Preliminary description of a single-commutator cryptograph suitable for War Department "restricted" or "confidential" communications.

1. This invention deals with a cryptograph in which the cryptographic principle is basically this: power is delivered to the keyboard at a specific instant in a period of 26 instants, the cipher resultant of depressing a given key depending then upon the specific instant the keyboard is made "alive", since for each of the 26 different instants a different mixed alphabet is presented. The order of presentation of alphabets is regular but the exact instant of selection is irregular.

2. The cryptograph consists of a single, constantly rotating, 26-segment, 26-character commutator wheel of the Hebern type, controlled by a control system including a set of rotatable, differential cam wheels. This control system consists of five or a multiple of five cam wheels which operate make or break contact levers and their action (by causing suitable interaction between sets of five cam wheels in case 10, 15, ... cam wheels are used in sets of fives) results in setting up five-unit code, Baudot resultants. The cam wheels are of different diameters, individually rotatable in stepwise manner, under control of the keyboard, the numbers of positions on the various cam wheels being preferably prime to one another so as to yield a resultant enciphering key of Baudot permutations, there being a total of 32 such permutations.

3. The 32 resultant Baudot permutations are carried, by means of a Baudot translator, or by means of a set of relays, into a "translation stage" where a specific permutation will set up a specific effect. Normally there would be 32 such specific effects, but for purposes of this invention

six of the 32 effects must be consolidated into the other 26, so that there will be only 26 different resultant effects for cryptographic purposes. In this invention this is accomplished very simply, by taking the six extra functions ("- + - - -", "- - + - -", "- - - + -","+ + + + +", "+ + - + +", and "- - - - -") and throwing them in with six of the other 26 letter-representing Baudot permutations. Which six will be selected to be "double representations" can be determined and varied at will by a suitable plug and jack arrangement.

4. In this invention the 26 specific effects thus rendered possible by cam action merely determine which of 26 segments will be made "alive" (that is, will be connected to a power-source) on a set of 26 segments in a circle over which a brush sweeps in synchronism with the commutator wheel.

5. When a specific segment of the element that is synchronized in its rotation with the commutator (the distributor) is made "alive" by being connected to a power source, and when the brush reaches this "live" segment, the keyboard of the cryptograph is made "alive" at that instant. If a key is depressed during that instant, the letter corresponding to that key will be enciphered in the specific mixed alphabet determined by the specific position of the cipher commutator at that instant. Thus, in other words, the keyboard is made alive at any one of 26 different instants in the cycle passed through by the commutator; each of these instants corresponds to a different mixed alphabet, of which there is a total of but 26. It is to be understood that the cam wheel assembly advances one step per depression of a key of the keyboard, and no more.

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

7. Means and circuits would be provided to prevent the cryptograph from recording or indicating a resultant more than once for the same set-up of key, so that there would be one and only one equivalent per keying operation.

Date of conception:
April 6, 1936.

William F. Friedman

William F. Friedman.