The Imperial Japanese Navy IKA Cipher Machine

Chris Christensen
Department of Mathematics and Statistics
Northern Kentucky University
Highland Heights, KY 41099, USA
christensen@nku.edu

Abstract

The Imperial Japanese Navy IKA cipher machine was a predecessor to the more familiar Japanese cipher machines of the 1931 and 1937 series. Nothing is known about the machine itself, but the cryptography of the machine is known. What follows describes the cryptography of the IKA machine and discusses that machine in the context of the 1931 and 1937 series of Japanese cipher machines that followed it.

1 IJN Cipher Machines

In the 1930s and 1940s, the Imperial Japanese Navy used a succession of three cipher machines for secret administrative matters among shore stations. The US Navy's codebreaking section OP-20-G referred to the ciphers as the "dockyard ciphers." Until 21 July 1933, the machine that was used was called IKA[1] (and the cipher was designated JN 111). It was followed by a machine designated M-1, or ORANGE (JN 141). M-1 was one of a series of three Japanese cipher machines that are referred to as the 1931 series: M-1, M-2 (naval attaché cipher), and RED (diplomatic cipher). These cipher machines were replaced by the three machines of the 1937 series: JADE, CORAL, and PURPLE, respectively. JADE (JN 157) was the last in the succession of dockyard cipher machines.

The Japanese language can be written in three different sets of characters. Kanji uses Chinese characters, and each character represents a word or phrase. Kanji precisely expresses language. An alternative method of expressing Japanese is kana. There are two versions of kana – hiragana and katakana -- which consist of 46 basic symbols plus some additional symbols and diacritical marks. Kana is syllabic, and each character corresponds to a sound. It is not unusual that several kanji have the same expression as kana. Reading kana is similar to deciphering a polyphonic cipher. Japanese has a special "kana Morse" code, and that code was used by the Imperial Japanese Navy to transmit codes and ciphers that used kana characters. The third method of expressing Japanese is romaji. Romaji uses Roman letters to transliterate kana. The three dockyard ciphers mentioned above used katakana characters.

The cryptography of the 1931 series machines was based on the Damm half-rotor and a 47-pin break wheel that staggered the motion of the half-rotor.

Unlike a full-rotor, a half-rotor has contacts on only one side of the rotor. The Damm half-rotor consisted of a rod with a disk on one end (Figure 1). Along the rod were slip rings through which the electrical charge from the plaintext typewriter keys entered. The slip rings were wired to outputs on the half-rotor's disk. Consider the enciphering of the six-letter alphabet shown in Figure 1. Letters on the slip rings are wired to the same letters on the half-rotor disk. The half-rotor disk makes contact with an output disk that is connected to the ciphertext typewriter. The output disk is labeled in the same manner as the disk on the half-rotor. Corresponding to Figure 1,

[1] In some documents the name appears as I KA. It appears to be the romanization of two kana characters.

if the letter A were typed on the plaintext typewriter, an electrical charge would enter the half-rotor by means of the slip ring corresponding to A. The charge would pass to the A-position on the half-rotor disk. If the A-position on the half-rotor disk were in contact with the A-position on the output disk, then the ciphertext typewriter would type an A. Corresponding to Figure 1, when a letter was typed on the plaintext typewriter, the half-rotor would step one position -- in this case, clockwise. If plaintext A were typed in the initial position of the half-rotor, the corresponding ciphertext letter would be A. If the half-rotor stepped one position and the plaintext A were typed again, ciphertext E would be typed. Then I, O, U, Y, A, etc. If the half-rotor stepped one position for each letter, the rows of the enciphering table correspond to the six successive encipherings of the plaintext letters which are shown in the table. The cipher is polyalphabetic; the cipher shown cycles through the six alphabets that are the rows of the enciphering table. The enciphering table has the pattern of the classical Vigenère cipher.

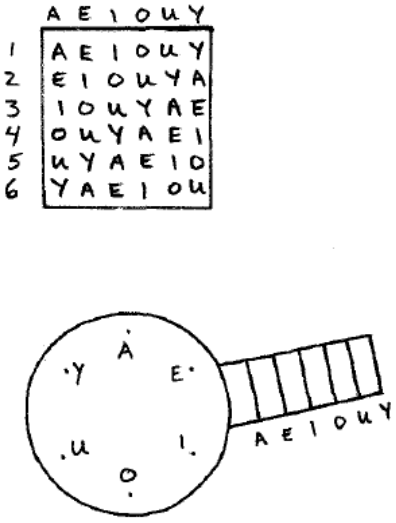

Figure 1. Damm half-rotor. (Raven)

The 1937 machines had regular stepping and composed ciphers that were implemented with 25-point telephone stepping switches.

IKA was the simplest of the machines and preceded the 1931 series. What follows is a description of the IKA cipher and what is known about the machine. No IKA cipher machine was captured or seen by US Navy codebreakers. The description that follows is based primarily on RIP 28A[2] "The M-1 Machine System," (CNO 1946) which reflects what the Navy knew about the IKA machine and its successor M-1 in April 1946. What the Navy knew about the IKA machine was based on their analysis of ciphertext messages. RIP 28A notes that there was little early data on either machine and that the data that existed was contradictory and confusing. It also notes that until 1936 IKA might have been known as M-1 and ORANGE as M-2.

2 Cryptography

Two stories describe trips to Europe by Japanese representatives to examine cipher machines. One describes a trip "commencing in approximately 1927" during which the Japanese acquired several commercial cipher machines including Enigma and Kryha. (Wenger, 286) The other tells of a trip in the early 1930s to Aktiebolaget Cryptograph, which had at that time been acquired by Boris Hagelin. Hagelin suspected that the Japanese wished to purchase a few machines to copy and, therefore, told the representatives that he had none to sell. Noticing two of Arvid Damm's obsolete cipher machines, the Japanese purchased them. (Raven, 1) Principles from the Damm machines were included in the 1931 series of Japanese cipher machines.

Much is known about the cryptography of the IKA machine, but essentially nothing is known about the actual machine.

IKA enciphered katakana characters. 49 characters were used in the system, and they were split into a minor sequence of seven characters and a major sequence of 42 characters. The reason for the split is not known.

The seven characters in the minor sequence (kana characters will be shown in romaji) were:

[2] SRH 355, page 61, which was written in 1971 by Captain Jack S. Holtwick, Jr., describes Holtwick as the author of RIP 28A, which was issued on 1 September 1935.

Ciphertext	Plaintext
RO	Parenthesis
WI	RO
SO	Nigori
NU	Hannigori
O	SO
WE	NU
X	Stop

This was a monoalphabetic substitution cipher; it was consistent throughout all messages. Existing records do not indicate how ciphertext X was transmitted. Kana characters were transmitted using kana Morse code. (Nigori and hannigori are diacritical symbols.)

The sequence (i.e., the ordering) of the 42 other characters changed monthly. Here is the sequence for September 1932:

KI	RU	TE	MO	MI	TU	WA	MU	RA	SE	ME	RE	KE	HI
A	U	HE	YA	HA	NE	E	N	YO	HO	I	YU	SA	KU
KA	TA	MA	SU	NI	TO	FU	KO	TI	NA	WO	SI	RI	NO

The IKA machine enciphered the major sequence by sliding a copy of the sequence against a copy of itself by one, two, or three places as each character was enciphered. This staggered motion was produced by a 47-pin break wheel. Active pins on the break wheel caused the machine to step one position. One inactive pin caused the machine to step two positions, and two inactive pins in sequence caused the machine to step three positions. It was not possible to have more than two inactive pins in sequence. Depending on the key, between 12 and 15 pins were removed. The machine stepped even when the minor sequence was used.

3 Settings

There were 50 message keys numbered 01, 02, …, 50. The key for a message was the last two digits of the originator's serial number – subtracting 50, if necessary. In addition to determining the status of the pins, the key also determined the starting position in the sequence. Here are keys 01, 02, and 03 from the key list for 1 January – 20 July 1933:

Key	Positions of inactive pins	Starting point
01	1 6 11 15 19 22 25 29 33 36 39 43 45	10
02	2 5 8 11 15 16 21 24 27 31 34 37 41 45 46	11
03	3 4 10 13 14 18 23 27 28 32 35 40 41 45	23

IKA messages appear as a, possibly incomplete, rectangle of ten columns. RIP 28A includes message number 608 from 22 October 1932. What appears below is the message with the heading removed.

```
6   0   8   0   8   0   2   2   1   0
SA  NO  TI  NO  SE  RE  KE  KI  WO  RU
NA  HE  RE  WA  E   TA  MA  TA  KU  SA
A   TE  KO  NE  SI  A   NI  FU  SU  A
MA  YU  YO  SE  KE  SE  SA  RA  TU  SI
HI  YA  MA  YO  FU  YA  YO  NA  HO  WA
MU  HO  MO  MU  KI  MU  WA  U   YA  TO
ME  TE  HE  NO  RU  SE  NE  MI  SO  SA
TA  I   KA  HI  NO  YU  ME  KU  RA  KE
WA  ME  ME  N   HI  X   KE  SI  X   TO
ME  NA  HO  YO  KO  SA  A   NU  KE  ME
TI  KU  ME  YU  NE  KI  TI  O   HA  NI
TE  MA  WA  MI  TI  KA  HA  RE  HI  MA
MO  TU  MO  SI  NO  SE  SU  KO  MU  TE
E   YU  HE  TA  KE  SA  SE  TA  NI  RA
A   SI  RA  SE  SA  MO  TA  KU  N   TO
HI  FU  KU  MU  YU  HO  YU  SA  MA  TE
TO  KA  RI  O   TE  YU  YA  YU  MA  ME
A   TI  KO  HO  SI  KA  YO  MU  SI  HA
WA  YO  MA  HO  YA  YO  TU  NE  N
```

The separators that would appear at the end of each line are not shown. RIP 28A describes the separator as "unknown," but SRH 355 (Appendix 8, 90F) suggests that it was // (and, furthermore, that the Japanese character // was called "IKA," which was used for the name of the machine).

The ten reference numbers above the message include information that determines the key.

```
6   0   8   0   8   0   2   2   1   0
```

The first three digits are the message originator's serial number 608. The last two digits of that number 08 is the key. Because it is important that the key be transmitted ungarbled, those two digits are repeated as digits four and five of the reference number. Digit six 0 is the part number; this is a one-part message. Digits seven and eight are the day of origin 22. Digits nine and 10 are the hour of origin 10.

Key 08 on 22 October 1932 is a special key that appeared at the end of the keylist:

Key	Positions of inactive pins	Starting point
08	5 8 11 17 22 25 26 29 34 37 41 44 46	10

Because the major sequence is periodic, there is no true "starting point;" the term "starting point" refers to the offset of the plain and cipher components of the major sequence. A starting point of 0 would have plain and cipher components aligned with no shift. The other offsets could be as small as 1 or as large as 41.

4 Deciphering

Navy codebreakers took "KI" as the first letter in the sequence. For October 1932, the sequence was:

```
KI  HI  WO  ME  KE  TO  SA  KO  SE  HO  MU  NO  YU  RU
KA  FU  RE  RA  YA  SI  HA  TU  N   U   A   I   MA  TE
WA  MO  ME  KU  E   NA  TA  NI  YU  TI  RI  NE  HE  SU
```

Starting point 10, means an offset of 10 between the cipher (on top) and plain alphabets:

```
KI  HI  WO  MI  KE  TO  SA  KO  SE  HO  MU  NO  YO  RU
MU  NO  YO  RU  KA  FU  RE  RA  YA  SI  HA  TU  N   U

KA  FU  RE  RA  YA  SI  HA  TU  N   U   A   I   MA  TE
A   I   MA  TE  WA  MO  ME  KU  E   NA  TA  NI  YU  TI

WA  MO  ME  KU  E   NA  TA  NI  YU  TI  RI  NE  HE  SU
RI  NE  HE  SU  KI  HI  WO  MI  KE  TO  SA  KO  SE  HO
```

The 22 October 1932 intercept has starting point 10, therefore, the first character `SA` deciphers to `RE`. Following the Navy's procedure, the plaintext alphabet (i.e., the bottom row above) slides to the left. To decipher the second ciphertext character, the plaintext alphabet slides one position to the left, and ciphertext `NO` deciphers to `N`. To decipher the third ciphertext character, the plaintext alphabet slide one more position to the left, and `TI` deciphers to `KO`. Next, `NO` deciphers to `A`, which in plaintext represents the diacritical symbol nigori. The nigori signals that the `K` is to be voiced; so `KO` becomes `GO`.

Pin 5 is inactive; therefore, the next slide is two positions, and `SE` deciphers to `U`. And, the deciphering continues.

Deciphering can be done by hand with sliding alphabets while giving attention to whether pins are active or inactive.

Cryptographically IKA was similar to the Kryha machine. It also is cryptographically similar to a Damm half-rotor with staggered motion.

There does not seem to be any description of the physical machine. In particular, there is no record of how the staggered motion of the cipher alphabet against itself was produced nor how plaintext was entered and ciphertext outputted.

There also does not seem to be any record of how the machine was attacked. RIP 28A contains the comment, which seems to refer to both IKA and M-1, that:

> Unfortunately there are no longer any records available of the cryptanalytic attacks used in recovery of the machine. Whatever the methods, the solution must be recognized as a cryptanalytic masterpiece in the pioneering of machine solutions. (CNO 1946, 1)

5 Relationship to Other Japanese Cipher Machines

The IKA machine was replaced on 21 July 1933 by M-1. RIP 28A notes that there was a slight change in the machines. (CNO 1946, III-1) The major sequence of 42 characters was identical with the major sequence of IKA; however, the minor sequence consisted of 14 characters rather than the 7 characters of IKA's minor sequence. The minor sequence of the M-1 was the minor sequence of IKA with the X character removed and the digits – excluding 2 and 8 – added to the sequence. The plaintext for characters in minor sequence mostly consisted of diacritical marks, punctuation, and "stop."

M-1 output consisted of 10 x 10 blocks of kana characters.

Although the sequence of the characters of the major sequence was part of the machine setting, the characters in the minor sequence were always in the same order.

The polyalphabetic nature of the M-1 was caused by a Damm half-rotor. The minor and major sequences stepped together. Effectively, the enciphering consisted of a 42-position half-rotor with one of the 42 characters of the major sequence in each position on, say, the edge of the disk and the 14 characters of the minor sequence repeated three times, say, around the disk just inside the positions of the major sequence. Because a Damm half-rotor produces Vigenère tables, M-1 would produce two Vigenère tables – one with period 14 for the minor sequence and one with period 42 for the major sequence. The total period produced by the half-rotor is 42.

It is not known how IKA physically stepped the major sequence – whether, for example, it stepped with a half-rotor or with sliding disks like Kryha.

Similar to IKA, a 47-pin break wheel was used to extend the period of the M-1.

Two M-1 machines were captured at Rashin, Korea, at the end of the war. One of those machines (Figure 2) is on display at the National Cryptologic Museum, which is located next to NSA Headquarters in Fort George G. Meade, Maryland.

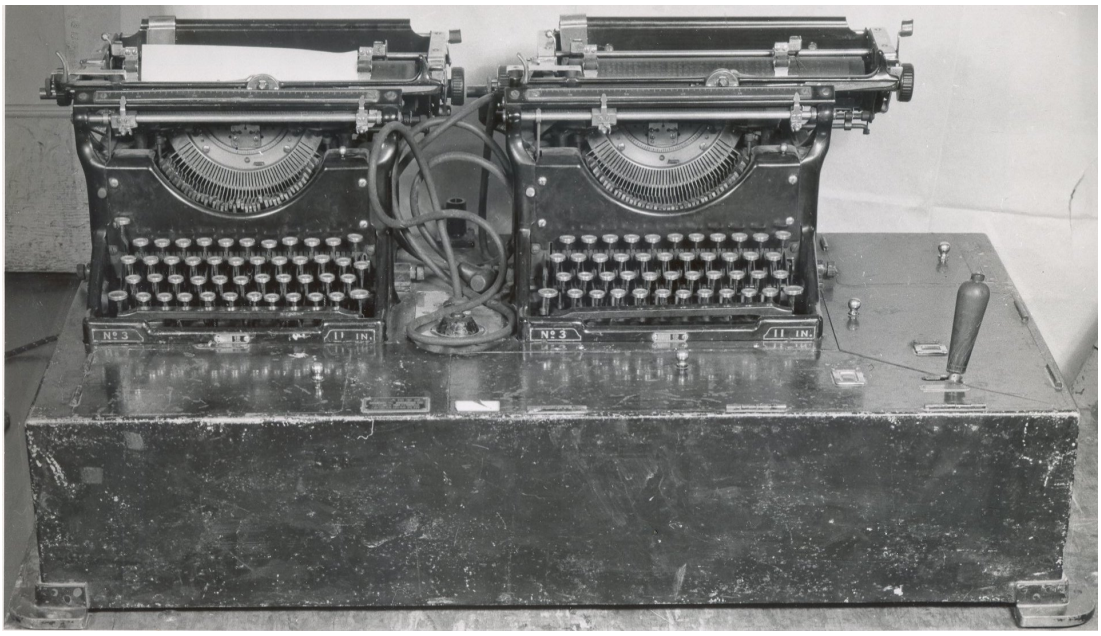

Figure 2. An M-1 cipher machine that was captured at Rashin, Korea after World War II. Courtesy of the National Security Agency.

All three of the 1931 series of Japanese cipher machines had a minor and major sequence, used a Damm half-rotor, and implemented irregular stepping by means of a 47-pin break wheel.

In the 1937 series of cipher machines, JADE replaced M-1. JADE had a 25-character minor sequence and a 25-character major sequence – low frequency and high frequency kana, respectively. The keyboard had 25 keys and a shift key to shift between sequences. Enciphering was implemented using 25-point telephone stepping switches. The period, which was length 25 for each switch was extended by composing the switches. JADE had 5 switches. The first three switches stepped; the last two switches were set to a given position but did not step. There was a plugboard only on the ciphertext side. The first three switches stepped regularly – one switch was fast, one was medium, and one was slow. Only three of the possible six orders of motions were available: fast-slow-medium, slow-medium-fast, and medium-fast-slow.

JADE came into use in 1942. It did not received much use. There was a break in its use for two weeks at the end of April 1943. Kwajalein was one of the heavy users, and after the Allied invasion (31 January – 3 February 1944) the shutting down of that station reduced the use of JADE significantly. Use was further reduced after a bombing of Rabaul. The last JADE intercept was 30 August 1944.

6 Analog

There is considerable confusion about an analog – or analogs -- designed by Holtwick. He is variously credited with designing an analog for IKA or an analog for M-1. Captain Laurance Safford refers to an analog designed by Holtwick about 1937. Although that occurred after the 1931 series of cipher machines, Safford notes that

> The cipher system was considerably older and had been solved for several years. … [We] had always read the messages by paper and pencil methods and rotating disks. Holtwick made an arrangement in which a kana typewriter was mounted on a box and inside of this box as a cylinder with pins. The pins were pluggable on the rotating cylinder. I do not recall whether its action was electrical or mechanical. The effect of the pins was chiefly to give an irregular stepping cycle. Two machine were built: one was retained at the Navy Department and the other sent to [Pearl Harbor]. Just about the time we got the machine to

> [Pearl Harbor] the Japanese abandoned the system so the machine actually never did any particular good. (Safford 3 February 1944, paragraph 2)

SRH 355, which was written by Holtwick, notes that:

> [Holtwick] assumed (incorrectly, as it turned out) that the M-1 was but the initial one of an era of cipher machines that would supplant codes and manual ciphers in Japanese Naval communications … .
>
> With this possibility in mind, he designed and roughly sketched a mechanical device, including interlocking gears and pin-controlled stepping sequences, which would not only duplicate the stepped slidings of the cipher sequence recovered in the M-1 machine, but included methods for coping with more complicated variations of the sequence, some of which he assumed the Japanese cryptographers might introduce in their next version of the machine. (SRH 355, 161)

As noted, however, the Japanese moved away from irregular stepping with the 1937 series of machines.

SRH 355 states that the M-1 analog was designed in 1935 but not completed until 1937. A 13 May 1937 letter to Holtwick from Lieutenant Joseph Wenger mentions that an M-1 analog and other material were being shipped to Pearl Harbor so that that station might take over deciphering of M-1. However, the last definite M-1 intercept was from March 1937.

SRH 355 (i.e., Holtwick) states that "Occasional reference to Holtwick's machine as the IKA may be encountered; these are not valid." (SRH 355, Appendix VIII, 90F) That seems to confirm that Holtwick's analog was designed for M-1 – not for IKA. Furthermore, SRH 355 assigns the designation RIP 41 to M-1. (SRH 355, Appendix VIII, 90G)

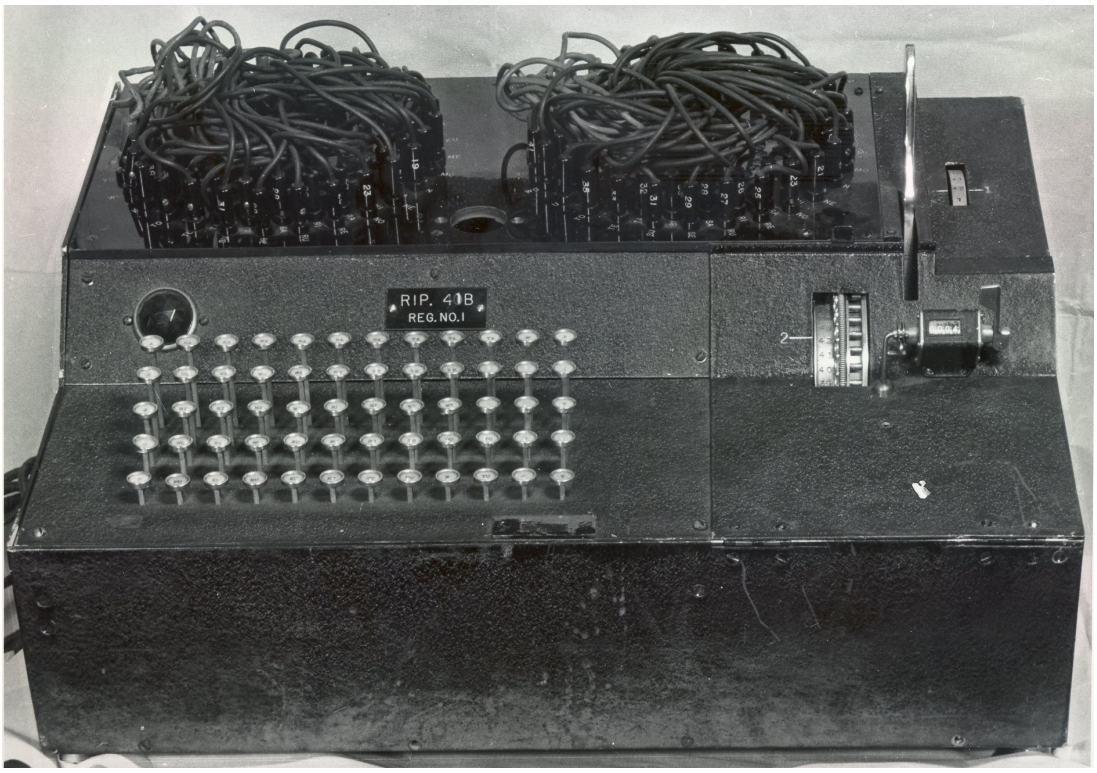

Figure 3. Holtwick's analog for the M-1 cipher machine. Courtesy of the National Security Agency.

Figure 3 is a photograph from NSA files of a machine designated RIP 41B, which therefore should be Holtwick's M-1 analog. The keyboard and plugs are labeled with kana characters. The wheel on the top right has 42 positions and should set the starting position. The wheel to the

left of the counter appears to be a 47-pin break wheel.

7 Conclusion

The IKA and M-1 cipher machines are cryptographically similar. Although M-1 machines were captured and, therefore, the nature of the physical machine is known, nothing is known about the physical IKA. It could have had a design like the Kryha – a machine with which the Japanese were familiar. IKA was in service only briefly before it was replaced by M-1. Holtwick designed an analog for M-1, but by the time his analog was constructed M-1 was no longer in use and the irregular stepping that Holtwick had expected to continue to evolve in use with subsequent Japanese cipher machines was replaced by regular stepping with composed switches.

References

Chief of Naval Operations. April 1946. "The M-1 Machine System: RIP-28A." National Archives and Records Administration College Park RG 38 Box 16.

Holtwick, Captain Jack S., Jr. 1971. SRH 355 "History of the Naval Security Group to World War II." Reprinted by U.S. Naval Cryptologic Veterans Association, Pensacola, FL.

"History of JNA-20 – Coral, Volume II." National Archives and Records Administration College Park RG 457, Box 1387.

Raven, Francis A. Undated. "Some Notes on Early Japanese Naval/Diplomatic Cipher Machines," CCH Series Files IV.W.III.23.

Safford, Captain L. F. 3 February 1944. "Memorandum for Lieutenant Commander Raven, Subject: History of Japanese Cipher Machines." National Archives and Records Administration College Park RG 457 Box 808.

Wenger, Jeffrey Joseph. Unpublished manuscript. "RADM Joseph N. Wenger, USN. Biography & Autobiography. Communication Technology in World War II to Computer Technology. "National Cryptologic Museum Library.

Appendix A

Information about Japanese Cipher Machines

IKA

Enciphering device	Unknown Sequencing of major alphabet
How period was extended	Staggered stepping
U.S. intercept dates	Late 1931/early 1932 – 21 July 1933
User	Major IJN stations
Alphabet	Kana
Split of alphabet	42/7

1931 Series

Enciphering devices	Damm half-rotor Input and output plugging
How period was extended	Staggered stepping caused by 47-pin break wheel

Machine	RED (or M-3 or Type A)	ORANGE (or M-1)	M-2
User	Diplomats	Major IJN stations	Naval attachés
Alphabet	Romaji	Kana	Romaji
Split of alphabet	6/20	42/14	Perhaps identical with RED
U.S. intercept dates		20 July 1932 – March 1937	
Replaced by	PURPLE	JADE	CORAL

1937 Series

Enciphering devices	25-point telephone stepping switches Input and output plugging except JADE (output only)
How period was extended	Composition of switches

Machine	PURPLE (or M-5 or Type B)	JADE	CORAL
User	Diplomats	Major IJN stations	Naval attachés
Alphabet	Romaji	Kana	Romaji
Split of alphabet	6/20	25/25	None
U.S. intercept dates	20 February 1939 – end of World War II	1 December 1942 – 30 August 1944	8 September 1939 – end of World War II
Number of composed switches	3 for 20s 1 for 6s	3 stepping 2 stators	3