IN THE UNITED STATES PATENT OFFICE

In re application of
William F. Friedman,
Serial No. 300,212,
Filed Oct. 19, 1939,
Cryptographic Device

Div. 53, Room 6897

May 7, 1940.

Hon. Commissioner of Patents,

Sir:

Responsive to Patent Office action dated Nov. 9, 1939, it is desired to amend as follows:

Claim 1, line 2, before "channel" insert - - horizontal - - , also cancel "and" . Same line cancel "of character-bearing material " and insert - - provided with discrete sequences of equally spaced alphabetic characters - - . Line 3, cancel " in respect to each other " and substitute - - independently of one another ; - - . Cancel lines 4 and 5 and for the cancelled subject matter substitute - - and means for facilitating the reading of said characters in selected columns. - - .

Claim 2, line 2 before "channel" insert - - vertical - - , Same line cancel "character-bearing " and substitute - - individually adjustable - - . Line 3, before "adapted " insert - - bearing discrete sequences of equally spaced alphabetic characters - - . Line 5, cancel "aligning the characters " , also cancel all of lines 4 and 5 and for the cancelled matter insert - - facilitating the reading of said characters in selected columns and in different relations for cryptographic purposes. - -

Claim 3, line 2, before "grooved" insert - - horizontally - -. Same line, cancel "character bearing " and substitute - - individually adjustable alphabetic - - . Line 3, cancel " for aligning said characters " and substitute - - to facilitate the reading of selected alphabetic columns - - .

Claim 4, line 3, cancel "slidable " and substitute - - individually movable - - . Line 4, cancel "for aligning " and substitute - - to facilitate the reading of - - . Lines 4 and 5 cancel " and in column formation " .

Claim 5, lines 1 and 2 cancel "open-ended " and substitute - - vertically - - . Line 3, before "slidable" insert - - individually - - . Line 4, cancel "aligning " and substitute - - facilitating the reading of - - . Line 5, cancel " and in column formation " .

Claim 6, line 2, cancel "character-bearing" and substitute - - alphabet bearing - - . Line 3, cancel "slidably" and substitute - - individually - - .

Claim 7, line 5, before "slidable" insert - - individually - - . Lines 5 and 6 cancel " , and means to permit said rule " and insert - - adapted - - . Lines 6 and 7 cancel "across the channel ways in cryptographic relation to said strip ; " and substitute - - of said strips to facilitate the reading of selected sequences of characters in varying relations for cryptographic purposes ; - - .

Claim 14, line 5 before "slidable" insert - - individually - - .

Claim 15, line 6, cancel "permit" and substitute - - facilitate - - .

Claim 16, line 5, cancel "permit " and substitute - - facilitate - - .

Claim 17, line 6, cancel "permit alignments " and substitute - - facilitate reading - - .

Claim 18, line 6, cancel " permit alignments " and substitute - - facilitate reading - - .

Claim 19, line 3, cancel "open-ended " . Line 8, cancel "permit alignments " and substitute - - facilitate reading - - .

R E M A R K S

Reference is made to a personal interview with the Examiner in charge of this case under date of May 2, 1940, the courtesy of which is hereby acknowledged. Attention is called to the fact that this application is filed under the Act of 1883 as amended April 30, 1928 and the Government holds the usual license under the application. It is therefore requested that the requirement for division be waived in accordance with the practice applying to Government cases. In this connection citation is made of the McCandless patents Nos. 1,925,149 of Sept. 5, 1933 and 1,960,454 of May 29, 1934, in which this procedure was followed. Another precedent is the ruling of the Classification Examiner based on an unpublished Commissioner's order mentioned in Office Action of April 8, 1936, (see Butler application Serial No. 573,011, Div. 18 ). It is in accordance with the understanding had with the Examiner upon the occasion of the interview that the divisional requirement will be waived under the existing practice.

Discussing the references cited against the claims, in connection with the Nicoletti patent it is desired to point out that this is a cipher device for accomplishing transposition of letters whereas applicant's device is for accomplishing substitution. These are two basically different cryptographic processes. In Nicoletti no plain text or cipher text letters are set up at all, the device merely yielding a table "providing rules for dividing into various assemblage the letters forming the message or writing to be ciphered, " . In connection with the structure of the Nicoletti device,

it will be noted that the transverse member e is a fixed part of the frame and is not movable transversely of the strips in the manner of the guide rule of the present invention.

Referring to the patent to Grassi, it will be noted that in this device by reference to page 1 of the specification, lines 24 to 31, that " the original word it is desired to transpose into code form is spelled across the columns, having one letter of each column, and the corresponding code word appears at a predetermined distance away from the point where the original word appears, said code word also having a letter of each column . " At this point it is desired to call attention to an important distinction which differentiates applicant's device over the Grassi device, as well as others of the citations : In the art cited there is a definite and unvarying relationship between the plain text and equivalent cryptographic text as to distance separation between these components. In this case this relationship is variable and subject to the random choice of the operator. As will be apparent, the feature as it appears in Grassi and in similar prior art cases constitutes a fundamental cryptographic weakness that renders the device extremely insecure. Moreover in this Grassi structure, it will be impossible to provide for the shifting about of various sections, which feature is covered by claims 8 to 19. Also in Grassi, the sequences are limited to arrangements in which vowels must occupy definite places in the sequences.

In the case of Gentet, the alphabets are composed of definitely fixed sequences, and the only thing which can be done in this instance is to couple and uncouple these alphabets in pairs. Also, there is a fixed and unchangeable distance between the plain text and the cipher text. Cryptographically this is a weaker system than applicant's device.

In the cited British patent No. 12,005, the invention is purely a device for converting code numbers into letters, and not for enciphering plain text. Also, distance between the plain and cipher lines is fixed.

In the case of British patent No. 23,204, the invention is very similar in principle, if not identical, with the previously discussed patent of Gentet.

As to the Mitchell patent and other citations of record, it is pointed out that none of these are cipher devices at all and they do not appear to have any pertinence.

Emphasis is placed upon the important function of the guide rule or means of aligning which really is to facilitate the reading of the characters in selected columns. The claims have been amended where necessary to express this function more exactly ; and in all cases where the indefinite term "permit" or "means to permit " had been used, the amendment has been made to overcome the Examiner's objection.

With respect to the structural arrangement of applicant's device to provide for the removal and rearrangement of various sections, it does not appear that any of the prior art citations disclose this advantageous feature. Williamson cited in this connection is not a cryptographic device but merely a device for teaching arithmetic. Therefore the sectional feature cannot be regarded as having any equivalent function as that forming part of the present invention.

Favorable reconsideration is requested of claims 15 to 19 inclusive, in view of the amendments directed in said claims to define positively the advantageous function of the guide rule, which in the present invention, accomplishes something not possible by the art cited where the line indicator is stationary.

Favorable reconsideration of the claims now presented is courteously requested in the light of the foregoing.

Respectfully submitted,

'illiam F. Friedman,

By:

Attorney