STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO : 00T
Thru : 41, 04T, 04
FROM : 412

DATE: 15 June 1951

SUBJECT: Telecrypto and Cryptex Model CI

1. Inclosed herewith is a report "Brief Security Estimate of Telecrypto", as requested.

2. Also inclosed are comments on Cryptex Model CI.

3. Mr. Hagelin's letter is returned herewith.

R. H. SHAW
Head, AFSA-412

Inclosures - 3
1 - Brief Security Estimate of Telecrypto
2 - Comments on Cryptex Model CI
3 - Letter from Mr. Hagelin [filed in Hagelin correspondence. Aug 5, 1950]

AFSA-412B/egb
15 June 1951

BRIEF SECURITY ESTIMATE OF TELECRYPTO

1. Telecrypto is a key generator using the M-209 pin wheel assembly (which steps as in M-209), 4 key cylinders and 12-bar drum. The key cylinders are stepped erratically by the teeth on the 12 bars of the drum which in turn are slid by the interaction of the pins and lugs. The selection of which key cylinder is to be used is controlled by a second reading position on 3 of the pin wheels.

2. AFSA 412B conducted a week's intensive security study of Telecrypto. This paper is a summary of the results of that study.

3. Cryptographic Requirements.

a. Daily Key. - Telecrypto has many variables that must be set daily, thereby creating many chances for operator error. The system, being a teletype system, does not permit easy checking. The daily set-up published in a key list would have to contain the following:

(1) Daily pin and lug set-up.

(2) Daily setting of 128 plugs, 32 on each of four cylinders.

(3) Daily setting of 4 "A" plugs between the cylinders and the selectors.

(4) Daily setting of 3 "B" plugs to choose the three selector pin wheels.

The lug set-ups must be carefully made up in order to assure 1 to 6 steps for each cylinder per half-turn of the drum, i.e., per operation of the machine. The fixed teeth in the model in the diagrams are probably not the best arrangement possible but no matter what arrangement is used, lug patterns must be carefully derived.

b. Message Alignments. - For each message the pin wheels and cylinders must be set. If the cylinders are set for each message, there is a chance for off cylinder situations to occur which may lead to reconstruction of the machine variables. To avoid such occurrences, the cylinders could be zeroized for each message. But this also leads to a bad situation because, if the cylinders are set the same at the beginning of each message, the cylinders will step in and out of phase between messages, since all cylinders step at approximately the same rate. This situation could become very dangerous. Therefore, either solution is undesirable.

Inclosure 1 to AFSA Serial _____ dated _____.

Inclosure 1 to AFSA Serial _____ dated _____.

6. Summary. - Telecrypto requires too much set-up time for it to be practical for use by the U.S. Armed Forces. ASAM 2-1 is less vulnerable to cryptanalytic attack so that Telecrypto would not be any improvement over the comparable system now in use.

Inclosure 1 to AFSA Serial _____ dated _____.

~~TOP SECRET~~

AFSA-412B/egb
15 June 1951

COMMENTS ON CRYPTEX MODEL CI

1. Cryptex, Model CI is similar to Telecrypto but differs from it in the fact that the pin wheel assembly in Telecrypto is the same as M-209 and in Cryptex, Model CI is similar to the modified Hagelin with erratic stepping. The paper on Cryptex, Model CI is dated 5 August 1950 and therefore may be a forerunner of Telecrypto. Perhaps there were difficulties in its manufacture with the more complicated erratic motion.

2. The security studies recently carried out by AFSA-412B were all on Telecrypto.

The set-up time for Cryptex, Model CI and its liability to operator error would be the same as Telecrypto. This time alone would appear to make the system impracticable.

~~U.S. EYES ONLY~~

Inclosure 2 to AFSA Serial _____ dated _____.

~~TOP SECRET~~