MEMO ROUTING SLIP

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

1 NAME OR TITLE Dr. Kullback	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION AFSA-03A	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Herewith some old papers which may be of interest and use in AFSA-03 files, for historical purposes. One set of papers (Encl 1) deals with an early type of coincidence machine. The other paper (Encl 2) deals with a proposed machine for locating idiomorphs and isomorphs. I would like to know if any machine for these latter purposes was ever built -- aside from any modifications in IBM to do the same kind of job.

FROM NAME OR TITLE WFF	DATE 16 Aug 50
ORGANIZATION AND LOCATION AFSA-14	TELEPHONE 455

NME FORM NO 95 1 OCT 48 Replaces DA AGO Form 895, 1 Apr 48, which may be used. 66—16—49487-8 GPO

	From	To	
1.	SIS	WP&T	1. Under date of April 16, 1937, there was forwarded a sketch and brief description of a machine which has been called a Cryptanalytic Coincidence Counter. This machine would be very useful not only in Signal Intelligence Section, but also in the Signal Intelligence School. It would accomplish, automatically, certain operations and calculations at a great saving in time and labor. It also would afford the basis for further extension of ideas regarding the construction of electrical and mechanical aids in cryptanalysis which is becoming a field of very considerable importance. 2. The principal pieces of apparatus required for the construction of the machine are printing telegram transmitters of the type known as Western Electric 1-B Multiplex. It is understood that a certain number of these transmitters may be obtained from the Hawthorne Plant of the Western Electric Company at Chicago at a price of $25.00 each. It is desired that six of these be obtained if funds are available therefor. H.G.M. W.F.F. 6-5-37 COPY

~~SECRET~~

1st Memo. Ind. 8

OCSigO, W.P.&T. Div. April 17, 1937 - To The Chief Signal Officer

1. It is recommended that this matter be referred to the Signal Patent Board for suitable action.

W. E. Rumbough,
Majdr, Signal Corps.

~~SECRET~~

SECRET

SIS files

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

8

April 16, 1937

MEMORANDUM FOR: War Plans and Training Division.

1. Accompanying this memorandum is a sketch and brief description of an invention of a machine which I have called "A Cryptanalytic Coincidence Counter" and which would be extremely useful in our work.

2. Also accompanying this memorandum is a description of an invention of a machine which I have called "A Cryptanalytic Idiomorph and Isomorph Locator". This machine is a good deal more complicated than the coincidence counter, but is not thought to be impractical. It would also be very useful in our work.

3. It is recommended that both inventions be submitted to the Signal Patent Board for such action as is deemed suitable. In my opinion both inventions should be placed in the secret category, at least for the present.

William F. Friedman.

Enclosures.

SECRET

REF ID:A105026

ROUTING AND WORK SHEET

(To be used under provisions of Par. 41, 6 b, Office Regulations, OCSig, 1934)

Number each Action	From	To	Memorandum	Initals and date
1	SIS	WP&T	1. Under date of April 16, 1937, there was forwarded a sketch and brief description of a machine which has been called a Cryptanalytic Coincidence Counter. This machine would be very useful not only in Signal Intelligence Section, but also in the Signal Intelligence School. It would accomplish, automatically, certain operations and calculations at a great saving in time and labor. It also would afford the basis for further extension of ideas regarding the construction of electrical and mechanical aids in cryptanalysis which is becoming a field of very considerable importance. 2. The principal pieces of apparatus required for the construction of the machine are printing telegram transmitters of the type known as Western Electric 1-B Multiplex. It is understood that a certain number of these transmitters may be obtained from the Hawthorne Plant of the Western Electric Company at Chicago at a price of $25.00 each. It is desired that six of these be obtained if funds are available therefor.	6-5-37 H.G.M. W.F.F.
			37 91	

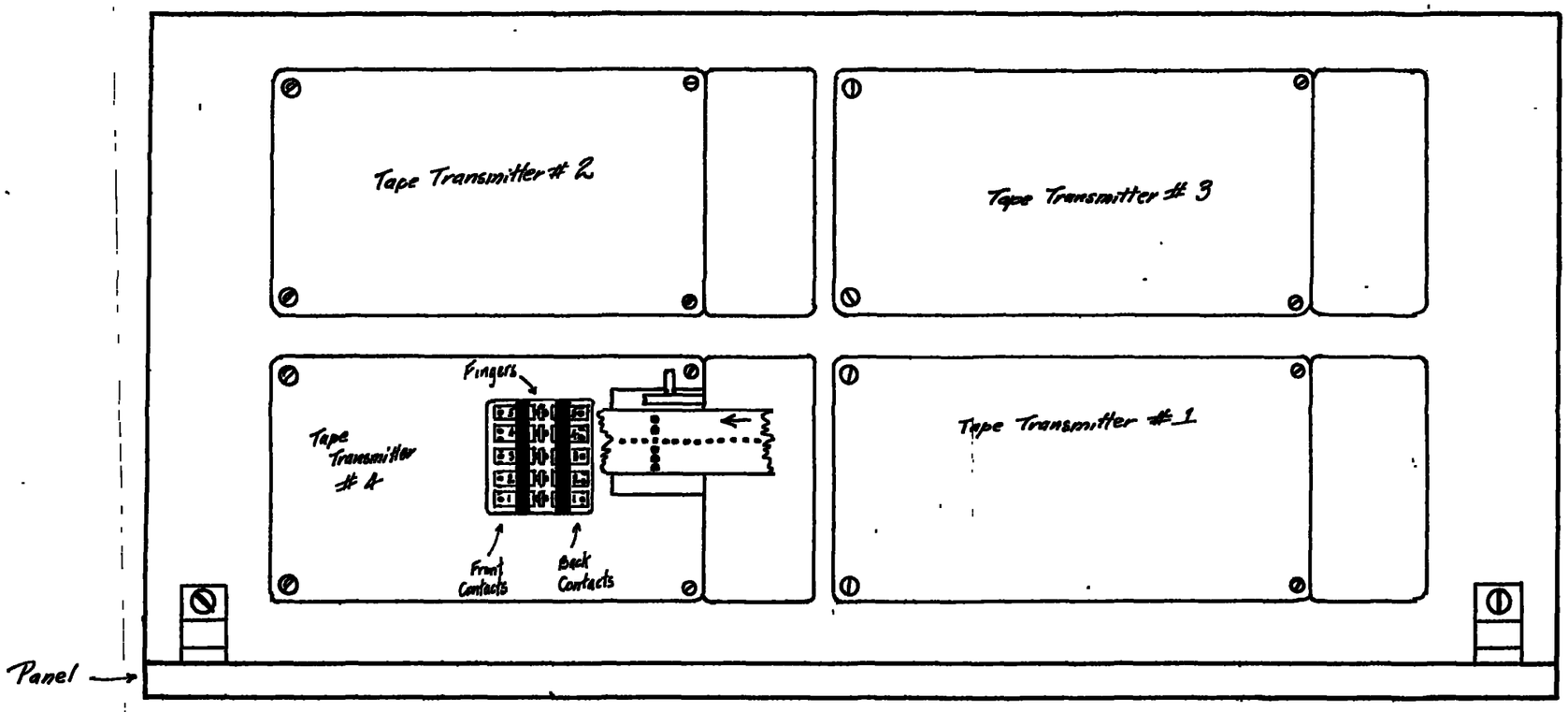
Sheet No.: _____

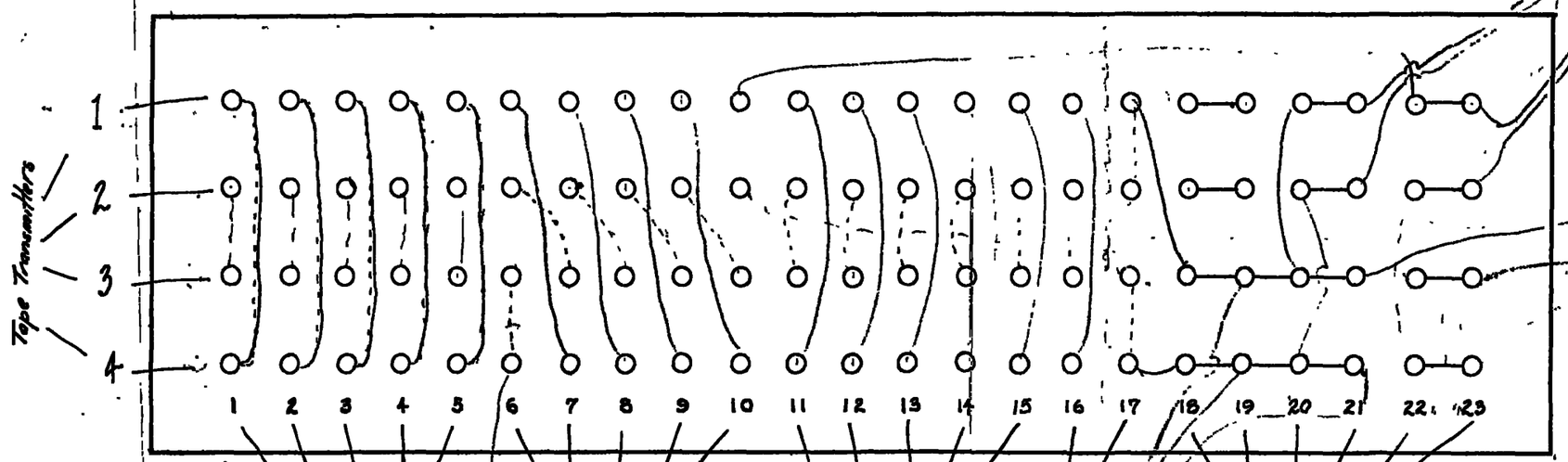
NOTES ON SETTING UP AND OPERATING THE COINCIDENCE MACHINE

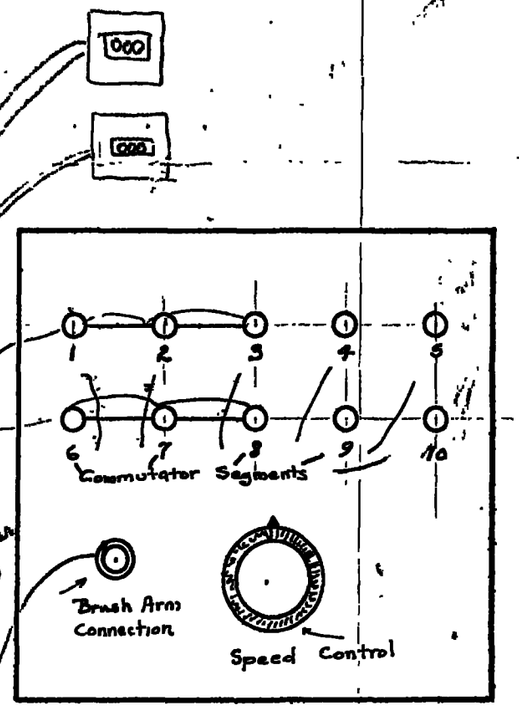
The attached diagram gives the location of the tape transmitters with respect to the row of jacks to which they are connected. The jacks are numbered from the left hand side of the panel. The first 5 of each row are connected to the back contacts of the tape transmitter, the second 5 are connected to the fingers, the third 5 are connected to the front contacts, and the 16th and 17th are connected to the stepping magnets. The connections for the remaining ~~contacts~~ jacks are as shown on the diagram. These remaining contacts are simply to be used for convenience in making connections and have no relation at all with the transmitters.

The machine operates best when the stepping magnets of two transmitters are connected in series. Four will not operate satisfactorily if connected in series, and if all are connected in parallel too much sparking of the commutator brush results. All 10 segments of the commutator should not be used at a speed of around 500 characters per minute. Best results were obtained by connecting segments 1,2 and 3 to energize the stepping magnets, and segments 6,7 and 8 to energize the counters in the comparing circuits. The counter giving the total number of letters counted is connected in parallel with the stepping magnets.

If only two transmitters are used a $\frac{1}{2}$-MF condenser should be connected in the stepping magnet circuit to suppress the sparks. A one megohm resistor connected across this condenser seemed to work fairly satisfactorily. When all four transmitters are used, the 3 3-MF's are connected in series in place of the $\frac{1}{2}$-MF used in the case of only two transmitters.

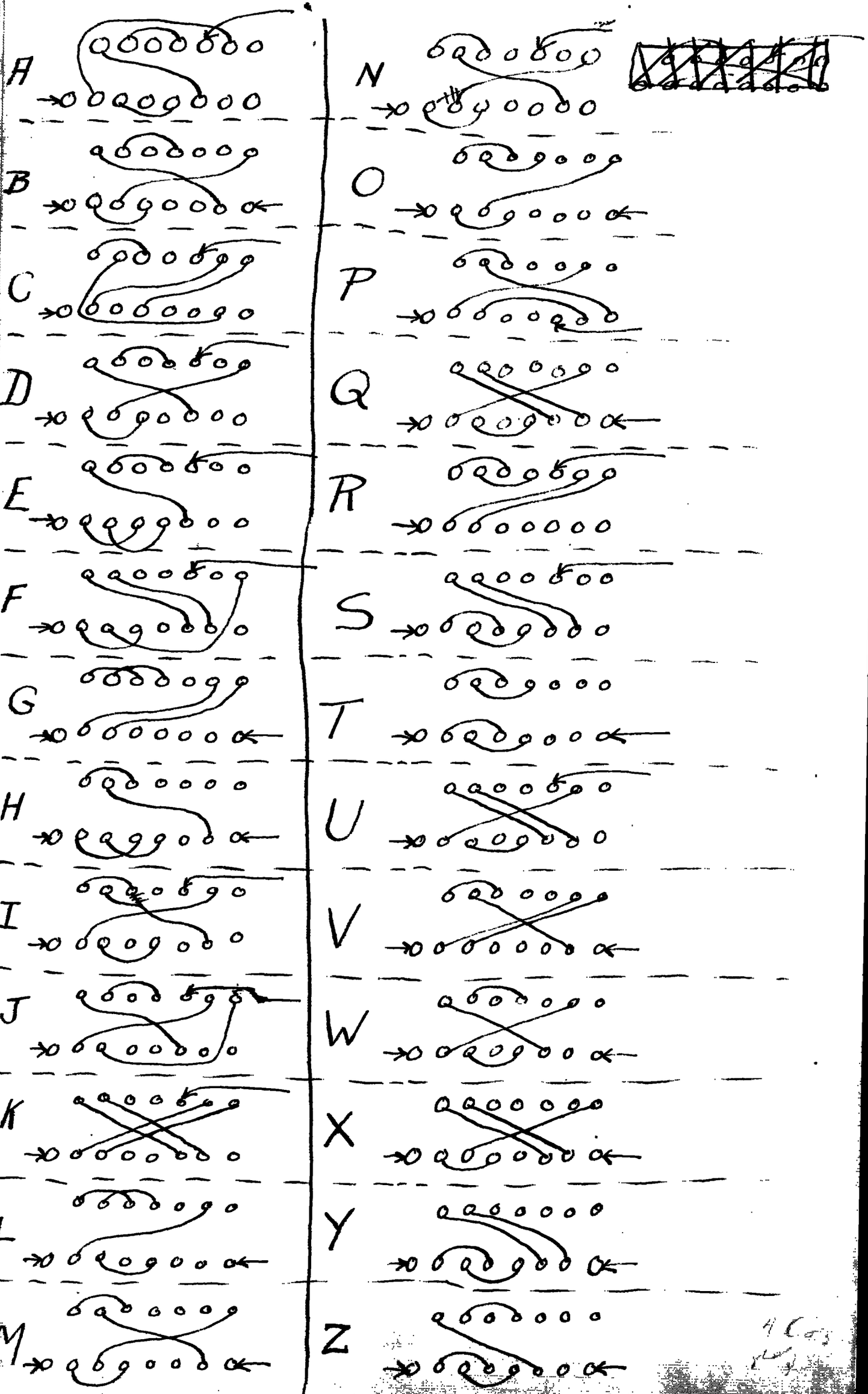


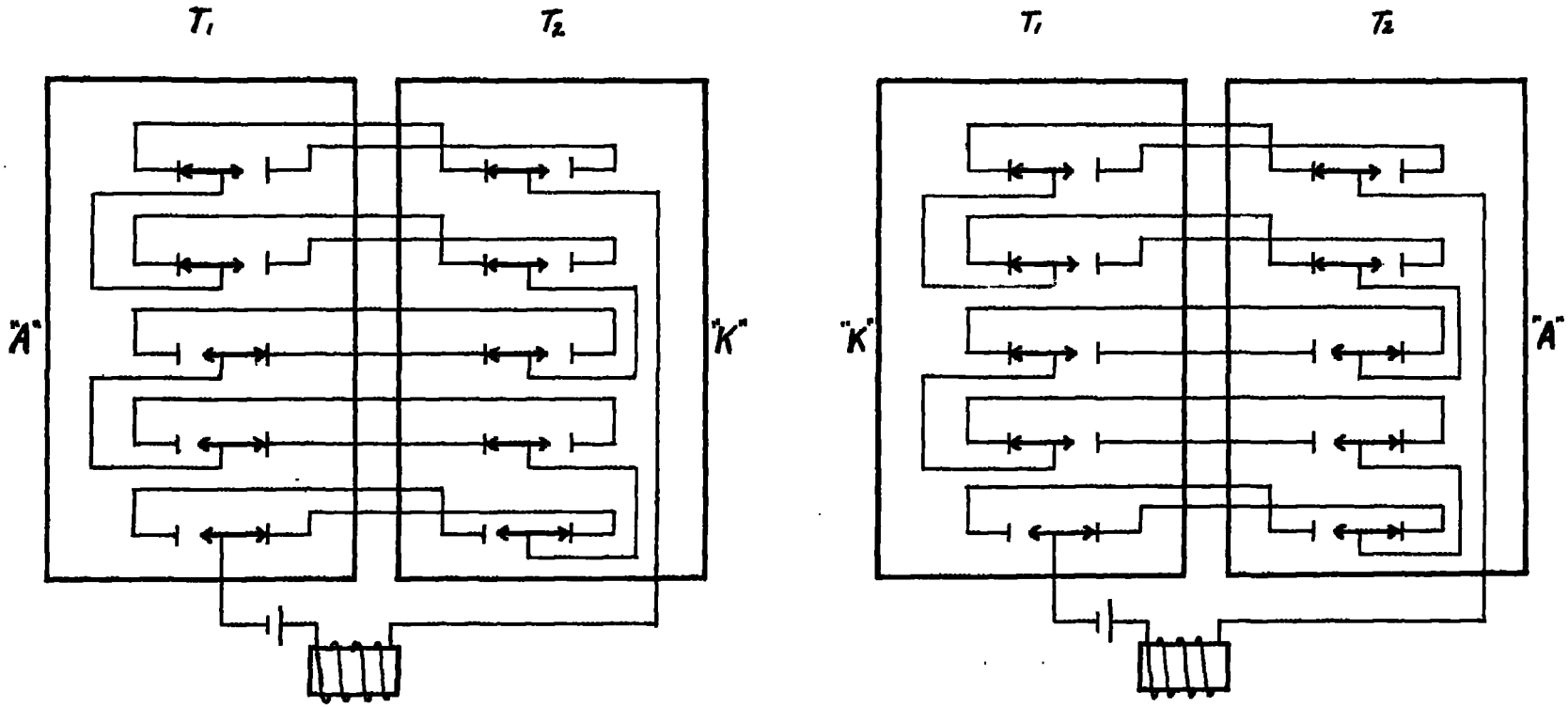


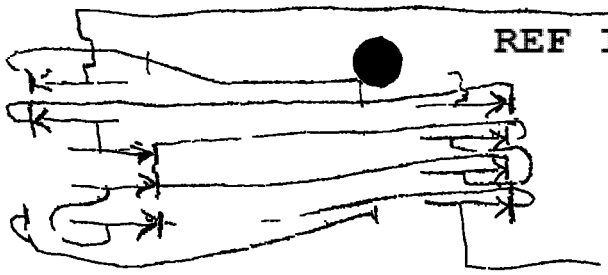


Pencil line shows connections for using Tape Transmitters 1 and 4 for conveying tapes

file: Coincidence Machine.


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





Memo for R+D Dir Thru WP+T

1 Attached hereto is a drawing + description of an apparatus which I have called a 'cryptanalytic coincidence counter' and which I have invented to assist me in cryptanalytic research.

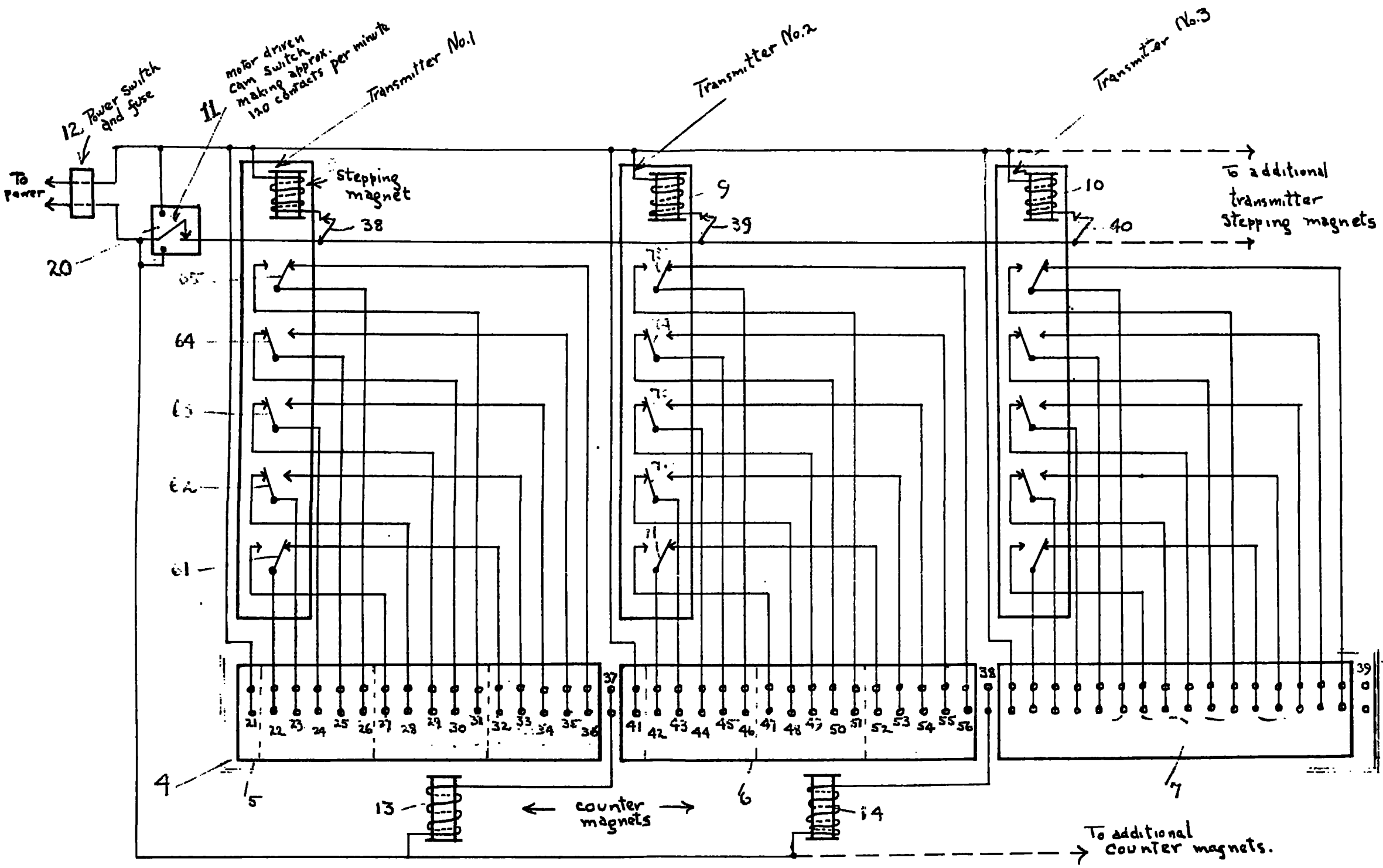
It is very desirable that one of these apparatuses be constructed as soon as practicable for use in this section.

2 Basically the apparatus comprises two or more tape transmitters of the 5-unit-code type; one or more electrically-operated counters similar to those used in telephone switching apparatus; and a means for periodic energizing of the stepping magnets of the transmitters.

3 I have three tape transmitters which can be used for this purpose but minor changes will have to be made in them to adapt them to this purpose. For periodic energization of the stepping magnets either a thermo-switch of the "flasher" type or a motor driven cam switch may be used.

4 If the laboratories are in a position to ~~be~~ assemble one of these apparatuses within the next few weeks, this would be highly desirable. Otherwise it would be advisable that the work be done locally ~~←~~ It is ~~estimated that one of these the apparatuses can~~ ~~work~~ could be done for about $150.00

SECRET



Disclosed to me Jan 11, 1937
Solomon Kullback
Asst Cryptt. O.C. Sig. O

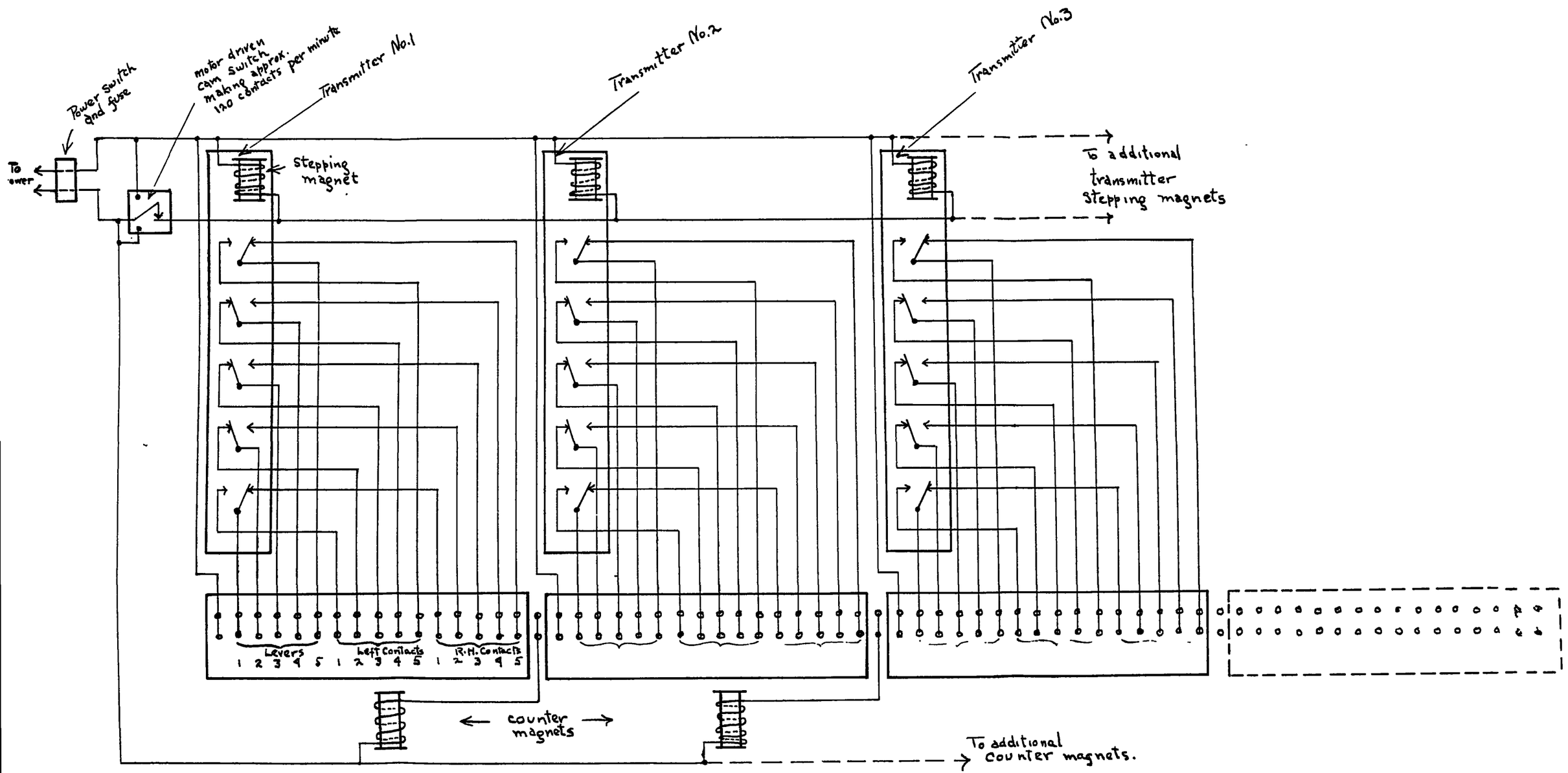
Disclosed to me Jan 11, 1937
Frank B Rowlett
Asst Cryptanalyst OCSigO

Harold S Smith
Capt. U.S. Jan 11th 1937.

Cryptanalytic Coincidence Counter
Invented by
William F. Friedman
Washington, Jan. 11, 1937.

~~SECRET~~

~~SECRET~~



Disclosed to me Jan 11, 1937
Solomon Kullback
Asst Cryptt. O.C. Sig. O.

Disclosed to me Jan 11, 1937
Frank B Rowlett
Asst Cryptanalyst OCSigO

Harold E Mills
Capt Sig C. Jan 11th 1937.

Cryptanalytic Coincidence Counter
Invented by
William F. Friedman
Washington, Jan. 11, 1937.

system + means of electrically determining coincidences between letters in a message + determining periodicities,

January 11, 1937

William F. Friedman

Jan 11th 1937

Harold H. Doyle

Cal. OSI

- Frank B. Rowlett and cryptanalyst OCSigO

Solomon Kullback and cryptanalyst OCSigO

Counter

Counter

Counter magnet

Counter magnet

T4

T3

T2

T

etc,

Tape of message set at pt #3;

Tape of message set at pt #1;

Tape of message set at point no. 2

Tape of message set at pt #2

Comparison circuit with two tape transmitters connected in series as per Graham + Friedman #

~~SECRET~~

Description of the General Principles of an Invention of a Machine for Locating Idiomorphs and Isomorphs in Cryptanalysis

A. Preliminary Remarks

1. The experienced cryptanalyst very frequently has occasion to use the "probable word method", that is, he assumes the presence of a word in the text and tries to find it by one means or another. The word for which he is searching usually contains several repeated letters the identities and positions of which impart to the word a characteristic or peculiar "pattern" or "formula". Such words are termed idiomorphic. For example, the words BATTALION, DIVISION, and ARTILLERY are idiomorphic, and each has a distinctive formula of composition. The formula for the word BATTALION is representable by a sequence of arbitrarily-assigned digits standing for the different and the similar letters, as shown herewith:

B A T T A L I O N
1 2 3 3 2 4 5 6 7

In other words, the idiomorph is "coded" in the sense commonly spoken of in connection with the use of tabulating machinery operations.

2. Suppose the cryptanalyst suspects the presence of the word BATTALION in a message. Having established the formula for the word, he goes through the text, beginning with the first letter and sliding the formula against the text one step at a time, until he finds a place where the formula for a sequence of nine letters in the text is matched by or coincides with the formula 1 2 3 3 2 4 5 6 7 (= BATTALION). In this process the cryptanalyst must either indicate on paper, or see with his mind's eye, the textual formula that is at the moment in juxtaposition with the formula of the word for which he is searching.

3. Again, the cryptanalyst may not have a definite word in mind for which he is searching, but is simply desirous of locating two formulae which are identical and which are technically called isomorphs. In this case, he establishes a continuously changing series of formulae, beginning with the first letter of the text, and tests each of them against the remaining text of the same message or against the text of another message. For example, he may start with the first ten letters of the message and note the formula for these ten letters. He then applies this first formula to another part of the text, beginning at a given point and sliding the formula against this text one step at a time to see if he finds another sequence with an identical formula. If not, he starts with the second letter of the message, notes the formula for a sequence of ten letters, and repeats the search. When he encounters a formula which coincides with the one he has set up, he has found a case of isomorphism. The two isomorphs may or may not correspond to the same plaintext word. For example, the three words WARRANT, LETTERS, and MISSION have

~~SECRET~~

identical formulae and are isomorphic. In searching for isomorphs, if the cipher text should contain all three of these words enciphered monoalphabetically, the cryptanalyst would not know whether the isomorphs he finds in the message represent three occurrences of the same word, or two occurrences of one word plus a different word with the same formula, or a single occurrence of three different words. These alternatives would be determined later, by further analysis. At the moment, the important fact is that he has located cases of isomorphism.

4. The present "hand" methods of locating idiomorphs and isomorphs are very tedious, slow, and subject to human error. Automatic machines for locating them would be quite useful, and it is the purpose of this invention to provide such machines and to describe the method of their use. Basically, the invention employs the comparison circuits used in the "coincidence counter" described in another paper, in combination with additional mechanisms to be described.

5. The text in which idiomorphic or isomorphic sequences are to be located is prepared in the form of perforated Baudot tapes. Several copies of the text tapes are prepared, the number depending upon the length of the sequences for which a given machine is constructed. Machines for locating 6, 7, 8, ... letter sequences may be constructed. This description will deal with machines for locating sequences up to the length of ten letters. In general, the automatic locator goes through exactly the same steps as does the human operator at present, but at a much greater speed, and without overlooking possible places where sought-for sequences may exist.

B. The idiomorph locator.

6. First to be described will be the idiomorph locator. Let us assume that we are searching for the word BATTALIONS, the presence of which is suspected in the following text:

A P D M M G F A A F V Q Z X R I Q V V W Z M A Z X Q O P A

7. The machine consists primarily of 10 Baudot tape transmitters, each being wired for comparison purposes, in a manner similar to that employed in the "coincidence counter". In this case, 10 tape copies of the message are prepared and these tapes are placed in the transmitters so that the successive starting points on the successive transmitters correspond to the successive letters A, P, D, M, ... of the message.

8. Closing a starting switch, the first letter of the message, A, in transmitter 1 is tested successively against the next 9 letters of the message, in transmitters 2, 3, 4, 5, 6, 7, 8, 9 and 10. This is done by means of a motor-driven rotary multiple switch, or other means, which successively

connects the whole set of comparison contacts of transmitter 1 with those of transmitters 2 to 10, in turn. The comparison circuits in this case merely serve to operate supervisory high-speed telephone relays to drive a series of 10 rotatable indicator wheels, the peripheries of which are divided up into 10 equal segments, numbered from 1 to 10. (This corresponds to the "coding" function referred to in Par. 1.) At the start all indicator wheels are at their reset or initial position, with segment 1 showing through a window or aligned at a bench mark. Indicator wheel number 1 is always set to position 1 and need not change; it may in fact be a "dummy" wheel. If no coincidence is encountered when transmitter 1 is compared with transmitter 2, indicator wheel 2 advances to segment 2; likewise, when transmitter 1 is compared with transmitters 3, 4, 5, ... and no coincidence is encountered in any case, indicator wheels 3, 4, 5, ... advance to segment 2. But if a coincidence is encountered at any comparison, the indicator wheel associated with the transmitter being compared at that moment is not permitted to advance any further and remains in this position. The arrangement for this stepping may be by means of a continuously acting ratchet and pawl for each wheel and only when there is coincidence is the pawl withdrawn and locked into inactive position. For example, take the first 10 letters of the illustrative message:

1	2	3	4	5	6	7	8	9	10
A	P	D	M	M	G	F	A	A	F

After transmitter 1 (set to A) has been tested against the rest of the transmitters, the indicator wheels are at the following positions:

Indicator wheel	1	2	3	4	5	6	7	8	9	10
Text	A	P	D	M	M	G	F	A	A	F
Setting of wheel	1	2	2	2	2	2	2	1	1	2

This corresponds with the repeated letter A in positions 1, 8, and 9 in the sequence A P D M M G F A A F. Indicator wheels 8 and 9 will now stay at position 1.

Transmitter 2 is now tested against the remaining transmitters, in turn. Since the letter F does not reappear in the sequence, the indicator wheels 3, 4, 5, 6, 7, and 10 advance one step. The formula is then:

Indicator wheel	1	2	3	4	5	6	7	8	9	10
Text	A	P	D	M	M	G	F	A	A	F
Setting of wheel	1	2	3	3	3	3	3	1	1	3

Transmitter 3 is now tested against the remaining transmitters, in turn. Since the letter D does not recur, the indicator wheels 4, 5, 6, 7, and 10 advance one step. The successive formulae set up on the indicator wheels as the successive transmitters are tested in turn against the remaining ones are as follows:

	1	2	3	4	5	6	7	8	9	10
Indicator wheel	1	2	3	4	5	6	7	8	9	10
Text	A	P	D	M	M	G	F	A	A	F
(A) T1 against remaining T's:	1	2	2	2	2	2	2	1	1	2
(P) T2 against remaining T's:	1	2	3	3	3	3	3	1	1	3
(D) T3 against remaining T's:	1	2	3	4	4	4	4	1	1	4
(M) T4 against remaining T's:	1	2	3	4	4	5	5	1	1	5
(G) T6 against remaining T's:	1	2	3	4	4	5	6	1	1	6
(F) T7 against remaining T's:	1	2	3	4	4	5	6	1	1	6

The formula for the word BATTALIONS is B A T T A L I O N S
1 2 3 3 2 4 5 6 7 8

while that resulting from the test is 1 2 3 4 4 5 6 1 1 6. Therefore, the message does not start with this word.

9. The tapes in all transmitters are advanced one step and the same procedure is followed as before, now testing the 2d, 3d, ... 11th letters of the message. When the test begins with the 6th letter of the message, the following sequence of movements of indicator wheels occurs:

	1	2	3	4	5	6	7	8	9	10
Indicator wheel	1	2	3	4	5	6	7	8	9	10
Text	G	F	A	A	F	V	Q	Z	X	R
(G) T1 against remaining T's:	1	2	2	2	2	2	2	2	2	2
(F) T2 against remaining T's:	1	2	3	3	2	3	3	3	3	3
(A) T3 against remaining T's:	1	2	3	3	2	4	4	4	4	4
(V) T6 against remaining T's:	1	2	3	3	2	4	5	5	5	5
(Q) T7 against remaining T's:	1	2	3	3	2	4	5	6	6	6
(Z) T8 against remaining T's:	1	2	3	3	2	4	5	6	7	7
(X) T9 against remaining T's:	1	2	3	3	2	4	5	6	7	8

The final formula corresponds with that of BATTALIONS and hence the word BATTALIONS <u>may</u> exist at this point in the message.

10. It will be noted that the operator must stop after each test to compare the final formula with that of the word being sought. But by going one step further, the apparatus may be constructed so as to eliminate this source of delay.

11. Let the periphery of each indicator wheel be provided with projecting pins permuted in accordance with ten different combinations of the Baudot code and let those pins operate the series of contacts of a set of comparison circuits (each as in Convertor Type M-134-T1) for testing the final formula against the formula for the word sought, as set up on a test frame. Then, whenever the final formula of a test [illegible] up on the test frame, a circuit is completed which causes a lamp to be lighted; otherwise the tape-stepping magnets of the tape transmitters are actuated and all the tapes stepped forward simultaneously whenever the final formula does not coincide with that set up on the test frame. Thus, once started on a message, the testing would continue without a stop until either a coincidence between a final formula and a test formula is encountered or else the end of the message is reached.

~~SECRET~~

C. The isomorph locator.

12. In operating the idiomorph locator it is necessary to set up a formula on a test frame, against which successive final formulae are tested in turn. If the word sought for is not in the message, a new test formula has to be set up on the test frame and this would be done by hand. But in searching for isomorphs we do not have any specific formula in mind; we take any sequence of letters in the text and compare it with similar-length sequences in the same text to see if they are isomorphic.

13. Suppose that there are two sets of tape transmitters, each operating a set of indicator wheels and let one set, hereinafter called the test set of transmitters, be used merely to establish test formulae on the test frame, these formulae corresponding to and being set up by actual sequences in the message itself. Let the other set of transmitters, hereinafter called the message set of transmitters, be used as the source of successive final formulae to be tested against the formula set up on the test set of transmitters. Let the tapes on the message set be circular, by joining first and last characters. Let the arrangement be such that when a test formula is set up by the test set of transmitters it stays there until the entire message has been tested against it; if no coincidence has been encountered, then a new test formula is set up by the test set of transmitters by advancing the tapes in these transmitters, and the process repeated, the tapes in the message set of transmitters being back again at their initial positions. When a coincidence occurs between a formula on the test frame and a final formula set up by the message set of transmitters, a circuit is completed which lights a red lamp and stops all transmitters.

WILLIAM F. FRIEDMAN,
Principal Cryptanalyst,
Signal Intelligence Section,
War Plans and Training Division,
Office of the Chief Signal Officer.

Washington, D. C.
April 14, 1937

The foregoing invention was described to us in February, 1937 by Mr. Friedman:

Rowlett } Witnesses
Miller }

~~SECRET~~

INVENTION OF A CRYPTANALYTIC COINCIDENCE COUNTER

1. In cryptanalysis it is often necessary to test two or more sequences of cipher letters to ascertain whether they are enciphered in the same cryptographic substitution period. One method of testing such sequences is to superimpose them, count for each column the number of coincidences (i.e., cases of identity) between letters, total the coincidences for the entire superimposition, and calculate the total number theoretically to be expected. If the observed number falls statistically within the limits of the theoretical expectancy, the superimposed sequences may be regarded as belonging to the same cryptographic substitution period.

2. "Hand methods" of counting the number of coincidences are slow, tedious, and subject to error due to eye and brain fatigue after a few minutes work. The present invention primarily provides a system and a mechanism for automatically observing and totalizing coincidences. It may be employed for other cryptanalytic operations, as will be set forth subsequently.

3. Basically, the mechanism comprises a series of tape transmitters of the standard Baudot or 5-unit-code type, but wired in a special manner for series-circuit employment, preferably through the intermediary of a plug and jack switchboard employing flexible conductors, and one or more electrical counters controlled by the transmitters. The accompanying sketch, Fig. 1, shows three transmitters, 1, 2, 3, arranged in this manner, with certain conductors wired permanently to switchboard, 4, which is shown as divided up into several panels, 5, 6, 7. The transmitters are provided with the usual tape-stepping magnets, 8, 9, 10, to which power is delivered intermittently through a cam switch, 11, driven by a motor or other mechanism, 20, so as to cause the tapes in the transmitters to step forward synchronously at about 120 steps per minute. These tapes bear sets of perforations in the Baudot code corresponding to letters of the alphabet, and the sequence of sets on each tape corresponds to the sequences of letters subjected to the count for coincidences, the tapes being placed in the transmitters at the proper initial points of superimposition for the count. For example, suppose there be a message of 2000 letters and it is desired to count the number of coincidences between letters 1 to 1000 and 1001 to 2000. Duplicate tapes of the message are made and one of these tapes is placed in transmitter 1 with letter number 1 at the initial position (above the transmitter pins); the other tape is placed in transmitter 2 with letter number 1001 at the initial position. Flexible conductors are now employed to connect certain contacts of panels 5 and 6, which for the sake of clarity will merely be indicated by stating the contact points thus connected:

Left-hand contacts of T1	27 and 47 28 and 48 29 and 49 30 and 50 31 and 51	Left-hand contacts of T2	Right-hand contacts of T1	32 and 52 33 and 53 34 and 54 35 and 55 36 and 56	Right-hand contacts of T2

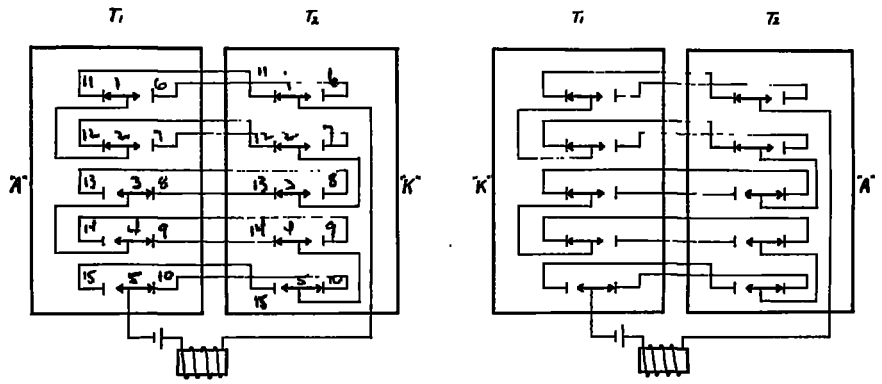
Power contact	Lever 61 of T1	Lever 62 of T1	Lever 63 of T1	Lever 64 of T1	Lever 65 of T1
21 and	22	23 and	24	25 and	26

Counter magnet	Lever 75 of T2	Lever 71 of T2	Lever 72 of T2	Lever 73 of T2	Lever 74 of T2
37 and	46	42 and	43	44 and	45

4. The circuit for the counter magnet 13 is a series circuit passing through all ten contact levers of transmitters 1 and 2. Therefore, in order that counter magnet 13 be actuated, all contact levers 61 to 65 of transmitter 1 must be in positions that are homologous with those of homologous contact levers 71 to 75 of transmitter 2; if this is not the case then no circuit is completed through the counter magnet 13. This will happen only when identical letters (no matter what these letters may be) are simultaneously passing through both transmitters, in other words, only when a coincidence occurs will the counter step forward.

5. By extension, any number of transmitters may be wired for such work, the number of counters being one less than the number of transmitters.

6. In the foregoing operations the counters of the machine are actuated by coincidences of identical letters, but it is obvious that the machine may be arranged to count coincidences of specific pairs of non-identical letters. For example, suppose it is desired to totalize the number of times an A meets a K in two sequences. By appropriate wiring this can be done, so that only when a K is passing through one transmitter while an A is passing through the other will the counter be actuated. Thus:



The principle here is that a pair of homologous levers which are in homologous positions (for coincidence of characters desired) must have their associated homologous contacts connected together; a pair of homologous levers which are in non-homologous positions must have the left-hand contact of one lever wired to the right-hand contact of the other, and vice versa, as shown in above sketch. When so arranged it is immaterial which letter comes in which transmitter; the results are the same whether "A" is passing through transmitter 1 while "K" is passing through transmitter 2, or vice versa.

7. The machine may also be used to count the non-coincidences just as easily.

8. By extension of the principle, it is possible to count the number of coincidences between 3, 4, ... different letters. For example, if it is desired to count the number of times the letters A and B, A and C, A and D, ... coincide, transmitters 1 and 2 are wired to count the coincidences between A and B; transmitters 1 and 3 are wired to count the coincidences between A and C; transmitters 1 and 4 are wired to count the coincidences between A and D, and so on. It is for this reason that the plugs in the panels of Fig. 1 are shown as provided for the possibility of establishing multiple connections.

9. The machine may be used for other cryptanalytic purposes, for example, determining the cryptographic period of a message without finding repetitions and factoring the intervals between them. Suppose a message is suspected of having a cryptographic period between 7 and 15. Assuming a machine comprising 10 transmitters (with 9 counters), the message is prepared in 10 tape-copies. Copy number 1 is placed in transmitter number 1, with the first letter in the initial position; copy number 2, in transmitter 2 with its 7th letter in the initial position; copy number 3, in transmitter 3 with its 8th letter in the initial position; and so on. The

machine is started and that counter which gives the greatest total number of coincidences shows which tape is in the correct position as regards periodicity and this gives the period. For example, if the 1st counter gives the greatest total, the period is 7; if the 2d counter gives the greatest total, the period is 8, and so on.

10. Suppose it is desired to find the intervals between occurrences of a specific letter in a message, for example, A. The pins of transmitter 1 are locked in the "A" position, opening switch 38 in the tape-stepping magnet 3 of transmitter 1 at the same time; the message tape is placed in transmitter 2, and the machine is started. Only when an "A" occurs on transmitter 2 will the counter 13 be actuated. By inserting a counter in the circuit of magnet 9 of transmitter 2, the number of steps the tape makes before counter 13 is actuated will be shown. But the operator would have to stop the machine instantly and this would require sharp attention. By substituting a relay for counter magnet 13, and placing this relay in the circuit of the cam switch 11, the machine may be caused to stop automatically. The counter in the circuit of the tape-stepping magnet of transmitter 2 will then show the interval.

11. Other uses for the machine may develop as its flexibility and limitations become better understood.

WILLIAM F. FRIEDMAN,
Principal Cryptanalyst,
Signal Intelligence Section,
War Plans and Training Division,
Office of the Chief Signal Officer.

Washington, D. C.
April 15, 1937.

This invention was disclosed to us in February, 1937, by Mr. Friedman.

Rowlett
Miller
} Witnesses