REF ID:A39507

8 Exp
M 1

Personal File on
Patent Application on Cipher Machine
Serial No. 157,383

W. F. Friedman

(This is the constantly-rotating commutator ~~control~~ machine)

SISDE-10

Patent No. 2,139,676 issued 13 Dec 38

Approved for Release by NSA on 09-30-2013 pursuant to E.O. 13526

REF ID:A39507

Brief Description of a Cryptographic Machine Employing a Single Cipher Commutator

By . Wm. F. Friedman

1. This invention deals with a cryptographic machine in which the cryptographic principle is basically as follows:

Power is delivered to the keyboard at the enciphering position at a specific instant in a period of 26 possible instants, the cipher resultant of a given plaintext letter depending therefore upon the specific instant the keyboard is made "alive", since for each of the 26 different instants a different mixed cipher alphabet is presented for encipherment. The order of presentation of cipher alphabets is regular but the exact instant of the selection of a specific cipher alphabet is very irregular and depends upon a keying factor.

2. The machine consists basically of a single, constantly rotating, 26 segment, 26 character cipher commutator, labeled 1 in Figure #1, controlled by a keying system including a set of rotatable, differential cam wheels or an equivalent electrical cam arrangement. This control system comprises 5 or a multiple of 5 cam wheels which operate contact levers, shown at 2. The inter-action of the 5 contact levers results in setting up at the 5 relays, 3, 4, 5, 6, 7, a permutation in the Bordeaux code. Corresponding to this permutation there is set up a permutation of 5 translater bars, labeled 8, 9, 10, 11, 12. These are slotted members and when a specific permutation is set up, one of 32 stunt bars falls into place and closes a contact. Several of these contacts are shown in the sketch at 13. These circuits lead to a switchboard 14, on one side of which there are 32 positions and on the other side of which there are only 26 positions. Referring to the cam wheels these are of different diameter and of different numbers of intervals, preferably all prime to one another. They are individually rotatable in step-wise manner, under control of thekeyboard. The potential cipher key which results from such an arrangement is in length the product of the individual interval numbers of the several cam wheels. For example, if there are 5 cam wheels the first of 100 intervals, the second of 99, the third of 97, the fourth of 91 and the fifth of 89 intervals, the total length of the cipher key would be 7,777,469,700. This merely means that the cipher key would consist of an unintelligible sequence of ciphering key characters of corresponding length.

3. The 32 possible resultant Bordeaux permutations which are led to switchboard 14 are for the purposes of this invention reduced to 26 by consolidating 6 of the 32 circuits into the other 26, so that there will be only 26 different resultant effects for cyptographic keying purposes. In this invention this is accomplished quite simply by taking what are usually known as the 6 extra functions and throwing them in with 6 of the other 26 letter-representing Bordeaux permutations. Which 6 will be selected to be "double-representations" can be determined and varied at will at the switchboard 14.

4. In this invention the 26 specific effects thus rendered possible by cam action merely determine which one of 26 segments will be made "alive" (that is, will be connected to a power source) on a set of 26 segments in the distributor head 15, over which brush 16 sweeps in synchronism with commutator wheel #1. As shown in the figure, this action merely means that at a given instant relay 17 is energized, the instant of energization being controlled by the cam arrangement and will be different for each key operation at the keyboard.

5. When a specific segment of the distributor 15 is made "alive" by being connected to a power source, and when the brush arm 16 reaches this live segment, the keyboard of the cryptograph is made "alive" at that instant by the completion of the circuit from power source 18 at contact 19. If a key is depressed during that cycle, the letter corresponding to that key will be enciphered in the specific cipher alphabet determined by the specific angular position of the cipher commutator #1 at the instant that the brush arm 16 reaches the live segment on distributor 15. In other words, the keyboard is made "alive" at 1 of 26 different instants in the cycle passed through by the commutator wheel; each of these instants corresponds to a different mixed alphabet of which there is a total of 26. It is to be understood that the cam wheel assembly is set at an initial keying position by pre-arrangement and that the cams advance one step or interval per depression of the keyboard and no more.

6. The cipher commutator may be made a reciprocal cipher commutator; or by suitable switching arrangements a nonreciprocal enciphering-deciphering relationship may be provided for, if desired.

7. The keyboard 20 is connected to the lefthand bakelite separator 21, and the circuits pass from 21 through cipher commutator #1 to the righthand bakelite separator 22 and thence to the bank of indicating devices 23, back to power source 18.

8. Means and circuits must be provided to prevent the cryptograph from recording or indicating a resultant more than once for the same set up of keys, so that there may be one and only one cipher equivalent per keying operation.

9. Instead of a set of 6 translater bars and 32 stunt bars an arrangement of multiple contact relays as shown in Figure #2 at 24 may be provided if deemed more practicable than translater bars.

10. For decipherment, having a reciprocal ciphering commutator the key setting of the cam wheels being the same as the initial setting at the enciphering end the sequence of keying characters would be identical at the deciphering end and the reciprocity between plain-text and cipher characters is established through the cipher commutator and the decipherment is effected in a simple manner, that is, if at encipherment at a given instant A equals K then in decipherment at that homologous instant (with respect to the cipher key) K would be deciphered as A.