~~RESTRICTED~~

5 June 1951

Rear Admiral Earl E. Stone, Director
Armed Forces Security Agency Council
3801 Nebraska Avenue
Washington, D. C.

Dear Earl:

I am inclosing a letter from General Corput and a prospectus concerning a cryptographic device which apparently is capable of a high degree of security.

It is considered that AFSA may be interested in obtaining test equipments and might even consider proprietary rights. If the EUCOM Signal Division can be of any assistance, I will be pleased to act as intermediary.

Sincerely,

W. T. GUEST
Brigadier General, USA
Chief, Signal Plans & Operations Division

2 Incls
1. Ltr fm Gen Corput,
   1 Jun 51
2. Ltr fm Col Cowles,
   15 May 51, w/prospectus

~~RESTRICTED~~

The composition of the crypto-impulse combinations varies from sign to sign and the series of these variations is to all practical purposes limitless. If one f.i. would always strike the key "A", then the ciphered impulse combinations in the line would change continuously.

Fig. 3 illustrates as an example the transmission of the letter "Y", according to the 5-pulse code. 1 - 5 are the five elementary impulses, + when current and - no current.

Line 1 shows the impulse combination, produced by the telewriter, line 2 shows a crypto impulse combination, in this example the combination for the letter "L" . In the line 3 multiplied product of lines 1 and 2 is obtained of the elementary impulses. The conversion is done according to the following rule of a multiplication

+ . + = + + . - = -

- . - = + - . + = -

It will be seen as a result of the ciphering operation that the letter "C" is obtained in this case. If the line is tapped with a telewriter (without telecrypto), there will be obtained the letter "C" instead of "Y" .

From the lines 4 - 6 will be seen that the original sign combination, as produced by the sending telewriter, will be reconstituted by the multiplication of the ciphered impulse combination with the corresponding crypto impulse combination.

5-pulse system.

As practically all the possible different impulse combinations in this system stand for signs (letters, numerals, punctuation signs), the ciphered impulse combinations will give readable signs during transmission. The action of the telecrypto apparatus consists in this case of the exchange of signs : The letter "Y", for instance, as written on the telewriter, may be exchanged for an "C" as shown in the example above. A person, who taps the line and has no knowledge of the crypto impulse series employed, will thus obtain letters and numerals in an absolutely arbitrary sequence.

14-pulse system

With the 14-pulse system about 16'000 impulse combinations can be obtained; of these only about 50 combinations (= 0,3%) give readable signs. By the conversion of the clear text combinations with those of the crypto series, there will generally be obtained unreadable impulse combinations in the ciphered impulse series, so that an "λ" may for instance be changed into ⇱ etc. A telewriter, branched on to the communication channel, and not equipped with a telecrypto apparatus, will here write unreadable signs.

D. The ciphering keys

The keying elements of the ciphering key serve to obtain the variable crypto-impulse series. As elements for the ciphering keys a number of wheels (f.i. 14) are used. These pin wheels carry a number of slidable or rotatable pins, which can be displaced individually, by hand, and can take two different positions. In one of these positions one or several contacts will be closed (or opened), and vice versa in the other position. Each pin is defined by a number on the circumference of the pin wheel (key number). These key numbers are also used to define the starting positions of the pin wheels. An operating mechanism acts on the pin wheels and moves them after each transmitted sign, in an irregular manner. The movement rhythms can be varied and can be changed arbitrarily by hand.

The pin wheel contacts are connected in accordance with a special system. The connections terminate at a collector, which has five sectors for the 5-pulse system and 14 sectors for the 14-pulse system. The individual segments are either electrically activated, or not, depending on the position of the pin wheels. When a collector brush passes all segments, a 5-pulse or 14-pulse combination, or the so called crypto impulse series, is obtained.

An exceedingly complicated "program" for the composition of the crypto impulse series is obtained on account of the system used for the connection of the pin wheel contacts. If f.i. the first impulse element gives "current" or not may depend on the position of up to 12 pin wheels, and their position at that moment is dependent on the combinations used for the movement of the pin wheels up to that moment.

Additional keying elements are also used, in the form of ciphering (permutation) collectors, of which one is always supplied. This is adjustable by hand. On special demand one or two extra ciphering collectors, which obtain the same irregular kind of movement as the pin wheels, are also supplied.

The ciphering collectors are marked on their circumferences with numerals in order to define their starting positions. There are also supplied special connector plates, which can be exchanged in a very simple way.

The pin wheels and the two ciphering collectors with automatic movements PS 1 and PS 2 (Fig. 4) are mounted on a shaft at the front end of the apparatus, while the hand operated ciphering collector PS 3 is to be found at the right hand side of cover of the machine.

E. Composing the ciphering key settings.

We distinguish between interior and exterior settings. The interior settings are changed more or less frequently, depending on the intensity of the crypto service, while the exterior settings are composed when starting a communication series, or eventually every time a telegram is sent.

The TKG 5/14 allows the following key settings :

a) Interior key settings.

1. The positioning of the pins on the pin wheels, which total about 500.
2. Arbitrary arrangement of the movement program for the 14 pin wheels and the two ciphering collectors.
3. The choice of different connection plates for the ciphering collectors.