Red and Purple: A Story Retold (U)

[redacted] (b)(3)-P.L. 86-36

~~(C-CCO)~~ *After studying the techniques used to solve World War II-era Japanese machine cipher systems, a small group of analysts attempted to use present-day techniques to solve these systems. The results were not what one might have expected.*

Introduction

~~(C-CCO)~~ Could modern computer techniques be used to solve the Japanese machine cipher systems of World War II? In June 1982, NSA analysts in the course "Japanese Cipher Devices of World War II" discovered that the task was not so easy. The purpose of the course, a part of the CA Summer Program in Innovative Cryptologic Education (SPICE), was to study the techniques used to solve Japanese machine cipher prior to and during World War II, and then to attempt to use modern techniques to solve these systems.

~~(C-CCO)~~ The seven individuals involved in the class included analysts from A, B, R, E, and P1, and two CA interns. One of the CA interns, at the time on tour in E42, taught the course and wrote this article. For two months she researched material in the NSA archives and in the Cryptologic Collection of the NSA library. Using original material, she prepared the machine data base on JEEP, along with problems from a course on Purple that is in the Cryptologic Collection.

~~(C-CCO)~~ The students were given five actual messages to analyze before they knew anything about the systems. The instructor had expected the properties she had studied in her research to surface in the initial analysis. This was not the case.

~~(C-CCO)~~ The problem, discovered during the analysis, was that the messages were not homogeneous. One was plain text, one was a variation on a later Japanese transposition system, two were Red, and the final one was of unknown origin (possibly Purple). There were not enough messages available to solve a system, and what was available did not demonstrate the properties that led to the breaking of the system. Though the class was unable to solve the system with the messages available, it was possible to study the historical solution of the system.

The Breaking of Red

~~(SC)~~ The M-3 cipher machine, held by all the major embassies of Japan in the early 1930s, was modified on 1 December 1938 for extra secret messages. The modification was called M-3A. On 20 February 1939 the M-3A was replaced with M-3B. American analysts named the M-3 and M-3A cipher Red, while cipher from the M-3B was called Purple.

~~(SC)~~ In the first M-3 messages, intercepted in March 1933, there were two classes of letters, vowels and consonants, with different frequency distributions. As there was not much traffic, the messages were put into one of those "to be looked at when there is nothing else to do" bins. However, it was postulated that vowels were substituted for vowels, and consonants for consonants. Two reasons for this supposition were that (*a*) telegraphic regulations allowed cheaper rates for pronounceable text (pronounceable meaning a minimum of two vowels per five-letter grouping) and (*b*) the transliteration of Japanese characters is unusual in that vowel-for-vowel and consonant-for-consonant substitution produces a pronounceable cipher. [1]

~~(SC)~~ In March 1934 the characteristics of the cipher changed. Though the text still divided into two classes, one with six letters and the other with 20 letters, there was a mixing of vowels and consonants in each class. At that same time there was also a change in telegraphic regulations: there was no longer a special rate for pronounceable text.[2]

~~(SC)~~ The initial study of the intercept revealed the following:

1. The messages had a five-digit indicator in the first group of the message.

2. The text was definitely cipher.

3. The nature of the substitution was such that repetitions were permitted to occur.

4. There was a radical change on the 1st, 11th, and 21st of each month.

5. The keying element produced a long cycle which appeared indeterminate in length.[3]

~~(SC)~~ From Manchuria in 1936 came an influx of cipher messages (10–15 per day) which exhibited the above properties. In particular, extensive traffic was received from 11–20 December, a single cipher period.

~~(TSC)~~ When the attack against the December messages came to a standstill, the analysts turned to the 1933 messages. One of these analysts, a Japanese linguist, thought of exploiting the fact that the doublet "OO" occurs frequently in Japanese, as does the aba construct "O-O." If the machine used rotors, then the sequence of letters on a wheel could be discovered when the wheel enciphered the same letter consecutively. The analysts made up the following two tables from the vowels in the longest message in the 1933 collection. The first table shows the

[1] *RED and PURPLE*, undated (pre-1960), S-119-785, U.S. Army A.S.A., p. 1.
[2] Ibid.
[3] Ibid., p. 2.

occurrence of two vowels next to each other; the second table shows the alternating vowels.

ADJACENT VOWELS (V–V)

	A	E	I	O	U	Y
A	6	9	4	0	4	4
E	5	2	8	2	3	5
I	5	6	3	1	5	8
O	4	4	0	3	13	7
U	9	1	2	6	0	1
Y	3	1	5	14	0	4

ALTERNATING VOWELS (V–C–V)

	A	E	I	O	U	Y
A	16	19	35	22	12	30
E	7	25	20	21	13	33
I	28	13	26	36	17	22
O	35	24	23	13	16	17
U	16	23	17	17	9	14
Y	22	19	20	21	23	31[4]

~~(TSC)~~ The chart of alternating vowels was studied first. The first step in chaining is to look for the highest number in the matrix. This number is 36, which corresponds to position I–O. For the next letter, look in the O row. O–A is the largest occurrence with 35, so the chain I–O–A appears hopeful for a rotor solution. In the A row, the highest frequency is A–I and next is A–Y. The description of the original analysis is hazy at this point, but the end result was that the analysts postulated two separate chains, I–O–A and E–Y–U. From the chart of adjacent vowels, a sequence of Y–O–U–A–E–I made sense, which fit together with (and was perhaps the reason for) the hypothesis from the V–C–V chart. Once the analysts had a sequence for a 6-long wheel, they found it possible to substitute values for vowels in the message, and then to guess plain text, based on their knowledge of past messages.

~~(TSC)~~ Next they considered the messages in their ten-day period from December 1936. They isolated the sixes and figured out that the order was BEIHOX. However, in the messages they were working, inconsistencies kept appearing. It was finally discovered that some messages had the sequence B–E–I–H–O–X, and others had the sequence X–O–H–I–E–B.

~~(TSC)~~ At this point the Navy analysts were consulted to find out if they had worked any similar systems. Lieutenant Wenger of the Code and Signal Section reported that the Navy had worked a machine with a 6-wheel, a 20-wheel, and a break wheel of 47 teeth, some of which were inoperative.[5]

[4] Ibid., p. 3.
[5] Ibid., p. 8.

~~(TSC)~~ If there were 47 active teeth on a break wheel with a 26 long alphabet wheel, then there would be a cycle length of 26 × 47 (1222), and coincidences would be observed more frequently on a width of 1222. In the case of a 6-wheel, a 20-wheel, and a break wheel with 47 effective teeth, the expected cycle length would be 20 × 6 × 47. Because of the common factor of 2, the cycle length would actually be 20 × 3 × 47.

~~(TSC)~~ The problem with measuring a cycle length of this size was that the messages were under 2000 characters long. The analysts therefore concentrated on the cycle of the 6-wheel. They considered counts for widths of 6 × 31 through 6 × 47. The highest count was for 6 × 43, width 258. The hypothesis from this information, which was correct, was that there was a 47-long break wheel, with 43 effective teeth.

~~(TSC)~~ In order to locate the places on the wheel where there were skips (four skips in each cycle of 43), the message was written on a cycle of 43 letters. It was then possible to align the skips vertically. Adjacent columns could be matched to give the relative shift between the columns.[6]

~~(TSC)~~ Further analysis led to a complete understanding of the Red machine and of the indicator system of the messages. It was possible to build an analog machine and to decrypt virtually all of the messages. Figure 1 is a photograph of an analog machine. It consists of a plug board, an interrupter wheel, a large alphabet wheel, a small alphabet wheel, a reversing gear, and an operating handle. The two alphabet wheels are under the plugboard.[7]

~~(SC)~~ There were 240 indicators for the settings of the three wheels of the machine. In addition, the sequences for the two alphabet wheels were set up on a plugboard which was changed daily. For key numbers starting with 0, 1, 2, or 3, the machine ran in ascending order, while for numbers 4, 5, 6, 7, 8, or 9 the machine ran in reverse order.

~~(TSC)~~ The following steps are instructions for deciphering the M-3A machine. Tables 1-A and 2 (mentioned below) had been generated by the analysts and were available to the decipherers.

1. Obtain the message key number used in enciphering by subtracting from the transmitted key number the following numbers:

a. 1st to 10th of the month	-- 32210
b. 11th to 20th of the month	-- 23120
c. 21st to the end of the month	-- 12320

2. Enter table 1-A with the date and pick out the plugboard sequence. The sequences vary with message key number for any one date.

3. With the key number (obtained by subtraction) enter table 2, pick out the initial settings for wheels B, C, and D, and set the wheels accordingly.

[6] Ibid., p. 9.
[7] R.I.P. 6, p. 1.

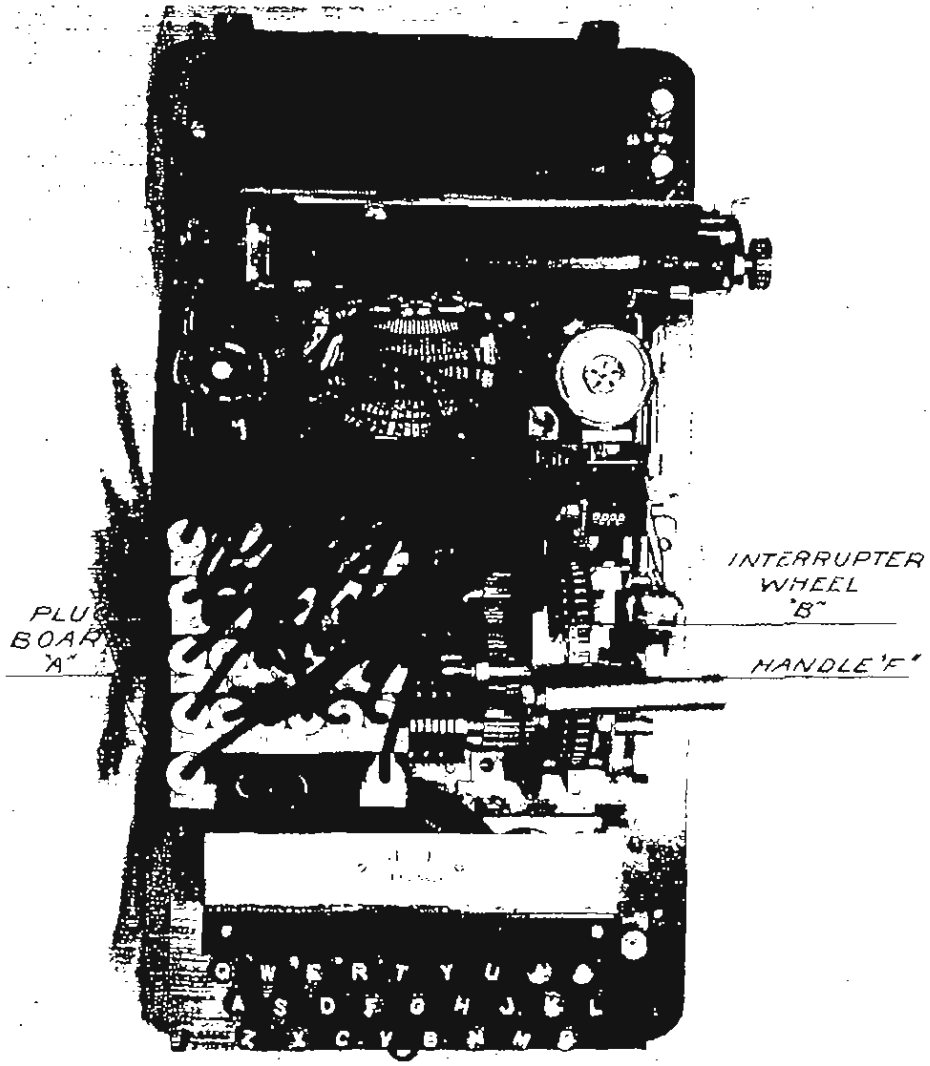

Fig. 1. Analog of the Japanese M-3 (Red) Cipher Machine

4. From table 2 pick out pin settings for interrupter wheel and set pins.

5. Decipher the first five letters of text. Reset the machine to its original setting. Decipher the next 495 letters. Pause. Pull handle 10 times. Continue. (This break at 500 was in effect for only a few months.)[8]

Because they were able to read the Red messages, our analysts learned about Purple even before the Japanese had started to use it.

The Breaking of Purple

~~(SC)~~ In December 1938 a message appeared in Red cipher which authorized a man named Okamoto to put certain cryptographic devices into service. The Japanese diplomatic officer referred to the machines as the Type B cipher machines. They were to replace the currently used Type A (Red) machine for highly secret communications between important Japanese embassies throughout the world and the Foreign Office in Tokyo. The B machine would go into effect on 20 February 1939.[9]

~~(SC)~~ The first message received after 20 February came from Warsaw, Poland. The message contained an indicator different from the normal A type. Six of the 26 letters had abnormally high frequencies, which was characteristic of traffic enciphered by the Red machine. The A machine continued to be used on a regular basis in Hsinking and Shanghai, and occasionally (apparently when the B machine was out of commission) at places which had been provided with a B machine. The B machine was assumed to be a modification of the basic A machine.

~~(TSC)~~ By April 1939 it was possible to decipher the sixes of the Purple messages in most cases. In the set of six letters each letter had about the same frequency; likewise in the set of twenty letters each letter had about the same frequency, but different from that of the smaller set. If the set of six contained two high frequency letters, the frequency of the six would be significantly higher than the twenty. If the six contained two low frequency letters, the frequency of the six would be significantly lower than the twenty. Either of these cases ensured that the sixes could be isolated. It was discovered that, out of 120 different indicators, there were only 25 unique starting points. A distribution table was built from which an analyst could recover the starting point of the sixes, and then fill in all plaintext values for the sixes. Appendix A is the explanation of this distribution table which was given in the course on Purple (available in the Cryptologic Collection).

[8] Ibid.

[9] William Friedman, "Preliminary Historical Report on the Solution of the "B" Machine," 14 October 1940, p. 1.

~~(SC)~~ Once the sixes and their starting point were recovered, it was possible to determine if the language was English or Japanese and to guess plaintext values. The assumption of plain text was facilitated by stereotypic message beginnings. For example, in the following message the sixes were recovered as E–Q–A–D–R–H, and the correct placement of these sixes was determined as follows:

```
Cipher: BRAXE FQCEV QOOXH ECFDL NHQRV QPPLC ERP
Plain:  .HE.A .A.E. E...E R..E. .REQ. E.... HA.
```
[10]

~~(SC)~~ The correct plain text was postulated to be "The Japanese government requests that . . . ." From the additional matched plain and cipher, the analysts could attempt to recover the 20-long alphabet.

~~(SC)~~ On 1 May 1939, the Japanese Foreign Office instituted a special code (Phillips Code) in connection with the use of the B machine. Often "text," when finally reconstructed, appeared more like code or a random assortment of letters, than like plain text. While this at first made the problem harder, once the code groups had been recovered the values provided excellent cribs, especially as message beginnings. The following is a typical stereotypic beginning for a message in Japanese which used the Phillips Code.

```
Cipher: FGPXP IXUDB DGECZ LBLNU ZQOQH YNMRQ ARJOP DEILO
Plain:  XFCGJ WFOVD DNOBB FYXFO CFYLC CFMSG TSJVR KHIFI

Cipher: AXPPP LIGDK ZDGRA
Plain:  CGURV FELBK WTLSI
```

[redacted]

XFC	=	Number	CCF	=	paragraph	
GJW	=	15	MS	=	3	
FOV	=	open parentheses	GTS	=	month	(b)(1)
DD	=	2	JVRK	=	16	(b)(3)-50 USC 403
NO	=	of	FIC	=	Begin kana spelling	(b)(3)-18 USC 798
BB	=	1	FEL	=	End kana spelling	(b)(3)-P.L. 86-36
FYX	=	close parentheses	GURV	=	Grew	
FOC	=	secret	BKW	=	United States	
FYL	=	additional classification	TLSI	=	Ambassador	

[10] Ibid., p. 2.

~~(SC)~~ The translation of this much of the message is "Number 15 (part 1 of 2) SECRET, to be kept within the department. Paragraph: On March 16, the American Ambassador Grew . . . ."[11]

~~(TSC)~~ Once a few words were known, it was sometimes possible to guess the subject of the message, and on occasion, to find government documentation on the subject. Some messages were exact quotes of particular documents. Another help in deciphering messages occurred when an operator transmitted a message in a known cipher, and then retransmitted the same message in Purple. There were several occurrences of isologs of this type. Plain text for parts of 15 fairly lengthy messages was obtained. These were subjected to a most "intensive and exhaustive" cryptanalytic study. In this study, the following phenomena were observed:

1. The ciphering mechanism started from a certain initial setting and progressed methodically without cyclic repetition of any sort to the end of the message. The longest message was over 1500 letters long.

2. Two identical plaintext letters in sequence could never be represented by two identical ciphertext letters. This phenomenon is termed "suppression of duplicate encipherments at the first and 26th intervals."

3. Two messages with identical indicators on the same day appeared to be identically enciphered and on direct superimposition – and when written on a cycle of 26 – were monoalphabetic within columns, but with the alphabet constantly, irregularly, and unpredictably shifting from column to column.

4. Two messages with identical indicators on different days were absolutely different.

5. Two messages with different indicators on the same day (i.e., same plugboard arrangement) were absolutely different – no cryptographic similarities whatever.

6. In each line of 26 letters, two identical letters could be identically enciphered except under certain conditions. Two adjacent letters were never identically enciphered, and two letters at intervals two, three, four, or five from each other were rarely enciphered identically.[12]

~~(TSC)~~ At this point in the study, the World War II analysts felt that with 20–25 messages with the same indicator on the same day, it would be possible to find a

[11] Ibid., p. 3.
[12] Ibid., pp. 4–5.

cyclic repetition and to solve the system. There were never more than two messages that met this condition. A second possibility was to convert several messages with the same indicator but on different days to the same base. In a thousand or more messages, a mere six were found which met this second condition. These six messages, with indicator 59173, were the key to the breaking of the system.

(TSC) The analysts discovered repeated sequences within these six messages on 20 September 1940 at 2 p.m. The first complete solution came one week later, on 27 September, the same day that Germany, Italy, and Japan signed the Tripartite Agreement. Two of the six messages were completely deciphered, and the other four were partially deciphered. More important, from this solution the analysts were able to build distribution tables which could be used to solve any message with indicator 59173. Since there were 120 indicators, only 119 were left to be solved.[13]

(TSC) One reason that the solution of Purple was so difficult was that the analysts had assumed that Purple was a rotor machine, like Red. In fact Purple was a uni-selector machine (see Appendix B). With Red, the sixes and the twenties were enciphered by a commutator whose stepping was controlled by a break wheel of 47 positions with certain skips in the cycle. With Purple, the sixes were enciphered by means of a single uniselector. The encipherment of the twenties was performed by three uniselectors in series.

(TSC) In more detail the machine consisted of 13 switches, each of 25 points. These switches were of the type used in automated telephony. One of the 13 switches controlled the encipherment of the sixes. This switch went through the same 25-point cycle over and over, as many times as necessary to encipher the message. The twenty-five different alphabets used in the enciperment were a carefully selected set of 25 of the possible 720 permutations of six elements. The remaining 12 switches enciphered the twenties. There were three banks of four switches each. Each bank contained 25 points which yielded 25 cubed or 15,625 different sequences for enciphering the 20-long alphabet.[14]

(TSC) The motion of Purple – difficult to describe – can be thought of as four wheels. The single switch that controlled the encipherment of the sixes will be called the fast wheel. The banks of switches that controlled the enciphering of the twenties can be thought of as three wheels: a delayed fast wheel, a medium wheel, and a slow wheel. These three wheels could be changed to any of six possible orders of motion: 1–2–3, 1–3–2, 2–1–3, 2–3–1, 3–1–2, and 3–2–1, where 1 represents the delayed fast wheel, 2 the medium wheel, and 3 the slow wheel. The fast wheel moved every time. The delayed fast wheel moved except when the medium or slow wheel moved. Thus the delayed fast wheel moved for 25 steps, and then paused as the medium wheel moved. When the medium wheel reached 25, and the fast wheel reached 24, the delayed fast wheel paused as the slow wheel

[13] Ibid., p. 6.
[14] R.I.P. 77, p. 1B-1.

stepped, and then continued to pause as the medium wheel stepped.[15] The following chart depicts what happens when the slow wheel turns.

Fast Wheel	Delayed Fast	Medium	Slow (1–2–3 motion)
23	1	25	1
24	2	25	1
25	2	25	2
1	2	1	2
2	3	1	2
3	4	1	2
.	.	.	.[16]

(TSC) Of the 120 indicators, 20 were used for each type of motion. The differences within each type of motion were determined by the starting point of the wheels. The starting points had been carefully selected by the Japanese to reduce the possibility of overlaps and to avoid messages in depth.[17]

(TSC) There were three cryptographic elements of Purple which had to be recovered if every Purple message were to be read.

1. The basic wiring of the switches.
2. The setting of the switches.
3. The *plugboard sequence* used for enciphering the message.

The first element, the basic wiring of the switches, was determined in the solution of the first few messages. This fundamental part of the system did not change. The setting of the respective switches was determined by the key (transmitted in the first group of the message). This remained constant, once determined for any one message, and was then known for all messages with the same key. The third element, the sequence used for any particular message, changed from day to day. In order to read all messages enciphered by means of this system (once the basic wiring of the rotary switches had been recovered and the settings for the switches for each of the 120 keys determined), only the third of the basic elements had to be recovered cryptanalytically. Since this was a function of the date, the problem became a matter of solving a new sequence for each day's traffic.[18]

(SC) Once the initial success was achieved, the analysts set out to create an analog machine. Figures 2 and 3 show this machine, which may be viewed at the NSA archives. As of 1 April 1941 it was possible to read 99 percent of the intercepted traffic. In addition, it had become possible to determine the route

[15] R.I.P. 77, p. 2–20.
[16] Ibid.
[17] Friedman, p. 7.
[18] Ibid., p. 2–3.

Fig. 2. Analog of the Japanese M-3B (Purple) Cipher Machine

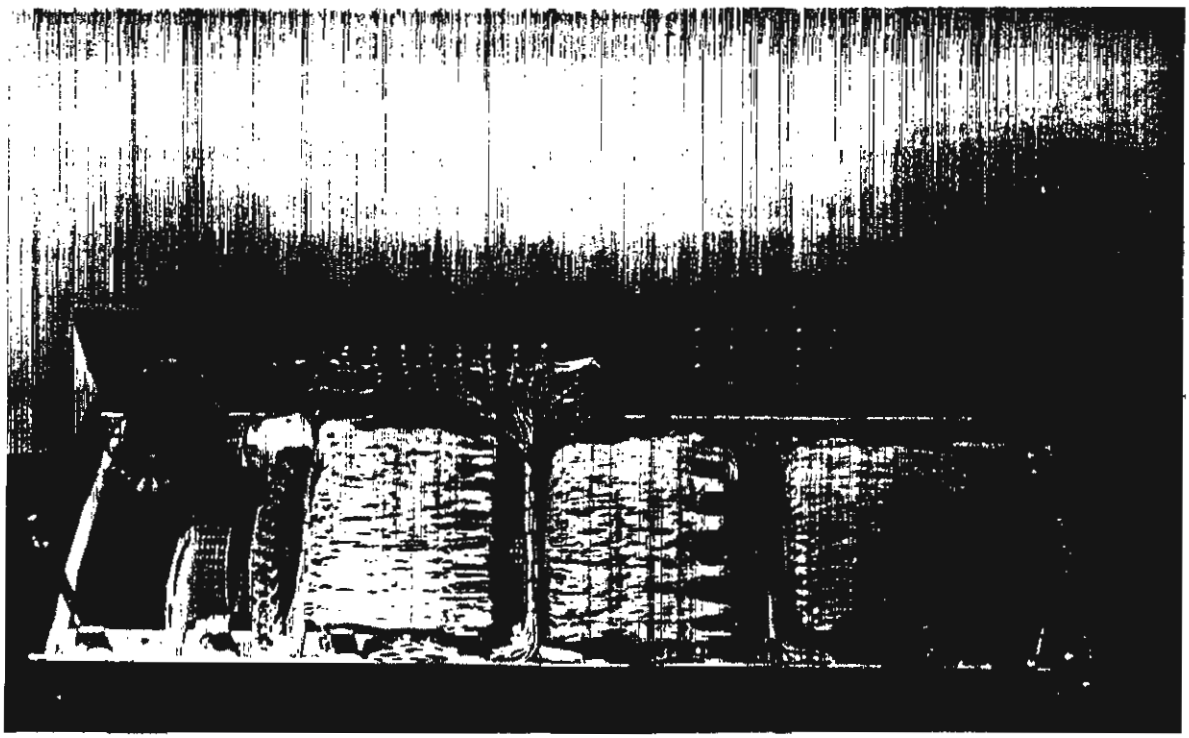

Fig. 3. View of Purple Analog Machine Showing Wiring of Selector Switches

being used to select the daily sequences in the Japanese book and to reduce the sequences to basic form. Finally, it became possible to reconstruct the sequences that were in the Japanese book and to make use of the recovered sequences. Fifty percent of the sequences from the Japanese book had been recovered as of 1 April 1941.[19]

~~(SC)~~ The Japanese transmitted all forthcoming changes in the system. Thus, the analysts were kept wellposted on indicator additives or selector starting points.

~~(TSC)~~ The following instructions could be used to decipher a Purple message.

1. From the date of the message, look up an additive to subtract from the five digit indicator (first group of the message). If the number obtained is one of 120 listed in Appendix 2, the message is a Purple message.

2. Read the paragraph in Chapter II C headed "Special Instructions," for any particular instructions applicable to that period.

3. Turn to Appendix 3A and select the sequence for the date. For sequence YVJNRDMBX . . ., plug number 1 in Y, number 2 in V, and so on for all 26 plugs.

4. From the table of indicators and starting points, select the data which gives the starting point of the sixes, the starting point of the twenties, the selector motion, and the switch setting.[20]

The unsolvable problem had been reduced to a mechanical exercise.

Conclusion

~~(TSC)~~ After the historical study of Red and Purple, the SPICE class analyzed several Purple messages. The description of the solution of a particular message before the analog machine was built sounds straightforward. [redacted]

(1)(1)
(3)-50 USC 403
(3)-18 USC 798
(3)-P.L. 86-36

~~(S-CCO)~~ The class felt that the course on Red and Purple had accomplished its goal. The students had learned how Red and Purple were solved, and had gained some hands-on experience with actual World War II messages. They also felt that

[19] Ibid., p. 2-1A.
[20] Ibid., p. 2-4.

the course on Japanese systems should be offered again but should be expanded to include the Jade and Coral machines.

(C-CCO) More messages have been discovered in the archives. If homogeneous batches of Red, Purple, Jade, and Coral messages could be entered into the data base and given to students along with a historical review of the knowledge of Japanese systems available to analysts in 1936, then another, more valid, effort could be made to solve the systems today.

(b)(3)-P.L. 86-36

(b)(6)

(FOUO) [redacted] a cryptanalyst in the Manual Systems Branch of the Signals and Cryptanalytic Development Division (B631), entered the Agency in September 1979 as a Cryptanalytic Intern. Her intern tours were in G952, B632, B131, A53, G43, and E42. Her previous work experience

REFERENCES

(Available in the Cryptologic Collection, NSA Archives)

Friedman, William. "Preliminary Historical Report on the Solution of the "B" *Machine," 14 October 1940.*

Notes on Japanese Cipher Machines (S-39, 369, 4 January 1939).

Purple and Red, S-119-785, Army A.S.A.

The Purple Course

Purple Notes 1X S-39343

The Red and Purple Story, S-9635 (includes The Japanese Red Machine)

R.I.P. (Registered Intelligence Publication) 6, 15 July 1939.

R.I.P. 77, April 1941.

APPENDIX A

Material from Original Purple Course

The Starting Point of the Sixes

Knowing the sixes but not the starting point, several attacks are possible in determining which of the 25 possible starting points is correct.

A distribution may be made, and since the position of each letter is known, it is only necessary to scratch one or more of the letters in its twenty-five possible starting points to see which gives the best distribution. The assumption may be confirmed by scratches of the other letters for that starting point. This procedure may often be done by inspection.

If a message is not long enough for a distribution, parts of the text having several sixes together may be deciphered in each of the twenty-five possible starting points to see which gives the best decipherment.

If possible guesses for the end or beginning can be made, the starting points can be narrowed to one or two possibilities. This is quite simple if D, B, O, W, or A are in the sixes.

Another possibility is for a certain pattern that would probably exist in the plain text such as the following, assuming the sixes to be X T J L Z R.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Q	T	Q	S	I	D	D	D	D	X	F	C	J	B	B	M	S	F	O	V	D	D	N	O	B	B	F	Y	X

If we now underline the sixes in the message and hunt for this pattern, the starting point of the sixes may be recovered as well as a reliable guess. Suppose the following has been found:

```
CR - - M Z Q V O Y M F G T N P
PN       T             X

CR - - Z B O C Q F V K G I W Y
PN     J

CR - - A P O V J
PN           X
```

Now, by inspecting the wiring diagram of the sixes for the places where the above may be true, the starting point of the sixes is found to be 2 of the first cipher M.

There are other methods of attack possible, and it is hard to say which is best. Each problem is slightly different and demands different considerations. Knowledge of what the message has in it is the best bet to speed up the procedure.

DIRECT

CR		1X	2T	3J	4L	5Z	6R		
PN	1	2	1	3	5	4	6	1	
	2	6	3	5	2	1	4	2	
	3	1	5	4	6	2	3	3	Z = T
	4	4	3	2	1	6	5	4	
	5	3	6	1	4	5	2	5	
	6	2	1	6	5	3	4	6	
	7	6	5	4	2	1	3	7	
	8	3	6	1	4	5	2	8	
	9	5	4	2	6	3	1	9	
	10	4	5	3	2	1	6	10	
	11	2	1	4	5	6	3	11	T = X
	12	5	4	6	3	2	1	12	
	13	3	1	2	6	4	5	13	
	14	4	2	5	1	3	6	14	Z = J
	15	1	6	2	3	5	4	15	
	16	5	4	3	6	1	2	16	
	17	6	2	5	3	4	1	17	
	18	2	3	4	1	5	6	18	
	19	1	2	3	5	6	4	19	
	20	3	1	6	4	2	5	20	
	21	6	5	1	2	4	3	21	
	22	1	3	6	4	2	5	22	
	23	6	4	5	1	3	2	23	
	24	4	5	1	2	5	3	24	
	25	5	2	4	3	6	1	25	
	1	2	1	3	5	4	6	1	
	2	6	3	5	2	1	4	2	
	3	1	5	4	6	2	3	3	
	4	4	3	2	1	6	5	4	
	5	3	6	1	4	5	2	5	J = X

Fig. A1. Worksheet for Recovery of the Sequence of the Sixes

APPENDIX B

On Rotors, Telephone Selectors, and Mushroom Wheels

by [redacted] (b)(3)-P.L. 86-36

(S) The NSA Basic Cryptologic Glossary (1971) defines rotors, mushroom wheels, and telephone selectors as follows:

> (C) **rotor.** 1. A wired wheel that moves in a cipher machine. (A non-moving wheel is called a STATOR.) 2. A wired wheel, typically in the form of a rotatable flat cylinder or drum, having a circle of electrical contacts on each of the opposing faces and one-to-one cross wiring between them.
>
> (C) **mushroom wheel.** A wired wheel, typically in the form of a rotatable cylinder carrying a shorter but wider drum at one end. There are slip rings on the stem of the mushroom wired to spring-loaded contacts set in a circle in the flat head.
>
> (C) **telephone selector wheel.** A wired wheel composed of an assembly of rotary switches such as are used in automatic-dialing telephone systems.

In discussing the Japanese World War II cipher machines, the term rotor technically applies to neither Red nor to Purple. A true rotor is a device for "rotating a permutation." The Japanese Red machine used mushroom wheels which implement the slide of a permutation as in the Viginere family of ciphers. Several mushroom wheels together in a maze can show characteristics of rotors if the motion is identical for stretch of text for adjacent wheels. In the Red machine, the mushroom wheels were stacked. There were some properties similar to a rotor.

(S) The Japanese Purple machine used the telephone selector "wheel," which is capable of being wired for many unrelated permutations limited only by the hardware employed in any one device. These different permutations are selected by the position of the wipers at any one setting of the machine. There is no rotation nor sliding of these permutations.

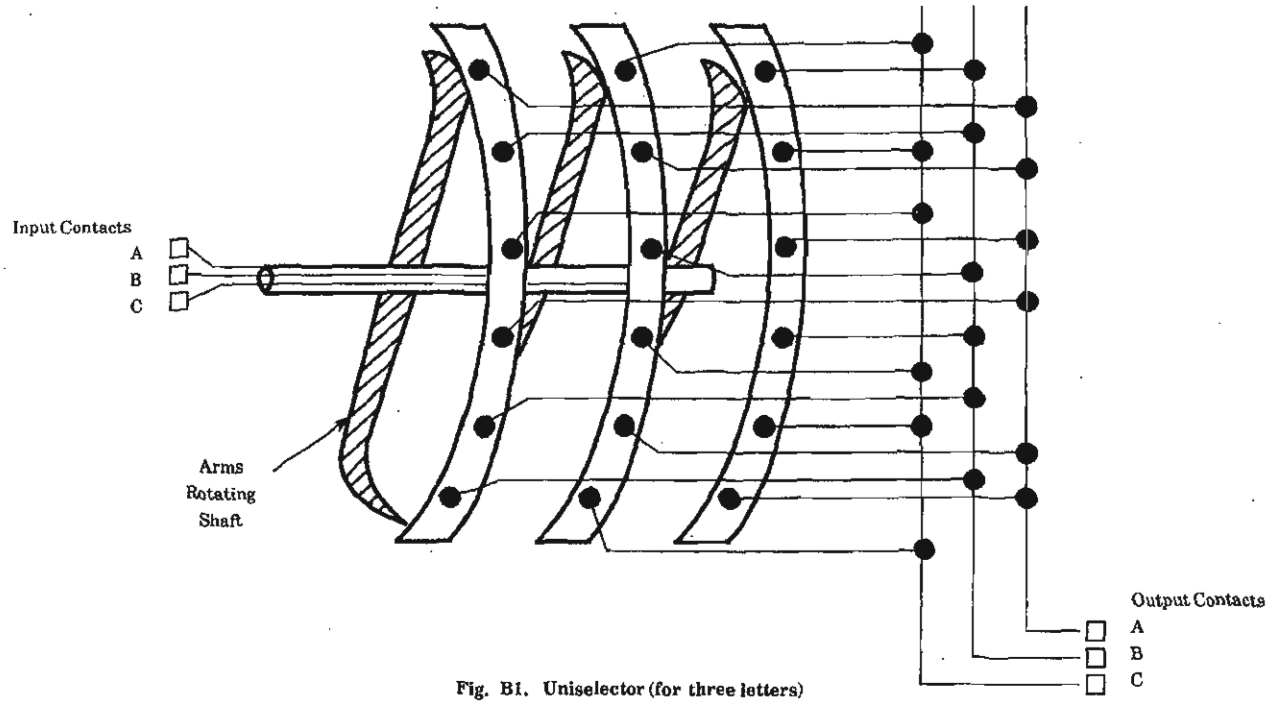

Fig. B1. Uniselector (for three letters)

Actual machine had 26 inputs divided into two sets, one of six and one of twenty.

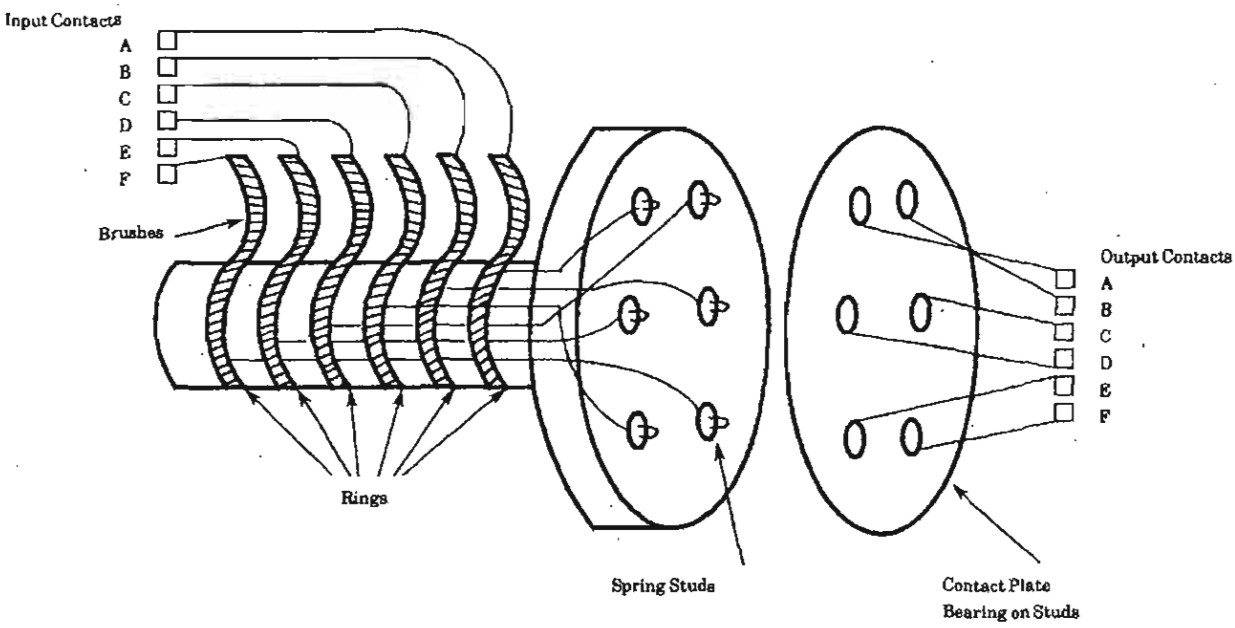

Fig. B2. Half – Hebern Wheel, or Mushroom

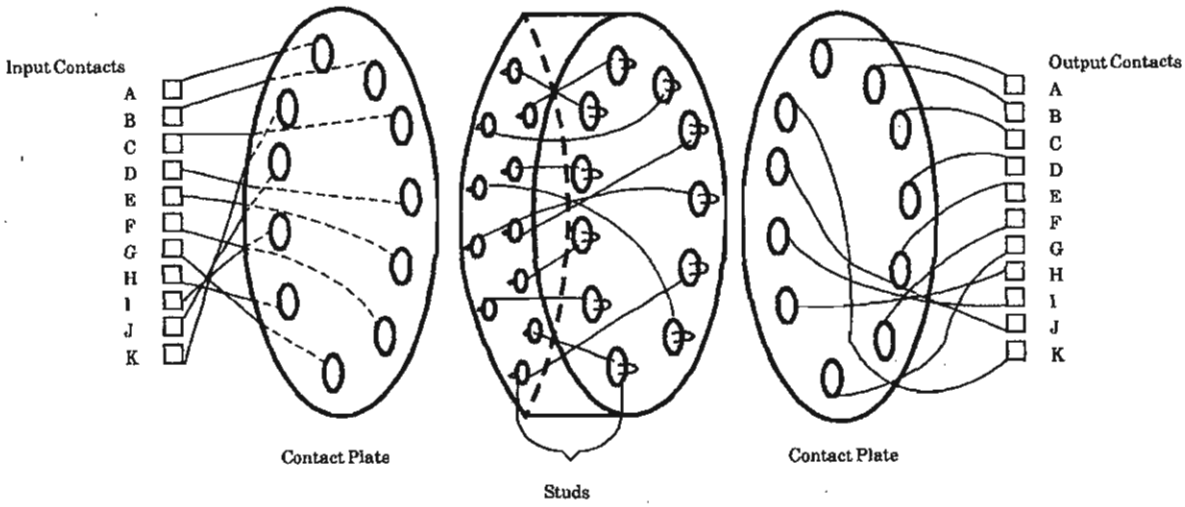

Fig. B3. Full - Hebern Wheel, or Rotor