File

G-4's copy

~~CONFIDENTIAL~~

(COPY)

OP-20-GY

1 April, 1938.

Copied 11/24/42 ?

MEMORANDUM.

1. I should like to propose the following method of mechanizing the processes of (1) decoding messages, or (2) entering newly recovered values in messages during the progress of cryptanalysis, when a considerable amount of material is involved.

Mechanical Decoding.

2. The apparatus required consists of the following items of standard International Business Machine equipment:

Punch,
Sorter,
Reproducer,
Collator,
Tabulator.

Preparation.

3. Messages to be decoded are filed in any desired order, preferably chronologically. They are then considered, for purposes of punching, one single message. The messages, including headings and other desired data, are now punched on cards. Only one code group is punched on a card. As the cards are punched, each successive card is assigned a successive number in a single series. In other words, if there are 100,000 cards the first card of the first message will be 000001 and the last card of the last message will be 100000. Cards used for headings and other data will also be numbered according to their position in the series.

4. All the cards containing code groups are now sorted by code groups using the lower zone punches only. Sorting in this manner is equivalent to considering the code groups as numbers and sorting thereby. It is done thus to simplify sorting and to permit using the collator later on. This set of cards is called the Message File.

5. A card is now made up for each code group whose value has been recovered. This card contains the code group, the recovered value, and an "X" punch. The code group should occupy the same field on the card as the groups on the message cards described above. These cards with recovered values are next sorted in the same manner as the message cards above, i.e., by code groups using the lower field only. They will then be in the same code group order as those of the message file. This set is called the Decoding File.

Decoding.

6. To decode the traffic, the message file is placed in one hopper of the collator and the decoding file in the other. The machine is wired so that as the two sets of cards pass through the machine every message card for which there is a corresponding decoding card will be selected out of the message file. At the same time every decode card for which there is a message card will also be selected out of the decode file. The decode cards and message cards thus selected are then placed in the reproducer. Using the "X" punch for control, the recovered value on each decode card can now be reproduced on all corresponding message cards.

7. Having all recovered values entered on all corresponding message cards, the latter, together with heading and other message data cards, may now be sorted back into message form by means of their serial numbers. This done, the cards are ready for printing on the Tabulator.

Procedure During Cryptanalysis.

8. The same procedure as above is followed except that it must be repeated periodically as solution progresses. Under ordinary circumstances it is believed that fresh work sheets with all new values entered to date could be prepared at least weekly.

/s/ J. N. Wenger

(Shown to Friedman on 10
May, 1938)

J.N.W.