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 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:

15 april, 1937

File: RAM-Comparators (1)

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, fof 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

whidh 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 2nd 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 8 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 Div.
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 (Witnesses
MILLER (