

ADDRESS ONLY
THE COMMISSIONER OF PATENTS
WASHINGTON 25, D. C.

DEPARTMENT OF COMMERCE
UNITED STATES PATENT OFFICE
WASHINGTON

All communications respecting
this application should give the
serial number, date of filing,
and name of the applicant.

Please find below a communication from the EXAMINER
in charge of this application.

Lawrence K. King

Commissioner of Patents.
MLL/cg

MAY 13 1933

Henry B. Stauffer
Army Security Agency
The Pentagon
Washington 25, D. C.

Division:

23 room 3616

Applicant:

William F. Friedman

Ser. No.

682096

Filed

July 25, 1933

For

CRYPTOGRAPHIC SYSTEM

GPO 16-27515-7

Responsive to amendment of May 28, 1948.

(1) The claims now remaining in the case appear to be 1 to 10, 12, 14 to 25, 35 to 39 and 41 to 50 all inclusive.

(2) The allowance of claims 1 to 10, 12, 14 to 25 and 35 to 39 remains unchanged.

(3) Newly inserted claims 41 to 50 are rejected as being anticipated by Hebern No. 1,633,072 of record. The reference discloses a plurality of elements in the form of a keyboard associated with signaling elements through the medium of a plurality of juxtaposed rotatable switching devices. Appropriate means for rotating the switching devices in the manner set forth in the rejected claims is also provided.

IN THE UNITED STATES PATENT OFFICE

IN RE: Application of	*	
WILLIAM F. FRIEDMAN	*	
Serial Number	*	Division 53
682,096	*	
Filed	*	<u>AMENDMENT</u>
25 July 1933	*	
For	*	28 May 1948
CRYPTOGRAPHIC SYSTEM	*	

* * * * *

TO: The Honorable Commissioner of Patents
Washington 25, D. C.

Sir:

This is in response to Patent Office action of 30 May 1945 in the above-identified application for patent. The case is being prosecuted under the so-called three-year rule.

Please amend the application as follows:

IN THE CLAIMS:

Claims 26 through 34, and 40 - Cancel.

Please add the following claims:

41. In a cryptographic apparatus of the nature described, the combination of a plurality of elements in the nature of a keyboard, a plurality of signaling elements electrically related to said first-mentioned elements, a plurality of juxtaposed rotatable switching devices interposed electrically between said elements of said groups to vary the electrical relations therebetween said devices bearing identifying characters on their peripheries, and electrical means for rotating said devices in stepwise fashion to produce aperiodic permutative relations among the characters on the peripheries of said devices.

42. The method of enciphering text consisting of textual characters which includes introducing a character to a cryptographic maze comprising a succession of cryptographic operations variable in stepwise fashion said maze having a plurality of inputs and outputs each character having its own input, varying the cryptographic maze in permutative stepwise fashion responsive to external aperiodic control means, and identifying the cipher equivalent of the said character by the relative position of its output among a plurality of outputs each cipher character having its own output.
43. The method of enciphering text consisting of characters which includes introducing a character to a cryptographic maze having a plurality of inputs and outputs the selection of an input depending upon the character itself each character having its own input, varying the cryptographic maze in permutative fashion responsive to external aperiodic control means, and identifying the cipher equivalent of the first-mentioned character by the relative position of its output among a plurality of outputs each cipher character having its own output.
44. The method of enciphering text comprising characters which includes introducing a character to a cryptographic maze including a plurality of cryptographic operations variable in stepwise fashion the steps being in interrelated succession the maze having a plurality of inputs and outputs each character having its own input, varying the steps of the cryptographic maze in permutative fashion in a succession determined by a combination of substantially unpredictable keying sequences.

45. The method of enciphering text comprising alphabetic characters by a succession of interrelated cryptographic steps under the control of a keying sequence of multiunit code groups which includes eliminating from the cipher resultant of said text any permutations of said code which have no equivalents in the alphabet being used by using said code only to vary in permutative fashion the aforementioned variable steps of the said cryptographic succession.
46. The method of determining the motion of the individual rotors of a series of cryptographic rotors which includes applying thereto aperiodic controlling impulses to provide a succession of unpredictable rotatory relations among the rotors.
47. The method of determining the motion of each cryptographic rotor of a series of such rotors which includes externally supplying an unpredictable succession of multiunit motion control code groups and utilizing said groups to control the displacements of said rotors in stepwise fashion.
48. The method of determining the motion of the individual rotors of a series of n cryptographic rotors in stepwise fashion which includes supplying an unpredictable sequence of n -unit motion control code groups the stepping of a rotor depending upon a predetermined impulse in each of said successive code groups.

49. The method of determining the motion of the individual rotors of a series of n cryptographic rotors in stepwise fashion which includes generating an unpredictable sequence of n -unit code groups the stepping of said rotors depending upon the arrangement of the impulses in said successive code groups.
50. The method of determining the motion of the individual rotors of a series of n cryptographic rotors in stepwise fashion which includes generating a plurality of unpredictable sequences of n -unit code groups, interacting the groups of said sequences group by group and utilizing the resultant groups to control the stepwise displacement of the rotors.

REMARKS

New Claim 41 is similar to several of the claims already allowed and appears to require no extended argument. The principal reason for the submission of this claim is to point out in more specific language than already appears the fact that the aperiodicity of the movement of the rotors or switching devices results in an unpredictable succession of rotatory keys.

Applicant cannot concede that method claims have no proper place in the present application, or, more particularly, that mechanical features are necessarily improper in method claims, or that a method claim need include an object upon which an operation is performed.

New Claims 42, 43, 44, and 45, however, while in essence like the original method claims have been changed completely in form and are now altogether devoid of mechanical limitations; further, each claim includes a textual character which is "treated" or "acted upon". New method Claims 46, 47, 48, 49, and 50 define methods for determining the motion of the rotors or other elements of a cryptographic maze. These claims likewise contain no mechanical features except the objects upon which the methods are performed.

Since the new method claims are directed to subjects matter which have long been in the application and since the rejections of the original claims have been on the basis of form rather than substance, it is assumed that no extended argument with respect to the new claims is necessary.

Continued prosecution under the so-called three-year rule is desired.

Reconsideration and favorable action are requested.

Respectfully,

WILLIAM F. FRIEDMAN, Applicant

By _____

His Attorney