AMERICAN Brake Shoe COMPANY

METALLURGICAL DEPARTMENT

Mahwah, N. J. August 2, 1943

"CONFIDENTIAL" \ not a military classification

AMERICAN BRAKE SHOE COMPANY CRYPTOGRAPH

An Electrical Cyphering Device

Departmental Report No. 14-K-79

Earnshaw Cook, Chief Metallurgist

August 2, 1943

AMERICAN Brake Shoe COMPANY

METALLURGICAL DEPARTMENT

Mahwah, N. J. August 2, 1943

"CONFIDENTIAL" — not a military classification

THE AMERICAN BRAKE SHOE COMPANY CRYPTOGRAPH

An Electrical Cyphering Device

During the design of an electrical instrument for calculating continuously the solution of nine simultaneous equations of the first degree, it seemed that a modification of the apparatus might lend itself to a chance arrangement of the alphabet sufficiently random in nature to be useful as a military cipher. This apparatus and its circuits are illustrated in Figures 1 and 2, respectively.

The principle employed with the instrument in its simplest form is the use of three variable resistances, (1, 2, 3) connected in series with dial positions representing the letters of the alphabet, and with a constant, controlled voltage supplied to the circuit by a small dry cell. Millivolt meters, (1, 2, 3) are connected in parallel with each rheostat. It is obvious, then, that the smallest movement of any one dial changes the readings of all three meters. It is proposed that imposition of the letters of the clear message in sequence upon these dials will produce meter readings whose values will depend upon the random appearance of the two preceding letters in the message as illustrated below:

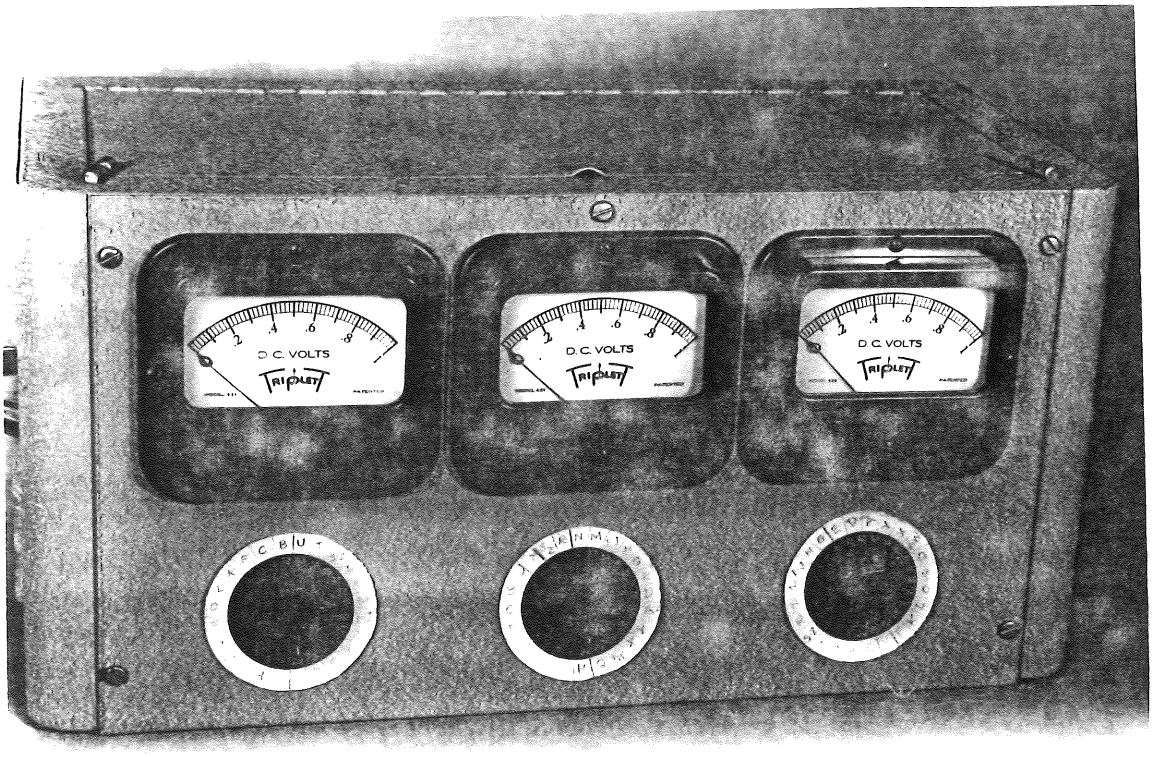
Table 1

	Clear	Examples		Preceding Letters	
1.	B	-	-	-	-
2.	A	A	-	XB	-
3.	N	-	N	-	BA
4.	N	-	N	-	AN
5.	A	A	-	NN	NA
6.	N	-	N	-	-
7.	A	A	-	AN	-
8.	S	-	-	-	-

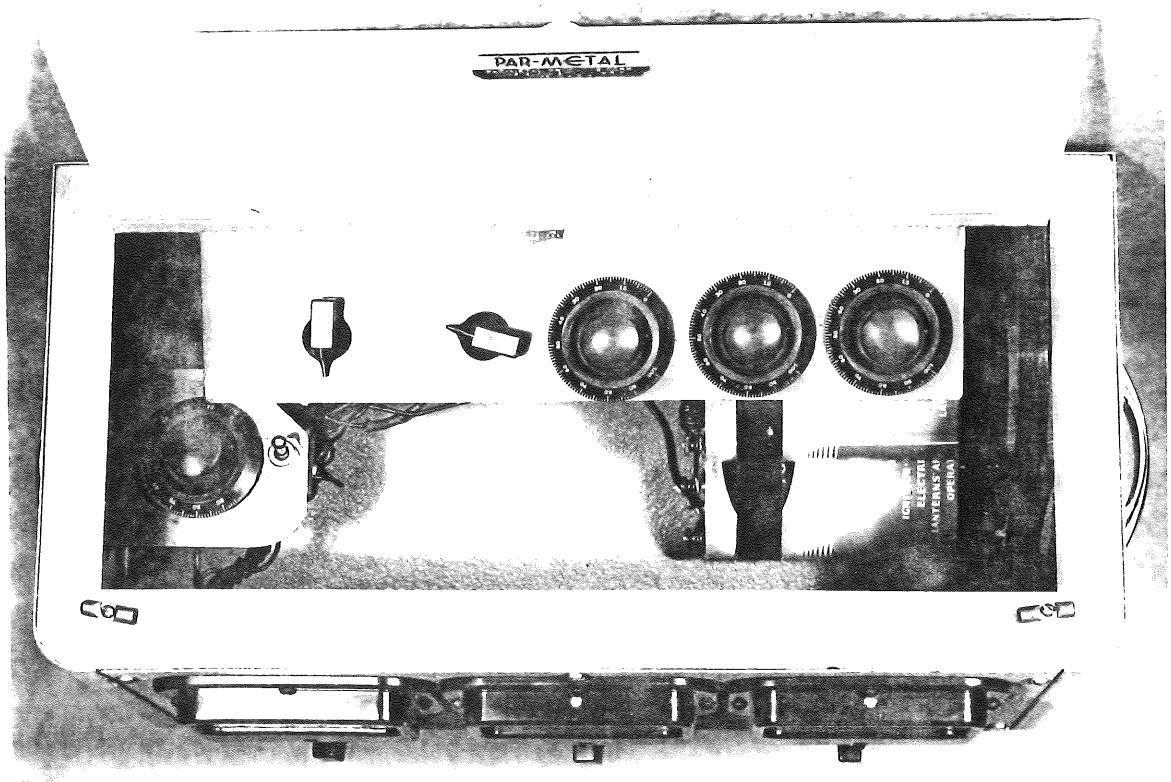
AMERICAN BRAKE SHOE COMPANY

METALLURGICAL DEPARTMENT

CYPHERING APPARATUS



Front View



Top View

Thus within one word, "bannanas", the meter number for the letter "A" has been established by the different preceding dial settings XB, NN, AN; while "N" has values from the combinations BA, AN, NA.

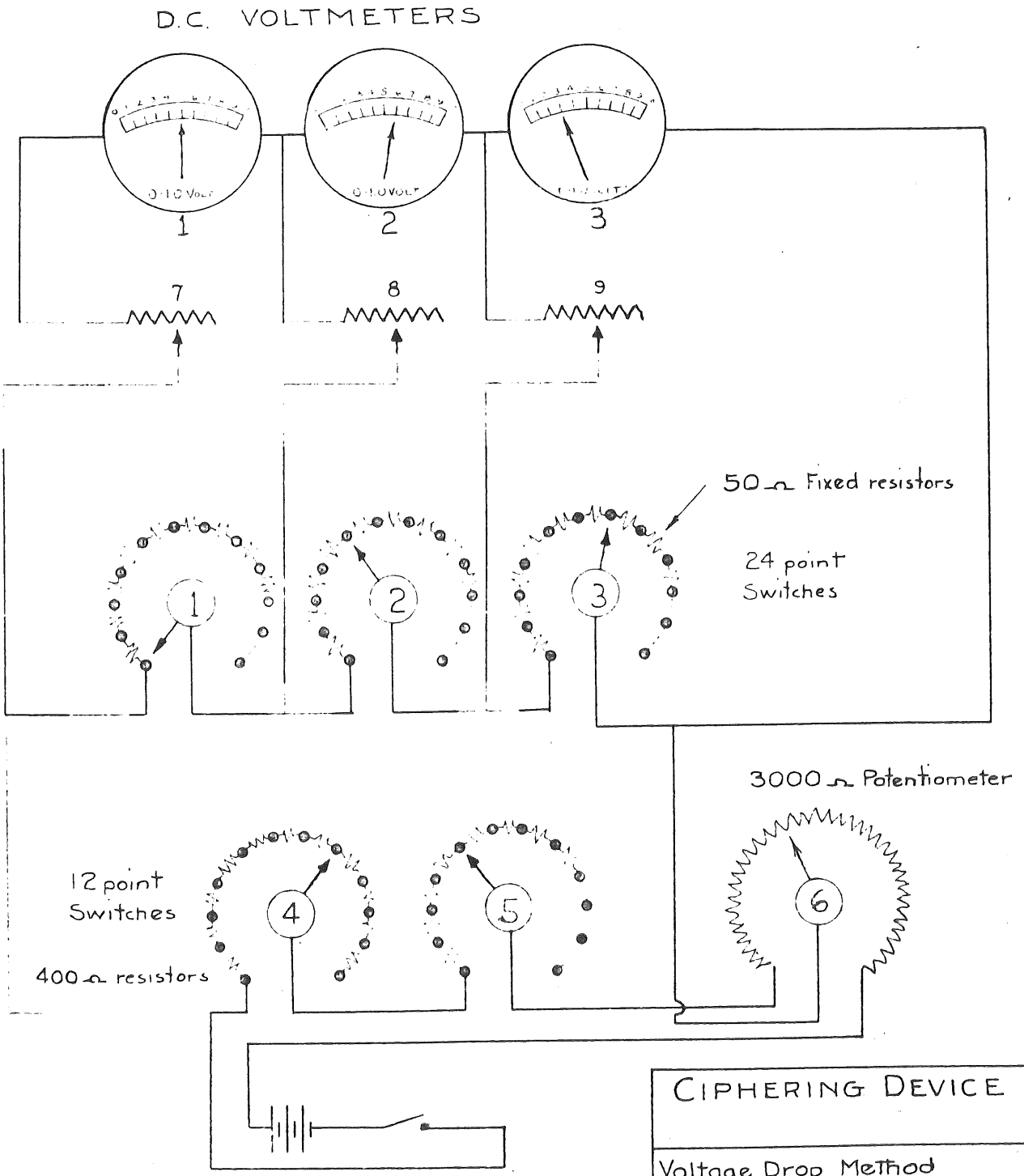
The obvious weakness of the cipher in this form exists in the cycling of any repeated word in the same message which has one chance in three of falling upon the same dial during ciphering. While this seemed to have little effect upon the random appearance of various letters for the same numbers in tabulations made from the cipher against the clear for an ordinary short message, it was considered objectionable and was eliminated by introducing combined 13-step rheostats (4, 5) in series with the main voltage control (6) which were changed each time a selected high frequency letter (such as E, T, or A) occurred in the message. Since "E" appears approximately 13 times per hundred letters of English, there might be one chance in 39 for cycling of the same word within 1300 letters (or within 250 words). Again, the same three-letter word, such as "man" or "the" may be imposed upon the machine 13 times in succession before exact repetition of the cipher can occur. This can be complicated further or extended with little difficulty if it is found to be expedient.

Since the tabulations above also indicated some tendency for particular letters to repeat for low meter readings, additional variable resistances (7, 8, 9) were introduced in series at the lower scale end of each of the three main resistances (1, 2, 3). The maximum readings of the meters can thus be adjusted with the main voltage control (6) while the minimum meter readings can be set with the auxiliary rheostats (7, 8, 9). Repetitions of the same letter for the same number were thus minimized sufficiently for safety.

AMERICAN BRAKE SHOE COMPANY

Metallurgical Department

Schematic Wiring Diagram



CIPHERING DEVICE
Voltage Drop Method
July 14, 1941 H.S.A. Dwg. 23

It is understood that many ciphers,- substitution, transposition, combination, grill, syllabic or mechanical types,- follow a definite and repetitive pattern for the same key. However involved it be, if the pattern is discovered, the entire system is revealed and decyphering becomes possible. Where in the electrical cipher, each message itself is depended upon inherently to produce a different pattern, and where the introduction of even a single null will also achieve a completely different pattern for repetitions of the same message,- solution would seem to be correspondingly more obstinate. It may be argued that electrical circuits also follow known formulae but it would be more than difficult to calculate the relation between millivolts, ohms and letters or intervals for continuously changing criteria which are necessarily different for each word or combinations of words.

Assuming that the circuits as established were sufficiently involved for messages of ordinary length, security was attempted by complicating the key rather than the instrument. Tabulation of the possible variations (which may readily be increased) appears in Table 2:

Table 2

Variations of Key

	Variable	Minimum Possible Variations	
(1)	3 Alphabet Dials:	24 x 24 x 24	= 13,824
(2)	1 Main Voltage Regulator:	25 (?)	= 25
(3)	3 Minimum Voltage Dials:	24 x 24 x 24	= 13,824
(4)	1 Automatic Voltage Changer:	13	= 13
(5)	Key Sequence:	8	= 8
(6)	Code Letters:	8 x 10	= 80

While the multiplication of these variables indicates an astronomical number of keys without changing the alphabet dials, it is always possible that some unexpected weakness may develop. Since the instrument has been presented in comparatively simple form, it is respectfully suggested that the existence of any such defects can probably be eliminated by slight additions or modifications of the present circuits. The key for the seventeen messages submitted is shown in Table 3. For convenience, the dial (1, 2, 3) positions have been numbered from 1 to 24: position 1 is a null while letters "Y" and "J", "S" and "Z", have been coupled.

Table 3

Key to Messages

Item No.	Sketch No.	Setting
(1)	Meters: 1, 2, 3	"74" with rheostat #6 for positions 24
(2)	Meters: 1, 2, 3	"50" with rheostats #7, 8, 9, for position 1
(3)	Dials: 1, 2, 3	Alphabet rings with letter "E" on positions 22, 17, 13, respectively.
(4)	Initial Dial Settings: 1, 2, 3	Positions: "X" : 12 : 24
(5)	Scrambling Dial #4	Change on "E", positions #0-11, incl.

The following procedure is employed for calibrating the instrument for a particular key with given alphabet dials.

Table 4

Calibration of Instrument

(1.) Set mechanical zeros of galvanometers with switch off.

(2.) Set dials 1, 2, 3, at positions #24, and adjust meters 1, 2, 3 to read "74" with rheostat #6. (#7, 8, 9 at zero position).

(3.) Set dials 1, 2, 3, at position #1, and adjust meters 1, 2, 3 to read "50" with rheostats #7, 8, 9 in sequence. Check readings for positions #24 now become "75".

Table 4 - (continued)

(4.) Set alphabet rings for dials 1, 2, 3 so that letter "E" is opposite positions, #22, 17, 13, respectively.

(5.) Initial dial settings: #1 - first letter of message
#2 - position #12
#3 - position #24

(6.) Scrambling dial #4: change progressively from position #0 through #11 as letter "E" occurs in message.

(7.) Dial letters of the clear in sequence, proceding from left to right, and record meter readings for each letter. This is the cypher.

It should be realized that these apparent complications disappear with familiarity with the instrument. Calibration can be checked in two minutes. The alphabet rings (subject to innumerable variations) are identical, with deliberate separation and location of high frequency letters. Even slight changes of any one of the key positions listed in Table 4 will change the entire complexion of the cypher, nor can the message be reduced to the clear without precise settings for each variable.

It is recognized that one of the objections to this particular cypher exists in having double numbers for each letter of the clear in its present form. An analysis of the Morse telegraphic code shows that there are a total of 83 separate signals (dots and dashes for 26 letters, all of which would be used at random in a standard cypher,- an average of 3.2 signals per letter. By combining the 10 shortest Morse letters, E, T, I, M, A, N, S, O, U, D, having a total of 22 signals, it is possible to represent all the numbers from 20 to 99 with a total of 336 signals,- an average of 4.2 signals per letter of the

clear as shown below:

Table 5

Code Letters

0	1	2	3	4	5	6	7	8	9
N	E	S	T	I	O	U	M	D	A

2 - U
3 - A

4 - M
5 - E

6 - T
7 - I

8 - N
9 - S

Thus: 20 = UN 42 = MS 64 = TI 86 = MU
31 = AI 53 = ET 75 = IO 97 = SM

The mechanical construction of the instrument, its speed and accuracy are beside the point for the present unless a new principle of cyphering of interest to the Government can be developed. The present apparatus has sufficient accuracy for demonstration purposes. The use of high resistances prevents deterioration of the batteries for long use or polarization in continuous service for hours at a time. Cyphering and decyphering speeds with complete manual operation are approximately 8 to 10 letters per minute as compared with an estimated 20 to 30 letters per minute for mechanical cryptographs. The present design may be compressed within a space of about 3" x 5" x 10". Engineering to print a tape with other automatic features would probably increase its size,- certainly its speed and accuracy.

It should also be noted that, while errors in cyphering or decyphering will produce a scrambled message in many cryptographs,- this instrument will return correctly to the clear within 3 letters after each error provided that

decyphering has omitted no letters of the message nor employed the wrong dial sequence.

In conclusion it should be emphasized that we are under no delusions concerning our general ignorance of crytography, nor of the human ingenuity applied over centuries to the unachieved development of an unbreakable cypher. This system is presented with due humility for what it may be worth and with the sincere hope that it can be useful during the national emergency. Even its consideration by the Signal Corps is highly appreciated. If further demonstration or cooperation can be of service in any degree, the War Department may be assured of our continued interest and prompt response.

Respectfully submitted,

Earnshaw Cook

Earnshaw Cook
Chief Metallurgist

EC:MD
cc: Col. Lippincott (3)
File (4)

MESSAGES

IX. COMMUNICATION WITH SECOND DIVISION WILL BE DISCONTINUED UNTIL JUNE THREE WITH THIRD DIVISION UNTIL FURTHER NOTICE STOP BEGINNING AT ZERO ZERO FIVE ZERO STRICT RADIO SILENCE WILL BE OBSERVED UNTIL CONTACT WITH ENEMY HAS BEEN MADE STOP WIRE COMMUNICATION WILL BE RESTRICTED TO ABSOLUTE MINIMUM REQUIREMENTS

X. MOVE FOUR BATTALIONS OF DOCK LABORERS IMMEDIATELY TO UNLOAD BAGGAGE OF SECOND CONTINGENT WHICH WILL ARRIVE AT TEN O CLOCK AM X

XI. GAS ATTACK ON AIRDROME AT ZERO EIGHT FIFTEEN STOP NO CASUALTIES IN SQUADRON PERSONNEL STOP ANTIAIRCRAFT DEFENSE HAMPERED ATTACK STOP AIRPLANES NOW BEING DECONTAMINATED

XII. ATTACK BEGAN THIS MORNING AT ZERO FIVE ZERO FIVE O CLOCK WITH HEAVY ARTILLERY SUPPORT AND ABOUT FIFTY TANKS STOP SECTOR OF OUR FIFTY FIFTH DIVISION WAS PENETRATED TO ABOUT TWO HUNDRED YARDS STOP ENEMY ARTILLERY VERY ACTIVE UNTIL ZERO SEVEN HUNDRED O CLOCK STOP OUR COUNTER ATTACK BEGINS AT ZERO NINE HUNDRED

XIII. TO MAINTAIN SECRECY MOVEMENTS MUST BE UNDER COVER OF DARKNESS AND COVERED BIVOUAC AREAS MUST BE OCCUPIED DURING DAYLIGHT HOURS STOP UNOBSERVED DAYLIGHT MOVEMENTS WILL REQUIRE THE RESTRICTION OF HOSTILE AIR OBSERVATION BY ANTIAIRCRAFT ARTILLERY AND COMBAT AVIATION

XIV. YOU WILL MOVE TO POSITION ON SOUTH MOUNTAIN TOMORROW COMPLETING MOVE BY TEN PM STOP RED FORCES ESTIMATED AT TWO DIVISIONS ARE MOVING ON GETTYSBURG DASH HANOVER ROAD STOP THIS DIVISION WILL CONTINUE TO GUARD THE RIGHT FLANK OF OUR CORPS STOP AMMUNITION WILL CONTINUE TO BE FURNISHED IN ANY AMOUNTS DESIRED BOTH FOR SEVENTY FIVES AND FOR LARGE GUNS STOP GASOLINE FOR TRACTORS WILL BE OBTAINABLE AT FOUR CORNERS AFTER EIGHT AM TOMORROW

XV. HOSTILE ATTACK HAS BEEN STOPPED IN FRONT OF BATTALION RESERVE LINE IN RIGHT CENTER OF RESISTANCE OF THIRD INFANTRY STOP THIRD INFANTRY IS COUNTERATTACKING WITH REGIMENTAL RESERVE TO REESTABLISH FRONT LINE

XVI. ENEMY TROOPS HAVE BEEN SIGHTED ON HIGH GROUND EAST OF GREENVILLE AND IN THE VICINITY OF EAGLE LAKE STOP SEVERAL COMBAT PATROLS HAVE BEEN SENT OUT TO GAIN CONTACT WITH THE ENEMY AND GAIN INFORMATION AS TO HIS EXACT POSITION STOP WILL REPORT FURTHER ON THEIR RETURN

XVII. THE ENEMY COUNTERATTACK HAS BEEN DEFINITELY STOPPED EAST OF WHITE RUN STOP MY LINE NOW EXTENDS FROM ROAD JUNCTION TWO THREE EIGHT TO THE CROSS-ROAD OF FAUPLAY