Note on Early Bombe History

by

Unknown

Probably
Commander Howard T. Engstrom

Source: NR. 1736, CBLH17, Box 705,
ENIGMA (Conferences, Theory, Related info),
NARA, RG 457, NSA Historical Collection

Editor: Frode Weierud

CBLH17
Box 705
35701, NR.1736

SECRET

SECRET

Bombe N.530 Proj

11 October 1943.

Cryptanalytic problems connected with German communication intelligence (differ from the Japanese in that Germans use a cipher machine called the Enigma Cipher Machine) almost universally for their military and naval communications, while the Japanese use a number of varied systems. The German Enigma Cipher Machine is a wire wheel machine using three or four wheels and an almost metric motion. Here we have one of the very old models. ~~The cryptanalysis of the simple Enigma machine has been studied extensively by the Poles, the French, and the British.~~ Methods of solution for the simple form of the enigma cipher machine consist essentially in assuming a word for a given portion of cipher text and trying all possibilities for settings of the machine to determine where the assumed output emerges as the given cipher text. This procedure has been handled in various ways. The original method consisted of cataloging the output of the cipher machine for each position. This catalogue can then be readily used to determine the required setting. A second method is to make use of the Enigma Machine itself (a version of which we have assembled) in a search for position. Since the search is a simultaneous one for as many successive positions as is contained in the known word, either ~~this many~~ several Enigma Machines must be run synchronously or some sort of device attached to a single machine which will "remember" this number of successive positions. The former method was first used by the Poles who have studied the German machine system. Such a bank of Enigma Machines now has the name "bombe". This term was used by the Poles and has its origin in the fact that on their device when the correct position was reached a weight was dropped to give the indication. Both the catalogue and the bombe methods were successful for the simple ENIGMA machine.

SECRET

S E C R E T

The Germans apparently appreciated the fact that the simple Enigma machine was susceptible to attack by this method of trying everything, since about 1938 an Enigma machine was introduced which carried a plugging arrangement, called a "stecker," which could be changed daily or oftener. This made the catalogue and the simple bombe of no use in the solution. In early 1939 Dr. Welshman, a British cryptanalyst, proposed a scheme for modifying the bombes which would break the stecker Enigma. The proposal of Dr. Welshman was at first rejected because of an estimated cost of 8,000 pounds. After considerable delay, no other solution appeared and the first modern bombe was constructed about 1940. It was immediately successful for the then current Enigma machine and is still in use. Since that time there has been no interruption of British bombe production. Two factories in Britain are devoted exclusively to this project. The task assigned to the bombe has steadily become more complex. The Germans continue to add at intervals new keys, new wheels, and more complications. In view of the fact that this solution of the Enigma was the source of practically all German cryptanalytic intelligence, the British have regarded this work as the most secret enterprise connected with the war effort. The First Lord of the Admiralty has said that the destiny of the British Empire depended on its security. Because of its tremendous significance, the British did not inform us of their work until after Pearl Harbor. Research by U.S. Navy cryptanalysts had proceeded in similar channels. Knowledge of the bombe technique had come to us ~~from~~ in piecemeal fashion. In June 1942, overcoming British reluctance, Admiral Redman and Commander Wenger made ~~the decision~~ a strong recommendation in view of the submarine menace in the Atlantic that the U.S. Navy ~~should~~ enter the field. Shortly prior to this time, German Navy introduced an extra wheel into their machines which made

the British bombes inadequate for handling the ~~naval~~ German submarine traffic. The problem which Admiral Redman presented was that of developing a high speed bombe for the four-wheel machine and of producing enough of them quickly to handle the naval situation. In order to bring about solution, the Bureau of Ships established the Naval Computing Machine Laboratory at Dayton, Ohio, under the direction of Lieutenant Commander R. I. Meader, USNR. ~~Joseph R. Desch, Head of the Electrical Research Laboratory of the National Cash Register Company, was designated Civilian Chief. At about this time Lieutenant R. B. Ely, USNR, now Lieutenant Commander, and Lieutenant (jg) J. J. Eachus, USNR, now Lieutenant,~~ two Naval officers were sent to England to investigate and report on the British machines. Their reception was entirely cordial and all technical details made available to the USN through these representatives. The first American machines made to solve the German Enigma traffic were placed in operation in April 1943 at Dayton. Forty of these machines have now been ~~delivered~~ completed and are in operation here. Between the American ad British machines, it has been possible to meet the various complications which the enemy has introduced and to read the submarine traffic with a high degree of currency. The production of these machines has been a constant battle concerning priorities ~~being~~ always hampered by the fact that the purpose of the machines had to be kept ~~so~~ secret from the various agencies controlling priorities.

The machines which you will see here do the following:

(1) Input
(2) Process
(3) Output
(4) How utilized
(5) Knowledge produced is disseminated