~~SECRET~~

IN THE UNITED STATES PATENT OFFICE

In re application of:

WILLIAM F. FRIEDMAN and FRANK B. ROWLETT

Serial No. 70,412 Div. 53

Filed March 23, 1936.

CRYPTOGRAPHS

Filed July 20, 1939

AMENDMENT

Hon. Commissioner of Patents,

Washington, D.C.

Sir:-

In response to the official letter of July 27, 1939, amendment is made as follows:

Claim 1 line 5 change "to cause" to: connected to

Claim 1 line 5 change "to perform" to: for effecting

Claim 2 line 5 change "to cause" to: connected to

Claim 2 line 5 change "to perform" to: for effecting

Claim 9, change the period at the end of the claim to a comma and add: said electrical means constituting means energized by the output of said commutators to energize said devices as well as to move said commutators irregularly according to the irregularities of the output of the commutators.

Claim 10 change the period to a comma and add: the last-named means comprising means driven by the output of the commutators for moving the commutators.

Claim 13 line 6 cancel: "self-controlled"

Claim 16 line 4 cancel: "self-controlled"

Claim 16 line 8 change: "permit" to cause

Claim 18 line 7 cancel: "means to provide". Change "channels" to: circuits

Claim 18 line 8 after "contacts" insert a comma and after such comma insert: means activated by said circuits

Claim 19 line 5 cancel "self controlled". Change the period at the end of the claim to a comma and add: said means also including means controlled by the output of said commutators for effecting movement of the commutators.

Claim 21 line 4, cancel "self controlled". Remove the period at the end of the claim and add: and including means related therewith for moving the same according to a law dependent on the output of the commutators.

Claim 22 lines 4 and 5, cancel "self controlled"

Claim 23 line 5 cancel "self controlled"

Claim 27 line 8 change "instrumentalities" to: means

Add the following claims:

34. In the art of cryptography, the method of enciphering a message which includes establishing a cryptographic relation between the plain text and the cipher text for a first plain text character, and changing the cryptographic relation for a subsequent plain text character in a manner dependent on the said cryptographic relationship for said first character.

35. In the art of cryptography, the method of enciphering a message which includes establishing a cryptographic relationship between the plain text and cipher text for each of a series of the characters to be transmitted which relationship is changed for each character in a degree dependent upon the cryptographic relationship of preceding input and output characters.

36. Control commutating means comprising in combination, a plurality of commutators cooperating to successively produce irregularities in the text transmitted therethrough, an output end plate cooperating with one of said commutators, a series of terminals located on said output end plate for receiving energization

SECRET

from said commutators, and means connecting said terminals into a plurality of groups, each group including more than one terminal.

37. The combination, in a cryptograph machine, of a series of two or more commutators cooperating with each other to successively produce irregularities in the text transmitted therethrough, an end plate adjacent to the commutator at one end of the series, the commutator adjacent said end plate having two sets of segments, terminals in said end plate complimentary in number and position and cooperating with the respective segments in the commutator adjacent thereto, means connecting the first and second sets of segments of said end commutator in an irregular manner, the commutator at the end of the series opposite said end plate having only one set of segments, means cooperating with the commutator at the end of the series opposite said end plate for interconnecting the segments thereof, means feeding the input energizations to one of the terminals of said end plate, and means connecting terminals of said end plate together into a plurality of groups whereby to form an output.

38. In a system of cryptography, commutating means comprising a plurality of adjacent cooperating commutators, and plate means for feeding plain text energizations into one end of said commutating means and for receiving the scrambled text from said commutating means, a plurality of devices, one for each of said commutators respectively, each such device including means to rotate its respective commutator when the device is energized, second commutating means having its input energized and having a plurality of groups of output terminals, one group for each of said devices, said second commutating means including means for energizing said groups of output terminals in irregular fashion, and a plurality of means respectively responsive to energization of said groups for respectively energizing said devices.

REMARKS

This is a "three-year" case and consequently this amendment is

a seasonable response to the official letter of July 27, 1939. All 33 claims remain in the case.

The official letter of July 27, 1939 states that the claims are rejected on the art as previously applied. A study of the record indicates that claims 1, 2, 9, 10, 12, 13-16, 18-23, and 27 were previously rejected and a response to that rejection is contained herein.

The examiner in his letter of July 24, 1936 rejected all claims on the ground the structure and function of the universal bar is insufficiently disclosed. If applicant overcomes this ground of rejection it is then apparent that claims 3-8, 11, 17, 24-27, and 28-33 which have not heretofore been rejected on any ground other than inadequate disclosure are apparently allowable.

The term "universal bar" has a recognised meaning in the art and accordingly a detailed description of the function and mode of operation of a universal bar is not believed necessary. As was said by the Supreme Court in Webster Loom Co. v. Higgins, 105 U.S. 580, 586, and also in Carnegie Steel Co. v. Cambria Iron Co. 185 U.S. 403, 437: "that which is common and well known is as if it were written out in the patent and delineated in the drawings."

The applicant has amended the remaining claims in an attempt to conform to the examiner's views. If the examiner has ideas on specific changes of wording or showings in the drawings and desires to suggest any changes in wording or showings, applicant will be glad to receive the suggestions.

The claims are all thought to be patentable since the references do not use the output of their commutators to control the movement of the commutator but the keys themselves control the commutators. The cryptographic security of applicants' construction is therefore very much greater. This is one of those cases often found in patent matters where a simple change effects marked improvement in results - in this case a marked increase in cryptographic security. The claims call for a double function of the commutating means, one function to move the commutating means and another function

is to code the message. Moving the commutating means in an irregular fashion depending upon the cryptographed output of the commutating means is not found in the cited prior art patents.

Method claims 34 and 35 differ from the art cited by the examiner in that cryptographic relation for subsequent plain text characters is changed in a manner dependent on the cryptographic relationship of the character transmitted. New claims 36 and 37 relate specifically to the control commutator per se of Figure 2, in which a plurality of commutators are connected together. New claim 38 relates to a combination of a control commutators that respectively control the movement of the several commutators that constitute the main commutating means. Therefore claim 38 is patentable for the same reasons as claims 1-33, inclusive.

Respectfully submitted

William D. Hall
Attorney for Applicant