REF ID:A56974

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS.

1 NAME OR TITLE S/ASST	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		COORDINATION
2		✓	FILE
		✓	INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE
REMARKS			

FROM NAME OR TITLE NSA-314	DATE 19 Aug
ORGANIZATION AND LOCATION	TELEPHONE 60391

DD FORM 1 FEB 50 94 REPLACES NME FORM 94, 1 FEB 49, WHICH MAY BE USED. 16—56968-2 GPO

PLAIN TEXT RADIATION STUDY OF TSEC/KL-7

(AFSAM 7)

GENERAL

The TSEC/KL-7 is a literal cipher machine designed for off-line use. It can encipher or decipher at any speed up to 60 words per minute and can be operated by either keyboard or punched tape input. The enciphered and deciphered text is printed on gummed paper tape.

The print wheel on the TSEC/KL-7 rotates continously, therefore it employs the "print-on-the fly" method. The print hammer is activated by the print magnet. The objective of this analysis was to determine what information could be obtained from the radiated signal from the print magnet. Mr. Collins, NSA311, has indicated that the print-magnet signal is detectable approximately 25 feet from the equipment. For this analysis the signal was picked up from a direct connection to the print magnet.

The print wheel is directly connected to the motor and any variation in motor speed causes a corresponding change in the speed of the print wheel. A second objective was to determine the variation in the motor speed for a given message, the primary cause of this variation, and how the shunt wound motor, now used on TSEC/KL-7, compared with a governed motor in respect to these features.

ANALYSIS

Tape input was employed for the analysis. The information to be analyzed (plain text) was punched on tape and this tape was enciphered through the machine, printing the cipher text on gummed paper tape.

TOP SECRET

This cipher text was then used to punch a second tape which was deciphered through the machine. It is during this deciphering operation that plain-text radiation from the print magnet is present. This plain-text signal, along with a one kc (kilocycle) sine wave, was filmed from a dual beam scope. The number of cycles of the one kc signal was counted, determining the time interval between consecutive print-outs.

For the initial analysis a typical military message of approximately 70 characters was filmed. The intervals between print-out were recorded, Figure I. The speed of the print wheel, given in the maintenance manual for TSEC/KL-7, is 2200 rpm. The time per revolution of the print wheel is 27.27 ms (milliseconds). Since there are 38 characters on the periphery of the print wheel, 0.7177 ms are required for each character to pass the print hammer.

The interval readings were reduced modulo 27.27, the time for one revolution, leaving a residue which is the number of milliseconds past the previous character printed. These time intervals were converted to the corresponding number of characters by dividing by 0.7177. At this point, given the print-wheel sequence (Figure 3) and the first character of the message, theoretically the entire message could be read without any difficulty; but because of variation in the speed of the print wheel, the number of characters from the film residue vary from the actual number as given by the message.

Mrs. Esther Cox, NSA-314, analyzed this data by assuming possible words and trying to fit them to the sequence of residues. After several

hours she was unable to recover any portion of the message. Further study was made on this message by comparing the calculated residue with the film residue; this was done by subtracting the film residue from the calculated residue, Figure I. (The calculated residue is determined by multiplying the time per character by the interval on the print wheel for successive pairs of characters of the message.) This difference showed an average bias of 2.163 ms, or approximately three characters. When this bias was removed by adding - 2.163 ms to each film residue, Mrs. Cox was still unable to recover the plain text after three hours. In order to speed up the analysis, because of Mrs. Cox's resignation, she was given three probable words, one of which was contained in the message. In a short time she recovered the remainder of the message.

A second set of films was run to obtain information about the variation in motor speed. Two different motors were used, the shunt wound motor now used on the TEC/KL-7, and a governed motor. Two pairs of films were run, that is, the same material was deciphered using each motor; these pairs were compared. The pairs were (1) decipherment of all spaces, and (2) decipherment of a message. Over the operating range 21 to 31 volts the shunt wound motor speed could vary to the extent that it caused the print wheel to be in an improper position when the print hammer would strike, thus producing unclear or improper print-outs. The use of a governed motor would be a solution to this problem, if it did not seriously effect the security of the

equipment. With this in mind further analysis was carried out, and is included in the remainder of this report.

In the comparison of the first pair of messages (all spaces) the objective was to determine variations in motor speed. The decipherment of enciphered spaces was used so that the print wheel would make an integral number of revolutions between print-outs; therefore the only difference in time between prints would be due to variation in motor speed. The analysis of the shunt wound motor indicates the average time between print-outs is 185.2 ms, with a range from 182.0 ms. to 188.0 ms. This is a variation of approximately 4 1/2 characters from the mean. The 185.2 ms represents 7 revolutions, or 26.46 ms per revolution, which gives an average print-wheel speed of 2269 rpm, whereas the maintenance manual indicates 2200 rpm. If at the beginning of a message several repetitions of one character (say space) were enciphered; this, when deciphered, would be valuable in calculating the print-wheel speed, which would be a much closer approximation than the speed given in the manual, thus improving the analysis.

Using the governed motor the average time between print-outs was 190.0 ms, with range from 189.5 ms to 190.5 ms. This is a variation of less than one character from the mean. Actually this variation may be less since part of it could be caused by the fact that it was difficult to read the film more accurately than 0.5 ms.

A second message was filmed when the TSEC/KL-7 was operated by the shunt would motor. The data is recorded in Figure 2. It may be

TOP SECRET

observed that the first 21 readings are either approximately 188 ms or approximately 214 ms, indicating that the same character had been deciphered, and the print wheel made respectively 7 or 8 revolutions. (188 ms corresponds approximately to 7 revolutions of the print wheel where the 2200 rpm speed given by the manual is used.) These first 21 readings were averaged and the print-wheel speed was calculated to be 2239 rpm, resulting in 26.81 ms per revolution and 0.7053 ms per character.

Analysis of this message was done by Miss Teresa Mimeau, NSA-314. The solution method was based on the theory that, if all the intervals between print-outs had been the true distance between plain letters, the plain text could be recovered in the following way.

Consider the print wheel in terms of the location of its letters (Figure 3). Then, given the successive intervals (i_1, i_2, i_3, ..., i_n where n is the number of letters in the message) between printed characters, which is the film residue in number of characters in Figure 2, choose an arbitrary location on the print wheel for the logical first letter of the message (say at position $\emptyset$, which is a "space"). Derive the numerical sequence composed of partial sums i_1, $i_1 + i_2$, $i_1 + i_2 + i_3$, ..., $i_1 + i_2 + ... + i_n$ (mod 38). This sequence will represent the locations, each varying by a constant, reflecting the distance from the chosen first letter to the true one, on the print wheel, of corresponding letters of plain text. Convert that sequence to the corresponding literal values from the known print wheel, mixed alphabet. That stream becomes the "pseudo-plain text." Let that "plain"

be the first row of a matrix 38 cells deep. Each succeeding row will be a slide of one from the preceeding sequence, where the first letter of each row is assumed to have been one letter beyond that of the row above, for all possible 38 first letter assumptions. In other words, each column becomes an inscription of the print-wheel alphabet, beginning with the letter designated in row one and continuing cyclically to row 38. The row beginning with the correct first letter will then contain the actual plain text, assuming that the original intervals were exact, that is there was no variation in speed of the print wheel.

In actuality, it was necessary to contend with a degree of variance which required making up the full matrix and scanning all its rows for portions which were words, or resembled part-words. Once such a segment was located, attempts were made to extend horizontally the portion in both directions, by considering the adjacent columns as possibly displaced a few positions up or down, i.e. searching for good text continuing in the rows nearby. From previous analysis it was found that a jump of five rows was possible, but several jumps of five, or jumps greater than five appeared to be unreasonable. Several apparent possibilities extended for a stretch but had to be discarded when unreasonable "jumps" (errors in computed intervals) made continuance unfeasible. When the correct text was hit upon it could be extended the entire width of the matrix without having to jump too many rows between any two columns. Approximately 30 hours were required to complete the entire analysis of this message.

TOP SECRET

Figure 4 lists the date from a filmed message where the governed motor was used on the TSEC/KL-7. This message was also analyzed by Miss Mimeau, using the same method as previously indicated. An approximation for the print-wheel speed was obtained from previous data, where the decipherment of "all spaces" was filmed using this same motor; the print-wheel speed was 2217rpm, or 27.06 ms per revolution and 0.7122 ms per character. Notice in Figure 5 how closely the film residue and calculated residue agree. As a result, when the first few columns of the matrix were written out, it was obvious which row contained the message.

Since the variation was small, it was only necessary to write out several rows above and below the row that theoretically contained the messages. The complete analysis for this message required two hours.

Up to this point it has been determined that the speed of the governed motor is constant enough to enable easy reading of a message, whereas the shunt wound motor has greater variation in speed, making analysis more difficult.

It was suspected that the variation in motor speed was a function of the number of rotors that stepped. To verify this the message indicator was set up on the machine, and each successive setting was recorded; from this the motion for each decipherment was determined, giving the number of rotors stepping for each encipherment. This sequence of numbers was properly aligned with the variations (calculated residue minus film residue, Figure 2), and it may be observed that there is high correlation between the number of rotors that step and the

TOP SECRET

print-wheel speed; that is, when the maximum number of rotors step there is a large negative deviation from the mean in print-wheel speed, and when the minimum number of rotors step the deviation from the mean speed is positive. It may be possible, with more precise recording and measuring devices, to get accurate information on the number of rotors that step.

For this analysis tape input was used, thus making the time intervals between print-outs relatively constant; that is, the print wheel would make 6 or 7 revolutions plus the distance it had to go from the previous character printed to the next one to be printed. If keyboard operation were employed, the number of revolutions of the print wheel would vary a great deal, due to the irregularity in typing speed of the operation. This would cause the variation in print-wheel speed to have more influence, adding to the difficulty of the analysis.

CONCLUSION

The print magnet on the TSEC/KL-7 radiates a signal which is detectable approximately 25 feet from the equipment. During the deciphering operation the signal indicates the plain text that is being printed on the gummed paper tape. Analysis of this signal, recorded during decipherment, showed that the plain text could be recovered. When the shunt wound motor was used on the equipment approximately 30 hours were required to recover the plain text by hand methods. When a governed motor was used only 2 hours were required to recover plain text because of the regularity of the print-wheel speed.

Mr. Joseph Collins, NSA-311, indicated that available through radiation, and detectable at the same distance as the print-magnet signal, is information that would enable us to determine the change in print-wheel speed between print-outs. With this information available the analysis would be trivial.

It has been determined that there is a high correlation between the number of rotors stepping and the variation in the speed of the print wheel.

Messages deciphered by keyboard input rather than punched tape, used in the previous analysis, would be more difficult to analyse due to longer intervals between characters allowing more accumulated variation in the print-wheel speed.

TOP SECRET RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE SHUNT WOUND MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F
Text of Message	Character Intervals on Print Wheel	Film Readings (ms)	Film Residue (ms)	Calculated Residues (ms)	Column E Minus Column D
T	17	204.5	10.8	12.4	- 1.6
H	7	174.5	8.5	5.1	- 3.4
R	25	210.0	16.3	18.2	1.9
E	36	193.0	27.0	26.2	- 0.8
E	0	194.0	0.3	0	- 0.3
	29	188.0	22.0	21.1	- 0.9
P	2	197.5	3.8	1.5	- 2.3
L	31	192.0	26.0	22.6	- 3.4
A	30	192.0	26.0	21.8	- 4.2
N	4	172.5	6.5	2.9	- 3.6
E	18	205.0	11.3	13.1	1.8
S	18	206.0	12.3	13.1	0.8
	11	178.5	12.5	8.0	- 4.5
S	27	190.0	24.0	19.7	- 4.3
I	21	185.5	19.5	15.3	- 4.2
G	16	205.5	11.8	11.7	- 0.1
H	36	195.0	1.3	26.2	- 2.8
T	31	192.0	26.0	22.6	- 3.4
E	30	191.0	25.0	21.8	- 3.2
D	21	183.5	17.5	15.3	- 2.2
	8	199.0	5.3	5.8	0.5
F	28	189.0	23.0	20.4	- 2.6
L	5	199.0	5.3	3.6	- 1.7
Y	23	187.0	21.0	16.8	- 4.2
I	30	192.0	26.0	21.8	- 4.2
N	19	208.5	14.8	13.8	- 1.0
G	35	169.0	3.0	25.5	- 5.2
	12	204.0	10.3	8.7	- 1.6
L	33	193.0	27.0	24.0	- 3.0
O	9	201.5	7.8	6.6	- 1.2
W	37	170.0	4.0	26.9	- 4.8
	35	219.0	25.3	25.5	0.2
O	4	175.0	9.0	2.9	- 6.1
V	32	190.0	24.0	23.3	- 0.7
E	11	201.5	7.8	8.0	0.2
R	2	196.0	2.3	1.5	- 0.8

LIBRARY NO. S60,081

Figure 1.

(Continued on page 11)

~~TOP SECRET~~ RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE SHUNT WOUND MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F
Text of Message	Character Intervals on Print Wheel	Film Readings (ms)	Film Residue (ms)	Calculated Residues (ms)	Column E Minus Column
	27	188.0	22.0	19.7	- 2.3
B	34	195.0	1.3	24.8	- 4.2
A	29	190.0	24.0	21.1	- 2.9
Y	31	190.0	24.0	22.6	- 1.4
	20	183.0	17.0	14.6	- 2.4
S	27	213.0	19.3	19.7	0.4
T	28	188.0	22.0	20.4	- 1.6
O	25	187.0	21.0	18.2	- 2.8
P	36	194.0	0.3	26.2	- 1.8
	36	194.0	0.3	26.2	- 1.8
P	2	198.0	4.3	1.5	- 2.8
R	9	177.0	11.0	6.6	- 4.4
E	36	194.0	0.3	26.2	- 1.8
S	18	206.0	12.3	13.1	0.8
U	23	184.5	18.5	16.8	- 1.7
M	19	184.0	18.0	13.8	- 4.2
A	32	193.0	27.0	23.3	- 3.7
B	9	203.5	9.8	6.6	- 3.2
L	37	195.5	1.8	26.9	- 2.2
Y	23	185.5	19.5	16.8	- 2.7
	20	183.5	17.5	14.6	- 2.9
					- 123.3 = Total bias

Figure 1.

Motor speed assumed = 2200 rpm

27.67 ms per revolution of print-wheel

0.728 ms per character

6 revolutions of print wheel = 166.0 ms

7 revolutions of print wheel = 193.7 ms

8 revolutions of print wheel = 221.3 ms

$\frac{-123.3}{57}$ = - 2.163 ms average bias per letter of message.

$\frac{2.163}{0.728}$ = 2.97 characters, average bias per letter of message.

~~TOP SECRET~~ CONTROL NUMBER B/055 1147
COPY 19 OF 25 COPIES 20
PAGE 4 OF 20 PAGES
LIBRARY NO 560,081

~~TOP SECRET~~ RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE SHUNT WOUND MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F	G	H
Intervals	Film Readings (ms)	Film Residue (ms)	Film Residue (Number of Characters)	MESSAGE	Actual Residue (Number of Characters)	Column F Minus Column D	Number of Rotors Stepping
1	214.0	26.4	37		0	1	3
2	188.0	0.4	1		0	- 1	5
3	188.5	0.9	1		0	- 1	5
4	188.5	0.9	1		0	- 1	5
5	189.5	1.9	3		0	- 3	5
6	189.5	1.9	3		0	- 3	6
7	213.5	25.9	37		0	1	3
8	186.0	25.2	36		0	2	3
9	187.0	26.2	37		0	1	5
10	186.5	25.7	36		0	2	3
11	213.0	25.4	36		0	2	4
12	185.5	24.7	35		0	3	3
13	186.5	25.7	36		0	2	4
14	188.0	0.4	1		0	- 1	5
15	188.5	0.9	1		0	- 1	5
16	215.0	0.6	1		0	- 1	5
17	186.0	25.2	36		0	2	3
18	187.0	26.2	37		0	1	4
19	187.5	26.7	0		0	0	4
20	189.5	1.9	3		0	- 3	6
21	217.0	2.6	4		0	- 4	5
22	176.0	15.2	22	T	17	- 5	6
23	193.0	5.4	8	H	7	- 1	3
24	205.5	17.9	25	E	23	- 2	5
25	182.5	21.7	31		29	- 2	6
26	207.5	19.9	28	A	25	- 3	5
27	192.5	4.9	7	L	8	1	3
28	186.5	25.7	36	L	0	2	4
29	197.5	9.9	14	I	15	1	4
30	187.5	26.7	38	E	37	- 1	5
31	175.5	14.7	21	S	18	- 3	6
32	197.0	9.4	13		11	- 2	5
33	207.5	19.9	28	A	25	- 3	5
34	177.0	16.2	23	R	24	1	4
35	188.0	0.4	1	E	36	- 3	6

Figure 2.

(Continued on page 13)

~~TOP SECRET~~ RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE SHUNT WOUND MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F	G	H
Intervals	Film Readings (ms)	Film Residue (ms)	Film Residue (Number of Characters)	MESSAGE	Actual Residue (Number of Characters)	Column F Minus Column D	Number of Rotors Stepping
36	208.0	20.4	29		29	0	4
37	200.5	12.9	18	T	17	- 1	5
38	178.5	17.7	25	O	25	0	4
39	186.0	25.2	36		34	- 2	6
40	198.5	10.9	15	R	11	- 4	6
41	185.5	24.7	35	E	36	1	3
42	200.0	12.4	18	F	19	1	4
43	201.5	13.9	20	R	21	1	4
44	198.0	10.4	15	A	14	- 1	5
45	179.0	18.2	26	I	23	- 3	6
46	202.0	14.4	20	N	19	- 1	5
47	192.5	4.9	7		9	2	3
48	182.5	21.7	31	F	28	- 3	6
49	202.5	14.9	21	R	21	0	4
50	182.0	21.2	30	O	31	1	4
51	205.0	17.4	25	M	27	2	4
52	190.0	2.4	3		7	4	3
53	182.5	21.7	31	D	30	- 1	5
54	200.0	12.4	18	E	17	- 1	5
55	202.5	14.9	21	M	22	1	4
56	183.0	22.2	32	A	32	0	5
57	189.5	1.9	3	N	4	1	4
58	187.0	26.2	37	D	1	2	4
59	212.0	24.4	35	S	35	0	5
60	195.5	7.9	11		11	0	6
61	193.0	5.4	8	O	4	- 4	6
62	193.5	5.9	8	R	7	- 1	5
63	178.5	17.7	25		27	2	4
64	205.0	17.4	25	A	25	0	4
65	192.0	4.4	6	C	7	1	5
66	176.5	15.7	22	T	23	1	4
67	209.5	21.7	31	I	31	0	6
68	180.5	19.7	28	O	32	4	3
69	202.0	14.4	20	N	25	5	3
70	185.5	24.7	35	S	36	1	6

Figure 2.

LIBRARY NO. S60,081

(Continued on page 14)

~~TOP SECRET~~ RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE SHUNT WOUND MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F	G	H
Intervals	Film Readings (ms)	Film Residue (ms)	Film Residue (Number of Characters)	MESSAGE	Actual Residue (Number of Characters)	Column F Minus Column D	Number of Rotors Stepping
71	192.0	4.4	6		11	5	3
72	188.5	0.9	1	W	3	2	4
73	201.5	13.9	20	H	21	1	5
74	177.5	16.7	24	I	24	0	6
75	202.0	14.4	20	C	22	2	4
76	208.0	20.4	29	H	30	1	5
77	171.0	10.2	15		14	-1	
78	218.5	4.1	6	W	3	-3	
79	188.5	0.9	1	O	1	0	
80	191.0	3.4	5	U	8	3	
81	175.5	14.7	21	L	21	0	
82	212.0	24.4	35	D	35	0	
83	192.5	4.9	7		8	1	
84	184.5	23.7	34	M	31	-3	
85	184.5	23.7	34	A	32	-2	
86	209.0	21.4	30	K	33	3	
87	179.5	18.7	27	E	27	0	
88	206.0	18.4	26		29	3	
89	193.0	5.4	8	I	10	2	
90	190.5	2.9	4	T	7	3	
91	173.0	12.2	17		21	4	
92	195.0	7.4	10	I	10	0	
93	202.5	14.9	21	M	21	0	
94	193.5	5.9	8	P	9	1	
95	189.5	1.9	3	O	2	-1	
96	203.0	15.4	22	S	23	1	
97	185.0	24.2	34	S	38	4	
98	201.0	13.4	19	I	21	2	
99	176.0	15.2	22	B	24	2	
100	211.5	23.9	34	L	37	3	
101	197.5	9.9	14	E	14	0	
102	181.0	20.2	29		29	0	
103	180.0	19.2	27	F	28	-1	
104	196.0	8.2	12	O	14	2	
105	191.0	3.4	5	R	7	2	

Figure 2.

(Continued on page 15)

~~TOP SECRET~~ RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE SHUNT WOUND MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F	G	H
Intervals	Film Readings (ms)	Film Residue (ms)	Film Residue (Number of Characters)	MESSAGE	Actual Residue (Number of Characters)	Column F Minus Column D	Number of Rotors Stepping
106	205.0	17.4	25		27	2	
107	200.5	12.9	18	T	17	- 1	
108	192.0	4.4	6	H	7	1	
109	175.5	14.7	21	E	23	2	
110	204.0	16.4	23		29	6	
111	198.5	10.9	15	K	20	5	
112	174.0	13.2	19	O	22	3	
113	218.0	3.6	5	R	7	2	
114	184.0	23.2	33	E	36	3	
115	195.0	7.4	10	A	16	6	
116	187.5	26.7	38	N	4	4	
117	183.0	22.2	31	S	36	5	
118	192.0	4.4	6		11	5	
119	200.0	12.4	18	T	17	- 1	
120	202.5	14.9	21	O	25	4	
121	181.5	20.7	29		34	5	
122	204.0	16.4	23	H	24	1	
123	200.0	12.4	18	O	18	0	
124	180.0	19.2	27	L	29	2	
125	188.0	0.4	1	D	35	- 4	
126	190.5	2.9	4		8	4	
127	216.0	1.6	2	O	4	2	
128	176.5	15.7	22	F	24	2	
129	188.5	0.9	1	F	38	- 1	
130	194.0	6.4	9		10	1	
131	199.0	11.4	16	T	17	1	
132	192.5	4.9	7	H	7	0	
133	201.5	13.9	20	E	23	3	
134	178.5	17.7	25		29	4	
135	209.0	21.4	30	C	32	2	
136	193.0	5.4	8	O	10	2	
137	179.0	18.2	26	M	27	1	
138	187.5	26.7	38	M	38	0	
139	200.0	12.4	18	I	17	- 1	
140	186.5	25.7	36	E	37	1	
						93 Total bias	

Figure 2.

(Continued on page 16) LIBRARY NO. 560,081

TOP SECRET Figure 2. (Continued from page 15)

Motor speed calculated from first 21 entries in column A = 2239 rpm

26.81 ms per revolution of print-wheel

0.7053 ms per character

6 revolutions of print wheel = 160.8 ms

7 revolutions of print wheel = 187.6 ms

8 revolutions of print wheel = 214.4 ms

$\frac{93}{140}$ = 0.664 character, average bias per letter of message.

TOP SECRET

Letter Location	ø	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Print Wheel Sequence	-	Q	P	W	O	1	ø	2	9	E	I	R	U	3	8	4	7	T	Y

Letter Location	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
Print Wheel Sequence	Z	K	5	6	X	H	A	G	S	F	N	D	M	C	L	B	J	V	-

Arbitary Character Location for Print Wheel Sequence.

Figure 3.

TOP SECRET CONTROL NUMBER RIDS5-1147
COPY 19 OF 35 COPIES 48
PAGE 17 OF 20 PAGES

LIBRARY NO. S60,081

~~TOP SECRET~~ RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE. THE GOVERNED MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F	G
Intervals	Film Readings (ms)	Film Residue (ms)	Calculated Residue (ms)	Print Wheel Intervals	MESSAGE	Column D Minus Column C
1	198.5	9.1	10.7	15	G	1.6
2	174.0	11.6	11.4	16	O	- 0.2
3	213.0	23.6	24.2	34		0.6
4	191.5	2.1	1.4	2	P	- 0.7
5	196.0	6.6	6.4	9	R	- 0.2
6	184.5	22.1	22.1	31	O	0
7	182.5	20.1	19.9	28	C	- 0.2
8	200.0	10.6	10.7	15	E	0.1
9	189.5	0.1	0	ø	E	- 0.1
10	204.5	14.1	15.0	21	D	0.9
11	175.0	12.6	12.8	18	I	0.2
12	202.0	12.6	13.5	19	N	- 0.1
13	187.0	24.6	24.9	35	G	0.3
14	197.5	8.1	8.5	12	-	0.4
15	185.0	22.6	22.1	31	M	- 0.5
16	212.5	23.1	22.8	32	A	- 0.3
17	179.0	16.6	16.4	23	I	- 0.2
18	203.0	13.6	13.5	19	N	- 0.1
19	192.5	3.1	2.8	4	L	- 0.3
20	184.0	21.6	21.4	30	A	- 0.2
21	193.0	3.6	2.8	4	N	- 0.8
22	190.5	1.1	0.7	1	D	- 0.4
23	195.0	5.6	5.7	8	-	0.1
24	191.5	2.1	1.4	2	P	- 0.7
25	183.0	20.6	19.9	28	D	- 0.7
26	222.0	5.5	5.7	8	-	0.2
27	181.0	18.6	17.8	25	A	- 0.8
28	195.0	5.6	5.7	8	L	0.1
29	189.5	0.1	0	0	L	- 0.1
30	192.5	3.1	3.6	5	-	0.5
31	197.0	7.6	6.4	9	E	- 1.2
32	184.0	21.6	21.4	30	Q	- 0.2
33	197.5	8.1	7.8	11	U	- 0.3
34	188.0	25.6	25.6	36	I	0
35	211.0	21.6	21.4	30	P	- 0.2

~~TOP SECRET~~ CONTROL NUMBER C/D55-1147
COPY 19 OF ~~35~~ 25 COPIES
PAGE 18 OF 20 PAGES

Figure 4.

(Continued on page 19)

TOP SECRET RECORDED DATA AND CALCULATIONS FROM FILM OF DECIPHERED MESSAGE.
THE GOVERNED MOTOR WAS USED ON THE EQUIPMENT.

A	B	C	D	E	F	G
Intervals	Film Readings (ms)	Film Residue (ms)	Calculated Residue (ms)	Print Wheel Intervals	MESSAGE	Column D Minus Column C
36	183.5	21.1	20.7	29	M	- 0.4
37	201.0	11.6	11.4	16	E	- 0.2
38	177.0	14.6	14.2	20	N	- 0.4
39	208.0	18.6	18.5	26	T	- 0.1
40	204.0	14.6	15.0	21	-	0.4
41	186.0	23.6	22.8	32	C	- 0.8
42	184.0	21.6	21.4	30	H	- 0.2
43	179.0	16.6	16.4	23	E	- 0.2
44	206.0	16.6	16.4	23	C	- 0.2
45	181.0	18.6	18.5	26	K	- 0.1
46	210.0	20.6	19.2	27	E	- 1.4
47	177.5	15.1	15.0	21	D	- 0.1
48	194.5	5.1	5.7	8	-	0.6
49	188.0	25.6	24.2	34	B	- 1.4
50	198.5	9.1	9.3	13	E	0.2
51	203.0	13.6	13.5	19	F	- 0.1
52	199.0	9.6	10.0	14	O	0.4
53	195.0	5.6	5.0	7	R	- 0.6
54	188.0	25.6	25.6	36	E	0
55	183.0	20.6	20.7	29	-	0.1
56	186.5	24.1	23.5	33	L	- 0.6
57	200.0	10.6	10.0	14	A	- 0.6
58	201.0	11.6	11.4	16	N	- 0.2
59	197.5	8.1	7.8	11	D	- 0.3
60	198.0	8.6	8.5	12	I	- 0.1
61	175.5	13.1	13.5	19	N	0.4
62	215.5	26.1	24.9	35	G	- 1.2
63	170.5	8.1	8.5	12	-	0.4
64	214.5	25.1	24.2	34	B	- 0.9
65	168.0	5.6	5.7	8	O	0.1
66	204.5	15.1	15.0	21	A	- 0.1
67	183.5	21.1	21.4	30	T	0.3
68	197.0	7.6	7.1	10	S	- 0.5
						- 11.3 Total ms bias

Figure 4

TOP SECRET CONTROL NUMBER W/D 55-1147
COPY 19 OF 25 COPIES 40
PAGE 19 OF 30 PAGES
LIBRARY NO S60,081

~~TOP SECRET~~ (Continued from page 4) Figure 4.

Motor speed calculated from film of "all spaces" filmed using the governed motor = 2217 rpm.

27.06 ms per revolution of print-wheel

0.712 ms per character

6 revolutions of print wheel = 162.4 ms.

7 revolutions of print wheel = 189.4 ms.

8 revolutions of print wheel = 216.4 ms

$\frac{-11.3}{68} = -0.166$ ms average bias per letter of message.

$\frac{-0.166}{0.712} =$ 0.233 character, average bias per letter of message.

Donald E. Schumacher
NSA-314
2 August 1955