1	3	8	13	16	5	6	10	19	18	15	12	4	2	17	9	7	14

Step 1: Rewrite, retaining only last digits.

1	1	3	8	3	6	5	6	0	9	8	5	2	4	2	7	9	7	4

Step 2: Repeat this sequence but now put the final digit (4) first.

4	1	1	3	8	3	6	5	6	0	9	8	5	2	4	2	7	9	7

Step 3: Add above two rows in columns without carry

5	2	4	1	1	9	1	1	6	9	7	3	7	6	6	9	6	6	1

Step 4: The new key is obtained by entering down the numbers 1 to 19 in the order determined by first using all 0s, then all 1s, and so on up to all 9s.

0s																		
1s				1	2		3	4										5
2s		6																
3s												7						
4s			8															
5s	9																	
6s									10					11	12		13	14	
7s											15		16						
8s																			
9s						17				18						19			

New Key

9	6	8	1	2	17	3	4	10	18	15	7	16	11	12	19	13	14	5

Although a new key could be derived from the old, no method was found for deriving the original key from the new.

The Ministry at Kabul used the new key method and the new cage while continuing to use Far Eastern and not European keys.

Instructions for the third variation of FUJI encyphering were circulated by Tokyo in a SUPER FUJI message which was afterwards put through the HINOKI machine.

FUJI cypher was discontinued on June 30th 1943. A catalogue of recovered keys and cages together with a copy of the code may be found in Appendix K [Missing].

SUPER-FUJI System

This is a special variation of FUJI with an extremely high security value, and is reserved by the Japanese for communications of a 'most secret' nature. The system was supplied to the Section by London who had read the instructions.

For this special cypher the normal FUJI indicator is repeated at the conclusion of the cypher text. The variation is as follows: Until February 1st 1943, the key in force at the time was reversed in pairs. The first 13 numbers of the new key were taken and the letters A through M were arranged in the order of these figures. Underneath were written letters N through Z in normal order. These thirteen pairs of letters were then used to provide a reciprocal substitution which was applied to the message.

E.g. Using the above mentioned key as original key:

11	1	3	8	13	16	5	6	10	19	18	15	12	4	2	17	9	7	14

Reverse the order in pairs

1	11	8	3	16	13	6	5	19	10	15	18	4	12	17	2	7	9	14

Keep only first 13

1	11	8	3	16	13	6	5	19	10	15	18	4

Insert A through M according to the order of these numbers

A	H	F	B	K	I	E	D	M	G	J	L	C

Write N through Z under these

N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Thus AG in the original code is substituted as NW.

This system is virtually unbreakable, as each message has the equivalent of a new code. Efforts were made by London, Washington and Melbourne to break one SUPER-FUJI message which was known to contain cypher instructions; but without success.

On February 1st 1943 the system changed, but the instructions were circulated in JAA which London read.

This new system is one of double transposition without substitution. In encyphering, the first transposition form is identical with the current form for ordinary FUJI. The second form uses the original cage with the top line removed and a special key derived as follows: If the width of the original key is n, the first n actual digits of the key are written down in order. Underneath these are written the last n digits of the key read backwards. These two rows are then added and arranged in order as described above for FUJI Change 3.

E.g. Using the same original key:

11	1	3	8	13	16	5	6	10	19	18	15	12	4	2	17	9	7	14

First 19 digits

1	1	1	3	8	1	3	1	6	5	6	1	0	1	9	1	8	1	5

Last 19 digits

4	1	7	9	7	1	2	4	2	1	5	1	8	1	9	1	0	1	6

Add without carry

5	2	8	2	5	2	5	5	8	6	1	2	8	2	8	2	8	2	1

Use order of numerals to write new key

1s											1							2
2s		3		4		5						6		7		8		9	
3s																			
4s																			
5s	10				11		12	13											
6s										14									
7s																			
8s			15						16				17		18		19		

New Key

10	3	15	4	11	5	12	13	16	14	1	6	17	7	18	8	19	9	2

Messages in the SUPER-FUJI system were not numerous, perhaps owing to the cumbersome method of encyphering. From the material these messages contained there is every reason to believe that the Japanese believed implicitly that the system was unbreakable. However, they compromised the system by sending both SUPER-FUJI and ordinary FUJI messages in the same key, which meant that a direct attack on a SUPER-FUJI message was rarely necessary; for once the original key had been determined, the SUPER-FUJI could then be decyphered immediately.

2. GEAM Transposition System (JBB)

GEAM was introduced on 21st July 1943. It is a transposition cypher with a bigram and tetragram code, the bigrams being consonant-vowel or vowel-consonant and the tetragrams made up of double consonant and a bigram. All letters of the alphabet are used and Y is regarded as both consonant and vowel. The code is patterned after the manner of LA.

The transposition system has appeared in three forms:

(a) Originally messages were transposed in blocks of ten by ten without blanks. There were 26 indicators, each providing a column and a row order, the row order containing only nine figures, as the bottom row of the cage was composed of dummies, namely the first letter of the indicator repeated ten times. The 26 keys were designated by the letters A through Z and each key was indicated by its letter and the following letter of the alphabet in the form ABABA. The indicator was located at the head of the cypher text.

(b) Shortly afterwards a new system appeared which was used conjointly with (a), but which eventually displaced it. The code remained the same, but the size of the transposition block was altered to 13 by 10, the dummies now being omitted, and a figure check added at the end of the text as in FUJI. Thirteen indicators were used each providing a column order and row order, and were built up on the pattern AZAZA, BYBYB etc, the keys being lettered from A through N excluding M.

(c) A further change was introduced on October 1st 1944. The size of the block was altered to 13 by 13, nine blanks being inserted in the cells with coordinates (1,1) through (9,9). The columnar keys of system (b) were reversed and used as both column and row orders. Any two keys could be used in conjunction. For example, the indicator ABABA gave B as the column order, A as the row order.

The Breaking of GEAM

As this cypher was introduced in a simple form, the breaking of the original system and the two subsequent improvements was not a difficult task. The actual steps of the analysis were as follows:

(a) A frequency count of a few messages showed that consonants and vowels were used in almost equal numbers. As we already had an example of a vowel-consonant, consonant-vowel code (LA), the theory was straightway suggested that GEAM was such a code transposed. The regular occurrence of the dummy letter at intervals of ten gave the probable length of the lines as ten. Moreover, as the dummies appeared at shorter intervals at the end of a message (when the final transposition form was incomplete) and these final dummies always began after a multiple of 100 letters, it was obvious that the size of the block was ten by ten. When a few messages were tested on these theories, fits of the required type were quickly found, while the only discrepancies were groups of the form BB, HH etc. Experience of the Japanese method of code construction showed that these were parts of tetragrams, and the five separate fits for all messages were soon established.

It merely remained to put these groups together on repeats. This part of the job did actually present a few stumbling blocks, as the presence of a row-order was not at first suspected and we were unfortunate enough to have constructed all the repeats backwards. The code-breakers were therefore somewhat baffled when these texts were presented to them — although it was later found that the main difficulty was the fact that the early messages were encoded from an English text.

The first guide to the real solution was given by the incomplete blocks in which an incomplete line of five letters appeared at the end of the line instead of at the beginning. Thus we saw that we had our keys backwards; this was remedied and then long repeats were found going from one line to another, the second line not necessarily being the next in order. From then on the breaking of the code and row order was a relatively simple matter and the complete code and cypher system were known within a fortnight.

(b) On the appearance of the second type of GEAM, the first messages were immediately examined for fits of the required type, but without success. Next day, when two messages in the same key had been received, these were written over one another producing repeats of letters at distances of l3. Moreover these repeats were the letters A D F I S S T U U V V V Y Z; our knowledge of the code immediately showed that these could be anagrammed into the traditional telegram reference: SSZA TI VU VVDY UF (*kiden 12 ni kanshi*). When the letters were lined up correctly in this order it was seen that two adjacent lines contained

both code groups and split groups, and therefore the cage had an odd width and a row order. All 13 keys were then broken as soon as traffic in the keys was received.

(c) The third variation of GEAM was broken by London shortly after its inception. A few keys were broken by the Section and by London, whereupon it was seen that the new keys were the reverse of the previous set.

GEAM was the main cypher of the Greater East Asia Ministry, its other two cyphers JAO and JBE being rarely and spasmodically used. Although GEAM was by no means a high-grade cypher, the Japanese appeared to have no fear in transmitting secret data encyphered by this system. When the Embassy at Bangkok was bombed out the cypher clerk was able to continue sending messages, relying upon his memory for code and keys. This the Japanese regarded as an excellent recommendation for their cypher.

The code and keys of GEAM cypher will be found in Appendix L [Missing].

3. BA (TOKI) Cypher (JBA)

This transposition cypher was introduced on August 20th 1943, and was the first of the new Foreign Office cyphers to be broken.

The code is unrestricted bigrams and trigrams, transposed in blocks 25 by 10. The keys for the blocks are given by a five-letter indicator located at the end of the text. The first letter of the indicator is one of the consonants B, C, D, F, G, the second a vowel (including Y), the third one of the consonants N through Z, and the last two progress in sets of five according to a fixed cycle. Each of the 1,500 indicators is assigned a key number, this key being used for the first transposition block. For the second and third blocks the two following keys are used (e.g. if the indicator BANAY is 127, the first three blocks would have keys 127, 128, 129). Any further blocks repeat the same keys in order.

First System

Ten nulls are inserted in each setting in Column 1 Row 1 through Column 10 Row 10 (according to the key), the nulls spelling out the originator's name, rank and post in English.

Blanks are inserted according to the date, the same blanking system being used for dates whose difference is a multiple of six. Such blanks are always in vertical blocks of five cells, and extend either from Rows 1 through 5 or from Rows 6 through 10. The number of blanks in each block range from 5 to 45, and varied for each block.

Incomplete blocks of more than five rows receive special treatment in that the first five rows and the remaining rows are taken off separately.

Second System

On December 20th 1943 a new system was introduced as follows: Nulls were abolished and fifty blanks were inserted in each block, their location depending upon the key; beginning from Cell 1,1 five blanks were inserted vertically, from Cell 2,2 five blanks horizontally to the right etc, as far as Cell 10,10. Incomplete blocks were now treated in the normal fashion.

Breaking of First System

First a frequency count was made which showed that the code was probably unrestricted as in FUJI. Tentative attempts were made at finding repetitive fits on the same style as FUJI, but no conclusive results were obtained. One message was received which from its count suggested that it was highly numerical, but although certain progress was made on it, the message was unfortunately too corrupt to be of any real use.

Some messages in the same key were written over one another giving repeats at intervals of eleven letters, whereupon it was found that these repeats were nulls. As in GEAM these nulls were regularly spaced except towards the end of messages, suggesting that the encyphering was done in blocks but here difficulties were encountered as the lengths of the separate sections could be 245, 235, 225, 215 or 205. The longer blocks tended to be those at the beginning, but apart from this no rule could be established. The unevenly spaced dummies were naturally examined, but the system by which they were distributed was not at all clear.

Within a fortnight of the introduction of BA, Minister Morishima at Lisbon compromised the system by sending identical messages in two different keys. London was fortunate in intercepting both of these messages and quickly pieced them together. As the message was less than one complete block, it first appeared that the two parts of the block had different keys but these two keys were obviously related and were seen to be identical when sets of blanks were introduced. An analysis of this message gave a few of the high frequency groups and one or two more keys were broken. Our technique was rapidly improving, although almost no code groups were known, when Tokyo sent out a six-part circular in both BA and GEAM. The GEAM cypher was already completely known by this time and all efforts were made to break the BA keys. This done, the equivalents of several hundred code groups were immediately recovered,

the only small difficulty being the presence of trigrams, the form of which was not at all obvious. From now on the breaking of BA keys was merely a matter of technique and experience.

Although the complete system by which the blanks were inserted was not discovered for some weeks, it was roughly known that the blanks were fairly evenly divided between the top and bottom of the cage, the top blanks being in Columns 11, 12 etc and lower blanks in 20, 21 etc. So that if the length of a block were 235 letters, the blanks were either in Columns 11, 12 and 20 or in 11, 20 and 21.

The method of breaking the keys was simply to write out a block in its twenty-five columns, inserting the required number of blanks on the above tentative basis. Fits were not difficult to find as the position of every letter in its line was determined and the whole process was greatly facilitated by stereotyped starts (c.f. FUJI where the beginnings and ends of lines were initially indeterminate). However the presence of trigrams and dummies gave no regularity in the pairing and splitting of two letters as in FUJI.

Virtually all traffic in BA was read until the introduction of the second system.

Breaking of Second System

All attempts to break into the second system failed until in January 1944 we received two small messages in the same key. Both of these were found to possess all the requisite letters for a 'repeat request' (v. Appendix B), and were successfully pieced together although they were so small that the actual key and blanking system could not be completely determined. The result was sent to London who fortunately possessed messages with complete blocks in both the old system and the new. They were thus able to establish the blanking system and to show that the transposition keys had not changed.

New messages in known keys were now readable but the breaking of new keys presented grave difficulties. Doubts were expressed both here and in London whether the breaking of the new system would ever become a working and a profitable proposition in view of the complexity of the system and the necessity of breaking three keys in order completely to read one message. Moreover the main recyphering tables were now well in hand and occupying almost the complete staff of the Section so that for many weeks no work was done on BA.

However, the volume of BA traffic began to increase in April 1944 when it began to be used as an interdepartmental cypher in conjunction with 10101, and it was decided to make serious efforts to evolve a technique for breaking new keys. Progress was slow and very difficult in the early stages and only possible when there were several messages in the same key. Eventually an effective

method of verticalising was found (v. Appendix M [Missing]) whereby we filled in the thirty blanks whose positions were known and distributed the remaining twenty horizontal blanks as evenly as possible. Fitting was of course difficult in view of the shallow depth of the blocks, the presence of unknown blanks, the lack of pattern in the pairing of the code groups and the uncertainty of the beginnings and ends of lines.

One of the main resources was as follows: Messages in the same key were written over one another and each was examined for a stereotyped beginning which would give possible beginnings for all the other messages. (e.g. JOR being *kiden* [meaning: 'your telegram'], letters corresponding to all the Js, Os and Rs in one message would be written down and all combinations of them examined. If for example one found the sets JSK, OBD, RKR, giving *kiden, Ōden* [meaning: 'my telegram'] and the first letters of '1', these lines would be written down and examined as potential fits).

Incomplete blocks were always virtually unworkable and even after a great deal of experience it proved almost impossible to break a key on one message alone. London was the first to discover the principle that the key of Block 2 of one indicator might be identical with the key of Block 1 of another indicator; it was then obvious that indicators could be linked together (See Appendix M [Missing]). This fact was most helpful in that additional depth was obtained when breaking keys. Furthermore if upon the breaking of Block 1 of an indicator it was found that the key was identical with Block 2 of another of which the key for Block 3 was already known, Block 2 of the new message could immediately be decyphered.

Employment of BA

BA was discontinued in April 1945, although the transposition system was used from then on to re-encypher JAA (HINOKI machine cypher) messages and for use in Super JBC described below.

BA was used only to a moderate extent and the material it contained was of varying interest ranging from general Tokyo circulars upon international happenings to dull routine matters about couriers. Most BA messages from Russia were on the subject of couriers, visas and rations. However Stockholm was in the habit of sending all his *chōhōsha* (spy reports) in BA and much information was obtained therefrom. Although the second system of BA cypher might well have proved unbreakable the Foreign Ministry did not regard it very highly and issued instructions that it was to be used only for routine matters; more confidential material was to be sent in the recyphering tables. This was satisfactory from our point of view as we encountered far more difficulty in breaking and reading the second BA system than we did in recovering recyphering tables.

Complete information on BA may be found in Appendix M [Missing].

Part III: The Recyphering Tables

1. Cypher Book No. 1 (JBC)

2. NE (JAM)

3. SOSOS (JBN)

4. 10101 (JBD)

5. JAO

6. 50505 (JBE)

1. Cypher Book No. 1 (JBC)

This is a recyphering table using a four-figure code and sent in five-letter groups with the letter-figure substitution OLFSCGRNYK equivalent to 0 through 9. The code contains 1620 groups with the following restrictions: the first three figures of the groups are all even or all odd; there is no zero in the first, second or fourth places and no 9 in the second place (N.B. This applies only to the code as recovered: it has been shown that the true Japanese code is 1111 lower).

The additive pad contains l00 pages numbered 00 through 99, each page containing 100 five-figure groups arranged in ten rows and ten columns. The rows and columns of each page are separately coordinated.

A dummy indicator of the pattern, consonant consonant vowel consonant consonant, stands at the head of the text. There are two true indicators, one at the beginning and one at the end of the text. The indicators are decyphered as follows: To the first four figures of the actual cypher-text add the day of the month, repeated to form a four-figure group. Use the result to find a five-figure group in the pad, the first two figures being taken as the page, the third the row coordinate and the fourth the column coordinate (11111 must be added to this group in our figures). This five-figure group is now subtracted from the first indicator. Then the date tetragram with the addition of a zero is subtracted from the result. This final five-figure group denotes the starting point, the first two figures giving the page, the next two giving the coordinates, and the last giving the digit of the five-figure group at which encyphering begins (e.g. a message on the 12th, front indicator 68053 and first cypher group 99256; the control is 9925 + 1212 = 0137; page 01, coordinates 3.7 gives, say, the group 90981; this subtracted from 68053 gives 78172; subtracting 12120 from 78172 gives the starting-point 66052, i.e. page 66, coordinates 0.5 beginning at the second figure of the group).

The rear indicator, also denoting the starting point, is decyphered on the same system, save that the first four figures of the second text group are used as the control.

JBC was introduced on July 1st 1943. On February 1st l944 the recyphering pad changed, but the second pad was quickly broken into and the first pages were recovered by this section in March. The complete pad was soon recovered, and all messages in this cypher have since been read on receipt.

Super JBC

This combination of BA and JBC was introduced on April 20th, 1945. Additives are obtained by transposing a page of the recyphering pad in a setting 25 by 25, using a BA key, and with 125 blanks inserted in 25 sets of 5 in accordance with the second system of BA blanks. Each page is used once only by each post and the pages are used in order. Separate BA keys and sections of the pad are allotted to posts abroad and to Tokyo. Full instructions were given in Tokyo Circular 383 of April 5th 1945, which was in BA put through a machine.

Only four messages in this system have been received to date, and consequently it is not yet known whether the BA keys progress similarly to the pages of the pad.

2. NE (JAM)

This recyphering table, introduced on July 1st 1943, has the same appearance as JBC, save that the indicators are systematic, are used in alphabetical order and are repeated at the end of the text.

A four-figure code is used, recyphered and sent in five-letter groups using the same letter-figure substitution as JBC, the middle letter of each group being a null. The code consists of 1,620 groups and has the following restrictions (N.B. These apply only to our recovered code; the actual Japanese figures are not known): The first three figures of a code group are all even or all odd. Even groups have no zero in the third place and no 2 in the fourth place; groups with a 2 in the third place begin only with 06, 20, 44, 46, 80 and 82; no groups begin with 08. Odd groups have corresponding restrictions: no 3 in the last place; groups with 1 in the third place are restricted to six pairs of starters which are not completely determined, although the pairs 17, 55, 57 and 93 are confirmed; no groups begin with 19. The main part of the code (elementary *kana*, numerals, punctuation and common words) is confined to the even groups, the odd groups corresponding roughly to the tetragrams of FUJI.

Two recyphering tables were employed, one for messages from Tokyo, one for messages to Tokyo. There is no figure indicator, the letter indicator giving the

starting-point, though no relation exists between the order of the indicators and corresponding starting-points. Encyphering always begins at the beginning of a group.

In July and August 1943, NE was used extensively, particularly by Tokyo, but thereafter was almost entirely replaced by JBC, traffic in NE averaging only about one message per month. Consequently NE was left over in favour of the more commonly used cyphers until October 1944. When these had been exhausted, several pages of the NE pad together with code recoveries were soon forwarded to London. London in turn passed these findings to Washington only to learn that the Americans had already been working on NE for some months without informing the rest of the world. Their recoveries, when made available, proved to be based on a different code and were very unreliable, and therefore they were of little assistance to this section. London accepted our recoveries and basic code and resumed work on NE shortly afterwards. The combined efforts of London and Melbourne have only resulted in the breaking of certain sections of the two pads and the establishing of the commoner code-groups, as very little workable depth was available.

The Japanese regarded NE as their highest-grade recyphering table and, after the initial abuse of this confidential cypher by Tokyo, instructions were issued that its use was to be confined to highly secret reports.

3. SOSOS (JBN)

This recyphering table was introduced on October 1st 1944 for use between Moscow, Vladivostok, Petropavlovsk and Tokyo. Very little traffic in this cypher was received.

In appearance it is similar to JBC and is a four-figure code recyphered and sent in five-letter groups, with the group SOSOS at the head of the text. There is no dummy indicator, but two figure indicators appear at the beginning and end of the cypher-text.

The second and third digits of the code-groups are of the same parity, and the first two digits are restricted to the ranges 4 through 9 and 0 through 5 respectively. It is presumed that there is a one-figure restriction in the last place, reducing the book to the normal 1620 groups.

The pad is made up of five-figure groups and encyphering can commence only at the beginning of a group. No additives have been recovered owing to insufficient depth and work on the cypher was abandoned upon Russia's entry into the war against Japan.

4. 10101 (JBD)

This is the interdepartmental recyphering table, introduced on July 1st 1943. It is a four-figure code recyphered and sent in five-figure groups prefixed by the group 10101. The message-number and number of parts are sent in clear.

The code contains 1,620 groups with the following restrictions: the first digit is even, but not zero; the third digit is odd and the last figure not zero; no groups begin with 86, 87, 88 or 89 (N.B. This is the actual Japanese code).

The recyphering pad contains 100 pages numbered 00 through 99, each page containing 100 five-figure groups arranged and coordinated similarly to JBC. Encyphering always commences at the beginning of a five-figure group.

There are two figure indicators, one at the beginning and one at the end of the text, the front indicator denoting the starting point and the rear indicator the end-point. The control for the first indicator consists of the 4th through 7th figures of the cypher-text, the first two giving the page in the pad and the last two the coordinates of a group on this page. The group thus found is subtracted from the front indicator to give the starting-point as page, page, check, row coordinate, column coordinate. The control for the rear indicator is the 4th through 7th figures reading from the end of the text and it is decyphered similarly.

The basis of the cypher was discovered by Washington's machining, and this section began work on JBD in April 1944; in May we recovered and telegraphed to London the first consecutive stretch of additives together with basic code groups. London immediately joined forces with us and practically the entire pad and code book were broken.

A second pad was brought into force on October 21st 1944, but poor local interception delayed the recovery of the new pad until April 1945. With the discontinuation of BA (which was also used to a moderate extent as an interdepartmental cypher), JBD traffic increased enormously after April and the pad was almost entirely recovered by August in cooperation with London. The entire traffic in this cypher was read until the cessation of hostilities.

5. JAO

This is a recyphering table for use within the Greater East Asia Ministry, introduced on July 1st 1943. It has a four-figure code book, the text being sent in five-figure groups with the middle figure checking the first two. The

indicator, which is repeated at the beginning, is a five-figure group, the first two figures being the originator's number and the last three the serial number in this cypher.

JAO has not been broken, but the following facts have been established:

(a) Encyphering is done in sets of 58 groups, so that the 59th group has the same recypherer as the first, and so on.

(b) The last code group of a message must be either 6300 (*tsuzuki*) or 0940 (*owari*). The actual number of the message is encyphered at the head of the text and is encoded in the following way: the number is divided into pairs from the beginning, each pair being made into a self-checking, four-figure group by the addition of its complement (e.g. 24 becomes 2486). If a single digit remains it is repeated to form a four-figure group (e.g. 247 becomes 2486 7777). The part of the message is treated in the same way.

(c) An unrecyphered message from Nanking has shown that the code is not built up on any apparent pattern.

London has informed us that their machining of this traffic has proved that it is not homogeneous. This cypher is not extensively used and the length of a message rarely exceeds 58 groups.

6. 50505 (JBE)

This is apparently a recyphering table, with the text sent in five-figure groups, the middle figure checking the first two figures of each group. The group 50505 stands at the head of the text, followed by two non-checking groups which are presumably indicators or encyphered message-numbers.

50505 has not been broken. A suggestion was made by Washington that it was encyphered in sets of 97 groups (this being the 'normal' length of a message) but no confirmation has been found. Machining by London and Washington has produced no results.

Part IV: Breaking the Recyphering Tables

1. Letter-Figure Substitution

2. Placing of Messages in Depth

3. Breaking of Additives

4. Indicator Systems

1. Letter-Figure Substitution

NE and JBC, which both used the substitution, were introduced on the same day and were examined in conjunction. The original machining done by London revealed that NE was a recyphering table, and it was observed that the letters of the substitution divided into two Classes, CFORY and GKLNS, such that the 1st, 2nd and 4th columns of the five-figure group depth were each made up mainly of letters of the same Class — e.g. a specimen depth would be:

CYKGN
ORRGL
FRGNY
FOYSO
GNOCG
FONLY

Columns 1 and 2 being Class I, and Column 4 Class II. The natural division of numbers into two Classes being evens and odds, it was deduced that the code consisted of five-figure groups in which the 1st, 2nd and 4th figures were either all even or all odd. Very soon after the introduction of NE, Tokyo sent out a three-part circular which proved conclusively that the middle figure of each group was a null: in one part of the message S was used practically throughout while in another part the middle place was filled with all the letters of the alphabet.

The actual recovery of the letter-figure substitution proved a tedious job. London decided to work on NE only (in view of the initially large volume of traffic), and it was several weeks before the problem was solved, whereas it was later seen that it could have been written down by inspection of a few JBC columns (in view of the 9 and 0 restrictions in the second digit).

The first method adopted was that of examining the frequencies of the basic differences with every possible system of substitution. As the only restriction known was that of the even and odd sets, the possibilities apparently ran into millions, but careful analysis showed that the relevant permutations of each

set were only six in number. Assuming, for example, that CFORY represented 02468, then any cyclic permutation of this order gives the same frequency distribution of basic differences; furthermore, the common difference of the arithmetical progression CFORY can be altered to 4, 6 or 8 without altering the frequencies, so that CFORY, COYFR, CRFYO and CYROF are all equivalent. Thus the 120 possible permutations of CFORY are divided by 5 and then by 4, to give only 6 basic permutations.

This method would certainly have given the order of the two sets, but the depth available for differencing was unfortunately not great and was further reduced, as only columns whose first three digits were all of the same class could be examined. The six frequency sets proved to be distressingly similar, and no conclusion could be made with any confidence.

At this stage a further restriction in the code was discovered by London, who noticed that one of the five figures was always missing from the third column, while another figure was rather rare. In this way a relation was quickly established between the five letters of each set, as the missing figure (zero) and the rare figure (2) obviously bore a constant relation to one another. The orders OFCRY and LSGNK were proved correct, and further examination of the relation between the two sets in the third column of the depth indicated the complete order OLFSCGRNYK (The evidence for this was rather scanty, but was fortunately conclusive). As any cyclic permutation of this order could be used, the above order giving O as zero was decided upon, and was finally proved correct by the JBC indicator system.

2. Placing Of Messages In Depth

Although the general rule for setting messages in depth is to break the indicator system, or, if this is not possible, to run all messages through a machine, the structure of the various codes studied by this section made such arduous work unnecessary.

NE

Obviously, if a recyphering table is used to encypher groups whose first three figures are all of the same parity, then the 'pattern' of the even and odd figures of the table will be evident from an inspection of the encyphered messages (e.g. If a four-figure group of the table is E O E E, then any group encyphered with it must appear as E O E or O E O). The possible arrangements are only four in number, and so each group of a message was classified as 0, 1, 2, or 3 (0 when all three figures were of the same parity, 1 for the first two, 2 for the first and third, and 3 for the second and third digits). Thus a message was typified by a series of numbers, known as its 'pattern', or more correctly as the pattern of

the section of the additive book from which it was encyphered. The problem of tying in messages was thus reduced to that of finding repeats in their patterns, which was easily done by logging sheets. An example of this patterning follows:

Additives:	3891	2675	3940	8827	6394	2831
Code:	3731	3578	8849	4408	3774	1775
Cypher Text:	6522	5143	1789	2225	9068	3506
Pattern:	2	1	1	0	3	1

which is the pattern both of the cypher text and of the additives.

It was established that the NE recyphering table consisted only of four-figure groups, encyphering always commencing at the beginning of a group, so that this method was sufficient to place all messages in depth.

JBC

The JBC recyphering table consists of five-figure groups with encyphering beginning at any figure of the pad, so that the above patterning system was not completely effective as it accounted only for messages whose starting points were a multiple of four figures apart. For JBC, therefore, a method of 'partial patterning' was evolved as follows: Numbering the figures of the additive page 000–499, a message is said to be on 'Cut' I, II, III or IV according as its starting point is 4m, 4m + 1, 4m + 2, or 4m + 3. Now if two messages on Cut I and Cut II respectively are examined, it is easily seen that the parity of the second and third figures of the groups of the Cut I message corresponds to that of the first two figures of groups of the Cut II message.[7] Accordingly, all messages were typified by the parity of the first two figures of the groups ('A' Pattern) and also by the parity of the second and third figures ('B' Pattern). The patterning was simply done by underlining pairs of figures which were both even or both odd and writing down the distances between them, e.g. 2294 8362 9004 3746 2215 0762 3485 0926 4408 'A' Pattern for this stretch would be (.) 3.1.4. …

As Cut I was by far the most commonly used, the various Cuts of a page could quickly be established, and when the entire pad was known the NE patterning system was resumed (all four Cuts on any page having, of course, separate patterns).

7

Code Groups	3731	3578	8849	4408	3731	3578	8849	4408
Additives	3814	5211	6963	4084	8145	2116	9634	0846
∴ Cypher Text	6545	8789	4702	8482	1876	5684	7473	4244
OE	OE	OE	EE		OE	OE	OE	EE

10101

The initial machining of JBD by Washington revealed that, when messages were placed in depth, in every second column the figures in that column were of uniform parity.

E.g.	29386	14077	29348	62314
	48728	06953	85754	50436

This led to the assumption of a four-figure code book in which the first figures were of a uniform parity and the third figures were of a uniform parity. An elementary patterning system was devised: in alternate digits of the text the evens were marked and the distances between them noted down. This system was continued until it was discovered that the pattern of the odd digits of one message could be linked with that of the even digits of another thus showing that, of the first and third digits of a code group, one was even and one was odd and thus Cuts I and III and Cuts II and IV could be linked by patterns.

The obvious defect of the patterning system outlined above was that each message had to be patterned twice, once for its even digits and once for its odd digits. The following method was therefore devised: As the cypher-text was sent in five-figure groups, there were three relevant digits in the 1st, 3rd, 5th, etc text groups, and two in the 2nd, 4th, etc groups. The odd-numbered groups were classified as 0, 1, 2 or 3 in the same way as NE patterns. The even-numbered groups were classified as 4 or 5 according as the two relevant digits were of the same or opposite parity.

E.g.	1st	2nd	3rd	4th	5th	6th	7th
	20946	34857	00428	39156	35338	29044	28927
Pattern	2	5	0	4	1	5	3

Thus messages on the same Cut or on Cuts differing by two had identical patterns, the actual cut being easily determined by the starting point.

The essential difference between JBC and 10101 was that, while all Cuts of the former could eventually be found from patterns alone, it was impossible to link Cuts I and III with Cuts II and IV of 10101. This difficulty was serious in the early stages, but when a good knowledge of the code had been acquired, it was not difficult to break a few groups of additives on two Cuts alone, pattern these additives and thus find the other two Cuts of the page.

SOSOS

The structure of the SOSOS code book presented by far the greatest problem in patterning. The text was divided into four-figure groups, and each of these was

classified as O or E according to the parity of the second and third digits. These patterns were very difficult to distinguish, and of course it was impossible to relate any of the four Cuts. The total traffic received before the cypher was discontinued gave a maximum depth of only five, which was however sufficient to portray the restrictions on the first two figures of the code-groups.

A sample depth was:

0709	6914	9778	9278	6099
0851	4221	0512	8167	2120
2544	73l5	5680	8293	4010
2679	5110	7466	8210	3766
4834	6916	7313	4233	1941

from which it may be seen that the first two figures of each group can always be limited to a 6-digit range, the actual ranges being as yet indeterminate.

The ranges were tentatively determined from an inspection of fillers (see Appendix B) as 4–9 for the first place and 0–5 for the second. This assumption was finally proved correct when London found a message on a Cut adjacent to that of a known depth.

The actual finding of such Cuts was an arduous process and was never completely developed, as the ranges were only established a week or so before Russia's entry into the war. The only method was that of writing down the possible additives for the first figure of each group of a depth and then searching among the remaining messages for one such that the second digit of its group could always be placed in the range 0–5 by at least one of these possibilities.

3. Breaking of Additives

Apart from the usual method of differencing columns, many other devices were used which depended on stereotyped starts and ends, fillers, the restrictions on the codes, and, of course, the actual sense of the Japanese.[8] There is no need to discuss these in great detail, as experience alone can allow one to 'spot' columns and 'prapse' effectively.[9] The information on starts and ends may be found in Appendix B; it is a simple matter to exploit the restrictions of each code: e.g. a column in 10101 —

8 Differencing columns: Where a large depth of messages has been established, two common words, e.g. *wa* and *no* (whose code values in 10101 are 8559 and 8416 respectively) will often occur in the same column. Where recyphered with the same additives their difference (0143), of course, remains constant. The cryptographer has beside him his list of frequently occurring differences and, in the same columns of cypher-text, subtracts groups from each other in search of these.

9 To 'prapse' — a verb coined by Professor Trendall from the adverb 'perhaps'.

5675
7856
7499
3136
5811
5394
7311
5393
5255

has fairly certainly the additive 9 for the first figure, giving five 6s, three 8s and one 4; the additive for the second figure can only be a 3 to eliminate the combinations 86, 87, 88 and 89; two groups with a difference of 0001 and beginning with 60 are most likely to be 6096 (*wo*) and 6097 (stop), and a trial of the required additives 07 for the last two columns gives a result which is seen to be certainly correct: quote, *wa*, *so*, *ni*, *dai*, stop, unquote, *wo*, *ki*. The open and close quotes will require their complements; the stop will have a final verb or brackets before it, possibly a paragraph after it, and the '*so*' will probably either be in quotes or be followed by '*ren*' or '*gawa*' [meaning 'Soviets'], and so on. In this way the whole section may be extended without great difficulty, the restrictions showing quickly whether one's 'prapses' are possible or not.

4. Indicator Systems

These were not broken by this section, as the great labour involved requires either a machine or a very large staff.

Part V: Miscellaneous Cyphers

1. HINOKI Machine Cypher (JAA)
2. SAKURA Emergency Cypher (JBL)
3. Unidentified Cyphers

1. HINOKI Machine Cypher (JAA)

JAA is the highest-grade of Japanese diplomatic cypher. The indicator is a five-figure group at the head of the text and is made up of all the permutations of the groups 02468, 13579, 01234, 56789.

2. SAKURA Emergency Cypher (JBL)

This emergency cypher was introduced for use by posts which were forced to burn their cyphers, as the system can be easily memorised. It is a plain-language double-transposition without blanks, indicated by the group XXXXX at the head of the text, with a figure check at the end. The instructions were circulated in NE and JAA, both of which messages were read.

The key for the first transposition, in encyphering, is derived from the word *umiyukaba* by numbering the letters in alphabetical order from the left (Thus the key is 764985132).[10] The key for the second form is derived in the same manner from the word *umiyukaba* followed by the originator's name (e.g. *umiyukaba* Harada produces the key 13 11 9 15 14 10 1 6 2 8 3 12 4 7 5).

3. Unidentified Cyphers

Following is a list of unidentified Japanese diplomatic cyphers. With each the small amount of traffic intercepted did not justify any serious work being done on them.

Hanoi-Vichy Figure Traffic

This was sent in five-figure groups and was used only in the circuit Hanoi–Vichy–GEAM. Only five messages of this type were received.

9009

This cypher was mainly used between Canton and other China posts. It was indicated by the group 9009 at the beginning of the text and was sent in four-figure groups.

---

10 *Umiyukaba* is the first word of a passage from a famous patriotic poem of the Late Nara period (8th Century AD):

> We are the sons of the fathers who sang
> 'At sea be my corpse water-soaked
> On land let it be with grass o'ergrown,
> Let me die by the side of my Sovereign!
> Never will I look back'.

When this was set to music by Nobutoki Kiyoshi in 1937, at a time of national fervour following the outbreak of war with China, it achieved wide popularity. The Japan Broadcasting Corporation used it as the background music for the declaration of war against the United States and, later, for bulletins announcing naval or military reverses.

5005

This cypher was current in the GEAM area and was sent in four-figure groups. The indicator 5005 led to the suggestion that it might be a form of 50505 (JBE) in which the middle figure check was omitted.

Petropavlovsk Code

This was a simple code, which came into use simultaneously with SOSOS (JBN) and was used by the same posts. Only ten messages of this type were received.

Part VI: General Remarks

1. Code-Building
2. Cypher Systems
3. Errors in Encyphering
4. Distribution of Cyphers
5. Cooperation with Linguists

1. Code-Building

A great deal of evidence has been found that the Japanese regarded their cypher systems as completely unbreakable. However, it is not advisable when constructing codes to have patterns or restrictions; and alternatives for common groups are most necessary. Yet no alternative groups were ever found in the figure codes, while the letter codes had only two equivalents for a few common groups: the alternatives in FUJI were *wo*, *ni*, *no*, and *ga*; in BA *wa*, *wo*, *ni*, *no*, *ga*, and *mo*.

As the standard Japanese diplomatic vocabulary is 1,620 groups, their figure codes had to be tetragrams restricted in some manner. The obvious method is to choose 1,620 groups at random, but a patterned code not only reduces chances of corruption but also saves a great deal of time by allowing the decode to be set up on charts and facilitating memorisation of the code groups. A study of Part IV: Breaking the Recyphering Tables will show what invaluable assistance the patterned codes were to us.

2. Cypher Systems

The recyphering tables introduced in July 1943 were the first the Japanese had ever used for diplomatic communications. Hitherto transposition systems had

been solely used, but curiously enough the Japanese regarded their recyphering tables as of such high grade that they were chary of using even the second system of BA for important messages, although this latter system proved to be the most difficult for us to read. Perhaps the swing from transposition to recyphering tables was most fortunate from our point of view, as it is impossible to say how complicated the transposition systems might have become.

3. Errors in Encyphering

[1 paragraph (approx. 7 lines) expunged][11]

(a) Both BA and GEAM were introduced in a reasonably simplified form, the complexity being afterwards increased by a series of changes in the cypher system while keeping the code consistent. [Concluding portion of the paragraph (approx 7 lines) expunged].

(b) [1 paragraph (approx 9 lines) expunged]

(c) [1 paragraph (approx 22 lines) expunged]

4. Distribution of Cyphers

A state of war invariably produces great difficulties in distribution, the usual result being that cyphers must be kept in force much longer than is safe. The Japanese, faced with this position, attempted to compromise by introducing changes in the existing cyphers (e.g. in FUJI — see Part II above). But however ingenious a new system may be, a knowledge of the previous system and code is usually sufficient to break it.

Another result of the war was that when the European countries were being overrun, the problem of cypher security became acute and the Japanese posts were forced to burn their cyphers and use emergency systems which could be memorized. The instructions for these systems had, of course, to be circulated in existing cyphers; they might have proved difficult to break, but it was fortunately not necessary to attack them directly.

5. Cooperation with Linguists

Although military and naval recyphering tables, with their great bulk of traffic, can be broken by purely cryptographical methods [1 paragraph (length unknown) expunged].

---

11 The expungements in this part were made by the NAA on 17 February 1998, pursuant to *Australian Archives Act* §33(1)(a) and (c) — 'information of a class concerning operational methods/techniques that remain current'.

PART VII: PERSONNEL 1942-45

Technical

Professor A. D. Trendall (University of Sydney) (January 1942 – June 1944)

NX139540 Lieutenant R. S. Bond (February 1942 –)

Dr Elizabeth Sheppard (September 1942 – March 1943)

N450470 Lieutenant E. S. Barnes (January 1943 –)

NX139427 Sergeant K. L. McKay (July 1944 –)

NX82807 Sergeant A. C. Eastway (February 1944 –)

VX94295 Corporal I. H. Smith (May 1944 –)

V143841 Sergeant P. Grange (Clerical Duties) (October 1943 –).

The following personnel were lent to Special Intelligence through the kind offices of Lieutenant-Colonel A. W. Sandford, Commanding Officer, Central Bureau, during heavy periods:

Sergeant A. W. F. Rogers, Sergeant H. W. MacKenzie (January 1945 –), Warrant Officer II P. Pledger (October 1944), Sergeant J. C. Davies (June 1942 – February 1943), Private K. McLeod (February – May 1944).

Language and Translation

Mr C. H. Archer (British Consular Service) (January 1942 – December 1944)

Mr H. A. Graves (British Consular Service) (February 1942 – September 1943)

Mr A. R. V. Cooper (British Government Codes & Cyphers School) (March – December 1942)

Mr J. O. Lloyd (British Consular Service) (December 1942 – March 1943)

Mr D. MacDermot (British Consular Service) (December 1942 – March 1943)

Mr H. R. Sawbridge (July 1943 – February 1944)

Mr R. L. Cowley (British Consular Service) (December 1944 –)

Mr E. T. Biggs (British Consular Service) (July 1944 –)

Miss Mavis Tilley (November 1942 –)

Mr L. R. Oates (February – November 1943)

Lieutenant C. A. James (British Army) (May 1944 –)

Lent by Central Bureau for short periods of heavy pressure — Warrant Officer II B. Pitman (British Army) (June 1945 –), VX128886 Private D. C. S. Sissons (April 1945 –).

Clerical and Typing

A staff of typists and women clerks was headed by Miss Reba Shearer (January 1942 –).

Clerical

Miss Mary MacRae Stewart (November 1942 – September 1943)

Mrs Marjorie Hattam (1943 –)

Mrs Catherine Gahan (September 1943 –)

Typing

Miss Pauline Dennis (1943 – June 1945)

Corporal Vailima Parbery (AWAS) (May 1944 –)

Corporal Thora Martin (AWA) (June1945 –)

[Report of Special Intelligence Section ends.]

Sources

It was, I think, in 1978, that my colleagues at the Australian National University, Desmond Ball and David Horner, came upon evidence in recently declassified files that a diplomatic Special Intelligence Section headed by Professor A. D. Trendall had operated in Melbourne from about January 1942 until the war's end, its function being to intercept the encyphered signals traffic between the Japanese Ministry of Foreign Affairs and its embassies and consulates overseas and to decrypt so much as was possible. They suggested that I make an attempt to put together a history of that Special Intelligence Section.

At the time it proved impracticable. Persistent enquiries at the NAA elicited the suggestion that the records of the Section had either been destroyed in toto in the 1950s or were held by the Department of Defence which was unlikely to declassify them in the foreseeable future.

I attempted to prepare the ground by writing to former members of the Section for their recollections: Eric Barnes, Ronald Bond, Kenneth McKay and Ian Smith among the cryptanalysts, and Mary Stewart from the office staff. They were patient and indulgent and provided a treasure trove of background information.

Ronald Bond and Ian Smith remembered that before the Section was disbanded they spent much time compiling a detailed and comprehensive report on the

Section's activities. This prompted me in about 1986 to apply to the NAA for access to that document. This elicited a reply from the Defence Signals Directorate (DSD) that the Report had survived as had an Army Central Registry file, '37/401/425: Special Intelligence Section' (NAA Series A6923, Item 37/401/425) that, when declassified, might be of considerable help to the historian. These documents were eventually declassified in about 1997. At the same time, in 1986, DSD presented me with a Xerox copy of a file held by the US National Archives & Records Service containing translations of diplomatic intercepts cabled by Trendall's Melbourne Section to the US Navy's cryptographic department in Washington throughout 1942.

At the time of the 1997 declassifications, DSD also declassified what appeared to be two wartime office files of the Major I(x) in the Directorate of Military Intelligence who administered the Section (NAA Series A6923, Items: 'Diplomatic Message Traffic' and 'SI/2 Attachment') which cast some light on the Section's daily activities over certain periods.

It would appear, therefore, that the office records of the Section, which were complete and in good order at the time the Section was disbanded, have been destroyed in toto — including the leather-bound register, referred to by the office staff as The Koran, in which the particulars of every intercepted message was recorded!

Surely the time has come for Defence to declassify their files on the 'TRENCODE', used by Allied operatives working behind enemy lines, and its development. (Incidentally I remember that it was still in use in the British Commonwealth Occupation Force in 1947) There can no longer be 'security' objections. After all, it was never considered to be unbreakable — merely that it could resist decryption for a period of two or three days.

My impression is that the Section was essentially one of the overseas out-stations of the United Kingdom's cryptographic organisation, the Government Code and Cypher School (GC&CS). Following the recent declassification of GC&CS wartime files, their detailed listing by the Public Record Office indicates that GC&CS had a much less cavalier attitude to their records than our Defence Signals Directorate has demonstrated to its own. There should be a good deal of information about the operations of Trendall's Section in the GC&CS files available at the Public Record Office at Kew.

My editing of the Report is confined to:

(i) Re-arranging the sequence of some of the chapters;

(ii) The insertion of section headings;

(iii) In the interests of clarity identifying each of the codes by the title used by the Section at the time, e.g. GEAM, 10101, BA, JBC, Umiyukaba;

(iv) The addition to the list, Personnel 1942–1945, of a few names that the authors had apparently forgotten;

(v) The rewriting and expansion of a few sentences where Ian Smith agreed that, as written, the meaning was not sufficiently clear; and

(vi) My attempt to reconstruct, using American sources, Appendix L (which is one of the several Appendices missing in the file).

Appendix A: Best Groups

Following is a classification of the best groups in the Japanese diplomatic vocabulary (This list must be used with discretion, as certain 'position' groups such as *gokuhi*, jōhō etc which are often very good at the beginning of a message are on the other hand very rare in the body of a message).

Class I: *no*, *ni*, *wa*, *wo*, *shi*, *mo*, *to*.

Class II: *chi*, *dai*, *ga*, *i*, *ji*, *ka*, *kai*, *kan*, *ki*, *kō*, *ku*, *ri*, *sen*, *su*, *tai*, *tō*, *tsu*.

Class III: *bei*, *bu*, *bun*, *chō*, *chū*, *dō*, *doku*, *e*, *fu*, *gawa*, *gō*, *gun*, *hi*, *jō*, *ken*, *koku*, *kyō*, *mono*, *nari*, *naru*, *ru*, *ryō*, *sei*, *shin*, *shō*, *so*, *sō*, *suru*, *ta*, *taru*, *teki*, *tokoro*, *yō*.

Class IV: *ari*, *arita*(*shi*), *aru*, *bō*, *gen*, *go*, *jin*, *kaku*, *kin*, *koto*, *mi*, *migi*, *mu*, *ni oite*, *re*, *sho*, *shū*, *te*, *yori*.

To this must be added punctuation and low numerals, which are usually 'position' groups.

Appendix B: Starts and Ends

Starts

Following are the most common starts of Japanese diplomatic messages:

Ōden or *Kiden* [numerals] *ni kanshi*. 1,

Gokuhi or (*gai*) *kimitsu*.

Kanchōfugō.

For multi-part messages — [Numeral no numeral] or [numeral].

[Place) *hatsu* [place] *ate dempō dai* [numerals] *gō* (*ni kanshi*).

Date.

Paragraph.

Other traditional starts were sometimes used by certain posts. e.g. Stockholm sent many spy reports which almost invariably began with some variation of '*chōhōsha hōkoku* [date] *sa no tōri*'.

Tokyo circulars very often began with '*kokusai jōhō*'.

Ends

Apart from final verbs (of which '*nari*' was by far the most common), circulars could usually be relied upon to finish with a formula listing addresses, like one of the following:

[Place, place, etc] *ni tenden seri*.

[Place] *yori* [places] *ni tenden aritashi/o kō*.

Honden atesaki [places] *ni tenden seri*.

Honden zaiō kaku taishikan (*so wo nozoku*) *ni tenden seri*.

The number of parts of a multi-part message was also found at the end occasionally, also '*tsuzuki*'.

Fillers, if a whole four-figure group, were often stop, comma, or close brackets. The usual fillers, however, were of the type 0000, 0123, 1234, etc, (the sequence often carrying on from the last figure of the final code-group).

Very short messages were often requests for repetitions and, if so, could usually be written straight in on the following formula: *Kiden* [numerals] *kaiyaku funō ni tsuki chōsa no ue saiden aritashi/o kō*.

Appendix C: R7F Lower Power Far Eastern Diplomatic Network

Traffic on this low-power Far Eastern diplomatic network was first intercepted in Melbourne towards the end of August 1944. By far the greater part of GEAM and interdepartmental messages were sent through this channel and in the year preceding the cessation of hostilities only a very small portion of the total Far Eastern traffic passed over commercial links.

The transmission procedure was somewhat different from that used by commercial stations.

(1) Addresses were in code instead of in clear (v. Appendix E [Missing]).

(2) Signatures of originators were not sent.

(3) The text was not sent in normal fashion from left to right. Each page of the transmission form contained 50 groups in five columns, and the text was transmitted by reading down the columns, the end of each column being denoted by the *kana* break AL.

(4) In figure messages the following short figure substitution was used:

T	A	U	V	4	5	6	B	D	N
0	1	2	3	4	5	6	7	8	9

Appendix L: Code and Keys for GEAM (JBB)

[Ed. The original Appendix is missing in the xerox copy of the Report held by the National Archives of Australia (NAA). What follows I have reconstructed from information derived from the US Army Signal Security Agency's file, 'US/UK Technical Exchanges and Information on Solution of JBB' (US National Archives, Record Group 457, Box 1328, File 190/37/34/3 (19 pages).]

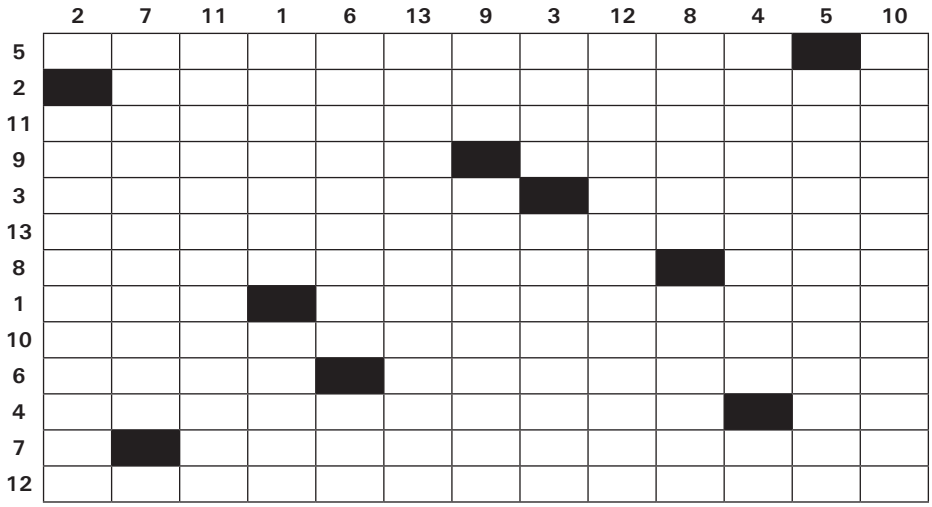
The following description is of GEAM in its final form, in use from October 1st 1944.

The Indicator and Keys

The indicator is the group of alternating letters (e.g. BKBKB) following the date and number group. These letters (A through N excluding M) indicate the horizontal row order and vertical column order respectively in the 13 x 13 transposition block, namely:

A	5	2	11	9	3	13	8	1	10	6	4	7	12
B	2	7	11	1	6	13	9	3	12	8	4	5	10
C	11	6	4	3	2	13	1	9	7	8	12	5	10
D	10	9	5	11	7	3	6	13	4	1	8	2	12
E	1	13	3	6	11	7	10	4	12	5	2	8	9
F	11	2	6	4	5	10	12	3	7	1	8	13	9
G	13	4	10	5	3	11	7	1	2	9	6	12	8
H	11	10	5	3	4	9	7	1	13	8	2	6	12
I	9	7	2	8	12	6	13	5	3	11	10	1	4
J	4	9	13	1	8	5	2	6	12	3	10	7	11
K	13	10	2	9	6	4	11	8	1	3	12	7	5
L	11	6	8	3	7	5	12	10	2	9	4	1	13
N	5	10	13	7	2	11	8	1	3	12	4	6	9

These keys also determine the positions of the nine blanks, which are inserted in the cells with the coordinates (1,1) through (9,9). Thus, for example, the transposition block indicated by the indicator group ABABA would be as follows:



Encoding and Transposition by the Sender

In this example the originator sends the following message in GEAM using the indicator ABABA.

Janku yusō ni kanshi

Dai 20 *ji*

Kinmangen (*kane. yorozu. minamoto*) 78 ton

Fujōhatsu (*futsū no fu. senshū no shū. hatsushin no hatsu*) 33 ton

Dai 21 *ji*

Chinryūjun (*chinkōin no chin. ryūtai no tai. suna …*

He encodes this into the appropriate digrams/tetragrams of the GEAM code and it reads:

20	40	60
JJXYERCURUDYVVDYUFAS	VUSAMIUFICAJELNICAGE	UKROKOMUUKJIGAJOFONU
80	100	120
UTEVOFUFHUYHIYNIHUIR	GOHUUKEDYFGOYFUKIYID	GOIYNUWEWEOFUFASVVTI
140	160	
MIUFIFYLTOERNIIFCYIB	GOIFUKYLWYGOWYUKDUGA . . .	

He divides this from the left into packets of 160 characters (i.e. 13 x 13 – 9) each of which he successively enters into the transposition block, row by row, from the left, in the numerical sequence indicated by the row key, as follows:

	2	7	11	1	6	13	9	3	12	8	4	5	10
5	U	K	J	I	G	A	J	O	F	O	N		U
2		V	V	D	Y	U	F	A	S	V	U	S	A
11	I	U	F	I	F	Y	L	T	O	E	R	N	I
9	I	Y	I	D	G	O		I	Y	N	U	W	E
3	M	I	U	F	I	C	A		J	E	L	N	I
13	L	W	Y	G	O	W	Y	U	K	D	U	G	A
8	U	K	E	D	Y	F	G	O	Y		F	U	K
1	J	J	X		Y	E	R	C	U	R	U	D	Y
10	W	E	O	F	U	F	A	S	V	V	T	I	M
6	U	T	E	V		O	F	U	F	H	U	Y	H
4	C	A	G	E	U	K	R	O	K	O		M	U
7	I		Y	N	I	H	U	I	R	G	O	H	U
12	I	F	C	Y	I	B	G	O	I	F	U	K	Y

Usually the final block of the message will contain less than the full 160 characters. In such cases he will reduce the number of rows accordingly, from the bottom. If the bottom remaining row is not full he will insert from the left edge the necessary number of blanks to fill it.

On completing the transposition he writes out for transmission the cypher text by reading off each block, column by column, from top to bottom, in the numerical sequence indicated by the column key. In the present example this would be:

IDIDF GDFVE NYUII MLUJW UCIIO ATIUO CSUOI ONURU etc.

Decryption

The recipient goes through the same procedures in reverse — he makes out the same transposition block as indicated by the indicator group, enters the cypher text column by column, reads off the encoded message row by row, and decodes it by reference to the GEAM decoding charts, which are here reproduced.

Decoding Charts

Consonant-Vowel Digrams

	A	E	I	O	U	Y	
B	A	E	I	O	U	Ō	B
C	KA	KE	KI	KO	KU	KŌ	C
D	SA	SE	SHI	SO	SU	SŌ	D
F	TA	TE	CHI	TO	TSU	TŌ	F
G	NA	NE	NI	NO	NU	NŌ	G
H	HA	HE	HI	HO	FU	HŌ	H
J	MA	ME	MI	MO	MU	MŌ	J
K	RA	RE	RI	RO	RU	RŌ	K
L	GA	GE	GI	GO	GU	GŌ	L
M	ZA	ZE	JI	ZO	ZU	ZŌ	M
N	DA	DE	(	DO	)	DŌ	N
P	BA	BE	BI	BO	BU	BŌ	P
Q	PA	PE	PI	PO	PU	PŌ	Q
R	YA	YŪ	YI	YO	YU	YŌ	R
S	Ø	SATSU	KATSU	SHO	KETSU	SETSU	S
T	AI	ZAI	1	JU	KOKU	ZEI	T
V	100	ZATSU	GAI	JO	2	ZETSU	V
W	ATSU	3	NICHI	SUI	KONO	TAI	W
X	EI	SHA	GAKU	4	GETSU	TAKU	X
Y	KAI	OYO(BI)	KYO	SEI	SAI	←	Y
Z	KAKU	SHU	KEI	RYŌZI	SAKU	TATSU	Z
	A	E	I	O	U	Y	

Vowel-Consonant Digrams

	A	E	I	O	U	Y	
B	AN	EN	IN	ON	UN	KYŪ	B
C	KAN	KEN	KIN	KON	KUN	KYŌ	C
D	SAN	SEN	SHIN	SON	SUN	SHŪ	D
F	TAN	TEN	CHIN	TON	⊞	SHŌ	F
G	NAN	NEN	NIN	→		JŪ	G
H	HAN	HEN	HIN	HON	FUN	JŌ	H
J	MAN	MEN	MIN	MON	→	CHŪ	J
K	RAN	REN	RIN	RON	⊙	CHŌ	K
L	GAN	GEN	GIN	GON	GUN	AYŪ	L
M	ZAN	ZEN	JIN	ZON	REP. VOWEL	RYŌ	M
N	DAN	DEN	⌊	DON	⌋	GYŌ	N
P	BAN	BEN	⊙	HYŌ	DUN	GYŪ	P
Q	PAN	HŌKI	TAISHI	MYŌ	TOKKI	NYŪ	Q
R	5	N	TSŪ	SHUKU	WA	KYOKU	R
S	DAI	MEI	6	RYO	FUTU	SHAKU	S
T	CHO	AAI	NAI	NEI	7	SHOKU	T
V	SONO	8	HAI	RETSU	HEI	CHAKU	V
W	TZI	RAKU	MAI	9	BEI	CHOKU	W
X	TETSU	RIKU	HAKU	YAKU	NAO	KYAKU	X
Y	TOKU	MURE	HATSU	YORI	HOKU	←	Y
Z	JOKU	RITSU	FUKU	SEIFU	MATSU	KYOKU	Z
	A	E	I	O	U	Y	

a/

Auxiliary Chart for English Spelling

The use of this chart is indicted by the digrams OG or UJ ('Open Spell') and its discontinuance by the digram YY ('Close Spell)

Consonant-Vowel Digrams

	A	E	I	O	U	Y	
B	BE	BI	BO	BU	BY	BA	B
C	CE	CI	CO	CU	CY	CA	C
D	DE	DI	DO	DU	DY	DA	D
F	FE	FI	FO	FU	FY	FA	F
G	GE	GI	GO	GU	GY	GA	G
H	HE	HI	HO	HU	HY	HA	H
J	SPACE	⊙	⊙	'	⊙	CAP	J
K	B	C	D	E	F	♣	K
L	LE	LI	LO	LU	LY	LA	L
M	ME	MI	MO	MU	MY	MA	M
N	NE	NI	NO	NU	NY	NA	N
P	PE	PI	PO	PU	PY	PA	P
R	RE	RI	RO	RU	RY	RA	R
S	SE	SI	SO	SU	SY	SA	S
T	TE	TI	TO	TU	TY	TA	T
V	VE	VI	VO	VU	VY	VA	V
W	WE	WI	WO	WU	WY	WA	W
X	J	K	L	M	N	I	X
Y	T	U	V	W	X	←	Y
Z	CON	CH	GH	PH	SH	COM	Z
	A	E	I	O	U	Y	

Vowel -Consonant Digrams

	Y	U	O	I	E	A	
B	∅	AB	UB	OB	IB	EB	B
C	1	AC	UC	OC	IC	EC	C
D	2	AD	UD	OD	ID	ED	D
F	3	AF	UF	OF	IF	EF	F
G	4	AG	UG	OG	IG	EG	G
H	5	AH	UH	OH	IH	EH	H
J	6	:	)	(	?	"	J
K	7	G	,,	‘‘	/	H	K
L	8	AL	UL	OL	IL	EL	L
M		AM	UM	OM	IM	EM	M
N		AN	UN	ON	IN	EN	N
P	9	AP	UP	OP	IP	EP	P
R		AR	UR	OR	IR	ER	R
S		AS	US	OS	IS	ES	S
T		AT	UT	OT	IT	ET	T
V		AV	UV	OV	IV	EV	V
W		AW	UW	OW	IW	EW	W
X		O	S	R	Q	P	X
Y		Y	SION	MENT	EX	Z	Y
Z		TH	TION	ST	PR	WH	Z
	Y	U	O	I	E	A	

SEQUENCES

A	5-2-11-9-3-13-8-1-10-6-4-7-12
B	2-7-11-1-6-13-9-3-12-8-4-5-10
C	11-6-4-3-2-13-1-9-7-8-12-5-10
D	10-9-5-11-7-3-6-13-4-1-8-2-12
E	1-13-3-6-11-7-10-4-12-5-2-8-9
F	11-2-6-4-5-10-12-3-7-1-8-13-9
G	13-4-10-5-3-11-7-1-2-9-6-12-8
H	11-10-5-3-4-9-7-1-13-8-2-6-12
I	9-7-2-8-12-6-13-5-3-11-10-1-4
J	4-9-13-1-8-5-2-6-12-3-10-7-11
K	13-10-2-9-6-4-11-8-1-3-12-7-5
L	11-6-8-3-7-5-12-10-2-9-4-1-13
N	5-10-13-7-2-11-8-1-3-12-4-6-9

Appendix Q: Unused Emergency Cyphers

Super – LA

Instructions for use of this refinement of JAH (LA code) were sent out in JAA in June 1942, but no traffic of this type was ever intercepted.

Method of encyphering

The message is first encoded in JAH. A figure bigram is substituted for each letter of the coded text according to a substitution table formed in the following manner: All the letters of the alphabet excluding Q are written in order into a square 5 by 5 beginning at the top left-hand corner. The columns are numbered from 0 to 4 beginning at the left and the rows from 0 to 4 downwards. The figure bigram to be substituted for a given letter is formed by combining the row co-ordinate with the column co-ordinate of the letter. Thus, if A is in the top left-hand corner of the square A = 00, and X = 42.

The figure text is then written out in blocks of 40 figures consisting of two rows of twenty. A block of less than forty figures is likewise divided into two.

Starting from the left of the block each upper figure is combined with the figure beneath to form a figure bigram which is converted to a letter according to the substitution table. This is the final cypher text.

The substitution square is altered for each message and is indicated as follows. The co-ordinates of A are encyphered according to the number code appendix to JAH (v. Appendix F). The resulting bigram is written before and after the letter Q. Thus if A = 00, then the substitution square indicator is BAQBA.

A five-figure group giving the data and serial number of the message is placed at the head of the text. 01001 would signify message No. 1 on the 1st of the month.

In March and April, 1944, when Rumania and Bulgaria were threatened by the Russian advance and the legations in these countries were forced with the necessity of burning their cyphers, each minister formulated an extremely primitive and cumbrous emergency cypher. Neither cypher was ever employed and in May 1944 instructions for the use of SAKURA (JBL), a much simpler and securer emergency system, were circulated from Tokyo.

Bucharest 'Consonant-Vowel' Substitution

Details of this system were sent to Tokyo in March 1944. It is based on the *kana* syllabary, the redundant '*wi*' and '*ye*' being omitted. Each syllable is written in reverse order against the remaining 45 syllables to form a substitution table. Thus '–N' is substituted for 'I' and 'SU' for 'RO'.

Each syllable, however, is always to be represented by a bigram of the form 'consonant-vowel'. If single vowels have to be substituted, they are preceded by one of the fillers V, X, or Z. Instead of '–N' 'Q: plus any vowel' is employed.

The consonants B, C, D, F, G, J, L, P, are used with any vowel to indicate the following:

B = preceding syllable is nigoried.
C = preceding syllable is half-nigoried.
D = long vowel
F = several syllables follow in quotes
G = stop
L = comma
P = close brackets

The text was to be sent in five-figure groups. The specimen text sent by the minister at Bucharest himself best illustrates the weaknesses of the system.

'*DAI NIPPON BANZAI*' was encyphered as follows:

Cypher text:	HU	BE	QU	MO	YA	HI	CE	XI	SE	BO	ZI	RU	BA	QE
Clear:	TA	nig	I	NI	TU	HO	semi-nig	N	HA	nig	N	SA	nig	I

In April 1944 Tokyo replied, adding a further process to the original system. The bigrams obtained by the first substitution are further substituted according to the following substitution table.

The letters from A to M are written above the letters from N to Z so that A is above N and M above Z. Substitution is effected in the following manner:

(a) Where both letters of the bigram are in the same row, the corresponding letters of the other row are substituted. Thus AB becomes NO; UV becomes HI.

(b) When the letters of the bigram come one in each row, the corresponding letter of the opposite row are taken in each case, but the order is reversed.

(c) Where the letters of the bigram are in the same vertical line, the letters immediately to the right of each are substituted. Thus AN becomes BO; MZ becomes NA.

(d) Double letters are treated as in (a) above. Thus LL becomes YY; XX becomes KK.

All tetegrams used in this method were to bear the prefix "BASBA".

Sofia Emergency System

Details of this emergency cypher were intercepted in a message from Sofia to Tokyo in April 1944, but were somewhat obscure due to the actual phrasing of the message and signal corruption.

The basis of the system is as follows: The message is first encoded in JAH and the coded text is written out in two rows. The first group of the first half of the final cypher text is formed by taking the first letter of the upper row, the first of the lower row, the second of the upper row, the second of the lower row, and the third of the upper row. The first group of the second half of the final cypher text consists of the third letter of the lower row, and the fourth and fifth letters of the upper and lower rows taken in order. Succeeding groups are taken off on the some alternating principle.

In the case of fillers the method employed is unknown and the specimen text given at the end of the instructions was so corrupt that no inferences could be drawn from it.