Rules for PURPLE Machine and JAA-1 Instructions

Source: NARA, College Park, Md., Record Group 457, National Security Agency, Historic Cryptographic Collection, Box 1004, NR 3127

Editor: Frode Weierud, Crypto Cellar Research
Web Site: www.cryptocellar.org

Version: 30 April 2018

November 25, 1943

RULES FOR PURPLE MACHINE FOR PERIOD SEPTEMBER, 1942--******

RULE NUMBER ONE

I. The Sequence

A. Determination of sequence plugged in:

1. Double the number of the month and add the number of the day. This total corresponds to the page of the basic sequence book.

2. On the page thus determined count down from the top the number of lines corresponding to the number of the month. That is, for January, line 1; for February, line 2; for October, line 10. This does not give the sequence but the key letter for finding the line used for deriving the sequence.

3. Using the last letter on the right of this line found as in paragraph 2 above, look down the column of letters on the left, beginning with the letter in the line below the line determined in paragraph 2 above until this letter is found. If this letter sought does not appear on the same page, it will be necessary to continue on subsequent pages until it is found. The line determined by this letter is the one used for deriving the sequence for the keyboard typewriter unit.

4. Counting from the left to right, the letter corresponding to the number of the month is the first letter used. The letters are taken in sequence from left to right, returning to the left edge when the right edge is reached. Therefore, for October, start with the tenth letter--proceed to the twenty-sixth--back to the first, and then to the sixth.

b. "Plugging-in" route.

1	4	8	15	13	23	19	26	11
10	9	8	7	6	5	4	3	2
2	5	10	22	14	25	24	7	9
11	26	25	24	23	22	21	20	1
3	6	20	21	17	18	16	12	
12	13	14	15	16	17	18	19	

6. Operating sequence:

The operating sequence for our machine is obtained from the sequence obtained in A above by inscribing in the manner shown in B and transcribing according to the numerical sequence shown in red. The sequence resulting therefrom is that which is plugged into our cryptograph unit.

Example:

To derive operating sequence for October 4, 1943, proceed as follows:

Key-letter line: Line 10 of page 24 reads:

10-WVEQTPCHJSBIZDYLFGKORXUMA(N)

We look down the left hand column until we find an "N", line 7, page 25. Line 7, page 25, is found to be:

7-(N)YGTWSACORDBPKJZMLEUXFQVHI

Since it is October--the 10th month--we start with the 10th letter which is "R" and write the sequence in the grill following the route indicated in B above.

1	4	8	15	13	23	19	26	11
B	L	M	Z	J	K	P	B	D
2	5	10	22	14	25	24	7	9
U	O	C	A	S	W	T	G	(R)
3	6	20	21	17	18	16	12	
X	F	Q	V	H	I	N	Y	

The following sequence results:

EUXLOF GMRCDYJSZNHIPQVAKTWB

II. The Indicator

With the exception of Rule Number Three, additives have not been applied to the indicator since July 1, 1942.

In Rule Number One any indicator may be used except those composed entirely of the last half of the digits. That is, 0 2 4 6 8, 1 3 5 7 9, or 0 1 2 3 4 may be used. 5 6 7 8 9 may not be used.

III. The Starting Point

The starting point for each indicator will change daily as follows:

a. The number of the month and day are written horizontally separated in digits as, July 12, (7-1-2).

b. These are added respectively to the positions A, B, C, D. If number resulting is over 25, subtract 25 therefrom.

IV. The Motion

The motion is the same as before.

Example: For indicator 4 6 0 2 8 on July 12th.

A	B	C	D	Motion
25	2	3	20	321 (1)
7	1	2		
7 -	3,	5,	20 -	321 (1)

Or translated to our machine:

A	B	C	D	
25	20	3	2	123 (1)
7		2	1	
7	20	5	3	123 (1)

RULE NUMBER TWO
(Red)

This rule is used for more secret messages than ordinary machine traffic.

I. The Sequence

A. Determination of sequence to be plugged in:

1. Find the key row and key letter exactly as in Rule Number One.

2. Using the last letter on the right look down the column of letters on the right hand edge instead of the left hand edge until the letter is found.

3. Counting from right to left, the letter corresponding to the number of the month is the first letter used. The letters are taken in sequence from right to left, returning to the right edge when the left edge is reached. Therefore, for October, start with the 10th letter from the right (the 17th letter from the left) and proceed to the left to the first letter, then back to the 26th letter and left to the 18th. (This is reverse to paragrah 4, Rule Number One.)

B. Plugging-in route:

Same as in Rule Number One.

C. Operating Sequence

Same method as in Rule Number One.

Example:

To derive operating sequence for October 4th, 1943:

Key line--line 4, page 24:
4-ERULMKGTFNSJUBCWZOYDQPAIVX

Looking down right edge until an "X" is found in line 5, page 27:

5-RCLYNVAWGEFBZUHJSPMTDIQKOX

1	4	8	15	13	23	19	26	11
W	G	E	F	B	Z	U	H	J
2	5	10	22	14	25	24	7	9
A	P	M	T	D	I	Q	K	S
3	6	20	21	17	18	16	12	
V	N	Y	L	C	R	X	O	

Thus the operating sequence to be used within our cryptograph is:

WAVGPN KESMJOBDFXCRUYLTZQI

II. The Indicators

Only those indicators will be used which appear in the block from 56789 to 98765.

III. Starting Point

The starting point for the Japanese will be the reverse of their result obtained in Rule Number One. That is, the Japanese order will be DCBA.

Due to the difference of wheel order between the Japanese machine and ours, the normal order of Rule I for our machine (ADCB) must be changed thus:

A D C B , giving DABC as the wheel order for RuleII.

IV. The Motion

The motion will be the same as for Rule Number One.

RULE NUMBER THREE

This rule is used only for especially secret matters and will be used among correspondents in Japan, Germany and Italy, with the following revision to Rule Number Two.

I. Indicators

A. In this rule additives will be used to disguise the basic indicators. In the list of additives:

12123	03102	21215	82313
30108	50525	50922	03210
90142	08083	12213	20300
21902	32321	90029	01230
50092	04140	18112	91008

"Yama" (12123) was used as additive for January: and the other additives were used in the indicator order for the succeeding months. Thus the additive for December, 1942, was "Kumo" (50922), and that for January, 1943, was "Shimo" (91008). In the summer months of 1943 no regular order seems to have been followed.

B. Any indicator may be used.

II. Starting Points

Starting points will be changed each day as in Rule Number One.

HIKALS

I. The Sequence

A. Sequence to be plugged in:

1. Find the key row for the day as in Rule Number One.

2. The line for deriving the sequence is obtained by counting down eight from the key line. That is, July 4--page 11, line 15; July 5--page 12, line 15; August 5--page 13, line 16.

3. The sequence is plugged in as indicated in paragraph A 4, Rule Number One.

B. Route of plugging.

The letters G A N Z I R O W of the Japanese typewriter plugboard are plugged in first and then the route of Rule Number One is followed.

(1)	(4)	(8)	(15)	(13)	(23)	(19)	(26)	(11)
A	O	B	F	J	M	Q	T	X
X	X							
(2)	(5)	(10)	(22)	(14)	(25)	(24)	(7)	(9)
E	U	C	G	K	N	R	V	Z
			X		X	X		X
(3)	(6)	(20)	(21)	(17)	(18)	(16)	(12)	
I	Y	D	H	L	P	S	W	
X							X	

C. Operating Sequence

Using the line obtained in Paragraph A2 above and starting with the letter corresponding to the month as in A3 above, inscribe the letters on the Japanese typewriter plugboard as indicated and transcribe the letters in the numberical order given on Japanese cryptograph unit.

Example:

To derive the operating sequence for July 4, 1942:

Key line--line 7, page 11:

7. -

Counting down eight lines from this:

15. DXGANOKYEVLWQBZIUCFMTSHRJP

(1)	(4)	(8)	(15)	(13)	(23)	(19)	(26)	(11)
(A)	(O)	B	F	J	M	Q	T	X
Y	Q	T	M	F	C	U	I	Z
(2)	(5)	(10)	(22)	(14)	(25)	(24)	(7)	(9)
E	U	C	(G)	L	(N)	(R)	V	(Z)
S	O	N	K	A	E	W	G	V
(3)	(6)	(20)	(21)	(17)	(18)	(16)	(12)	
(I)	Y	D	H	L	P	S	(W)	
L	H	R	J	P	D	X	B	

Accordingly the operating sequence to be used with our cryptograph unit is:

Y S L Q O H G T V N Z B F A M X P D U R J K C W E I

II. The Indicator

Any indicator may be used.

III. The Starting Point

The starting positions are the same as for Rule Number One.

JAA-1 INSTRUCTIONS

On Sunday 10 September 1944, three messages, in what looked like a new system, were received on the TOK-MSC circuit. On 12 September a service message from TOK-MSC dated the 9th September was read. This service message referred to these three messages as machine wires. A JAA type of frequency distribution was immediately made on the three messages and it was found that they were regular JAA machine cipher using a different method of obtaining the daily sequence and the starting points. These three messages were solved and read, but the method used by the Japanese to derive the daily sequence and the starting points was not known. Due to this several short messages which had been received in this new system but on different days could not be read.

Sunday afternoon the 17th September more long messages in this new system were received. While working on these messages Sunday evening, Captain Marston, who had come in to help, was studying the basic sequence book and discovered how the daily sequence was derived and along with this discovery the method of deriving the starting points was obtained. Because of this solution all messages in the new system can now be read as soon as the messages are received provided, of course, that the basic lines are in the basic sequence book.

The trigraph which has been assigned to this new method of usingthe JAA cipher machine is JAA-1.

A description of the new method of getting the daily sequence and starting points follows:

1. The page and line used to derive the daily sequence is found thus: To get the page the number 16 is added to the cryptographic date of the message. The line used on this page corresponds to the number of the month. For example: Find the line used for the daily sequence for the 17th September. 16 + 17 = 33 equals the page and the line is line number 9.

The daily sequence is derived from line 9 by using line ten as the plugging in route. The following series of letters being used for this: UOYAEIXFNMZPSCRKTVWQDHLGJB. Using the line found above and line ten directly below it find the letter U in line ten and take the letter directly above it in line 9 as the first letter in the sequence, "I" in this case. Doing the same with O the letter "C" is obtained as the second letter in the sequence. By doing this for the entire series of 26 letters the following sequence is obtained: ICBHDRKAXJSEPLUWZNGYTFOQMV. This is the sequence used for all JAA-1 messages on the 17th September.

The starting points are obtained by converting the sequence line(line 9 in this case) to the letters as they would appear in the

Japanese sequence book. The numerical position of the letters in this sequence correspond to the starting points as designated in the letter indicator. Line 9 page 33 in the Japanese book would be: TAUEJSKFGDP MVWRHBYNXLQZCOI. To obtain the above line, the following moncalphabetic sequence must be applied to the basic line in our book.

JAP.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
OUR BOOK	U	F	M	Q	O	R	H	D	Y	S	C	T	L	J	A	V	W	G	K	B	E	X	P	Z	I	N

All the starting points for that day may now be obtained from the letter indicators as follows: first the Japanese sequence is numbered 1 thru 26.

T	A	U	E	J	S	K	F	G	D	P	M	V	W	R	H	B	Y	N	X	L	Q	Z	C	O	I
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

Now using the indicator THOPD the following starting points may be obtained:

T = 1 = starting point of the sixes
H = 16 = starting point of our 3 wheel; Jap 1 wheel
O = 25 = starting point of 2 wheel
P = 11 = starting point of our 1 wheel; Jap 3 wheel.
D governs the motion. Just how is not yet known.

JAA-1 traffic may be identified as follows:

1. It should be used so far as we know, only on the TOK-MSC, MSC-TOK diplomatic circuits.

2. There is a five letter indicator which is repeated at the end of the message.

3. The first group following the indicator is a number group. The number should fit in either the TOK-MSC or MSC-TOK series.

4. The cipher text is the same as JAA and a JAA frequency distribution will cause the special characteristics of the machine to stand out.

An example follows:

RTZ DE JNU3 13475KCS S3R3 09SE1738 US4/02974

169 SCDE TOK 73 W 0515S RED JG

KOSHI MCW

DAIQU ZCVHY ZCRAU NPLYO FBKMQ EYCQU WRXHB HIGXL XLJWY XCBMN

XEHEX IEHFD LNQSA NEMMM TTULR EQIHZ ZGVVU USNVV DXMEB ONLDX

DEBCS AFJNS MVUAO UASEY ZLXPP CRNOQ GXIYP NQVAP ECJOC EKYOB

CNUKK ISGGP JKAJJ ZCCXZ IUKNE FEHIZ PFYUV QTXBF QDLGO XDMJL

VGCCM DFOIK ZVXXX GRUUE QSIPC XPCED JIIKC XECFL

P2/169 KOS 238

GVJSA FSDUF HZHQD PCYGX LHIBO KRNZP JSZBM ZYPYY FRISX GCGXP

SWFKW LEEAC QNCVV XPCDY MDONE YTIWQ OJQYX XXWUT ALHON CJYIF

FKWMC ZCVHY

SHIGEMITSU

JAA-1 JAPANESE

The trigraph JAA-1 has been assigned to a new type of Japanese Diplomatic traffic between Tokyo and Moscow. Messages closely resemble the regular JAA in appearance except that the number group in the beginning does not appear. Instead, there is a five-letter indicator which is repeated at the end of the message. This traffic may be expected to appear on another circuits in the future.