(U) History Today - 15 August 2012

FROM: Center for Cryptologic History | Run Date: 08/15/2012

(U) In 1941, when the Japanese attacked Pearl Harbor, the U.S. was unable to read Japanese army codes. Due to limited budgets and manpower, William Friedman and his band of army cryptologists were limited in the range of systems they could work and, in any case, little intercept of Japanese Army communications was available. Throughout the 1930s they worked and had great success breaking and reading Japanese diplomatic ciphers. With the great expansion of the Army cryptologic organization at the start of World War II, and greater availability of intercept, U.S. Army cryptanalysts turned their attention to the Japanese army code.

(U) The Japanese army code was a challenging problem. It was a book-based hand encipherment system. First, each word of a message was transferred into a four-digit number taken from a codebook. Next, each four-digit number in the message was enciphered by using an additive table, that is, a list of random numbers. The next available numbers from the additive table were added -- in noncarrying addition -- to the four-digit numbers in the first draft of the message. The product of this addition became the message. This system proved to be an effective encryption method.

(U) U. S. cryptanalysts were never able to break low-level Japanese army communications. It was difficult to get enough intercept because the Japanese used low-power transmitters. Also, these armies communicated vertically rather than laterally. Therefore, if the 78th Regiment wanted to get a message to the 79th Regiment, it had to send it to the 20th Division, which then sent it to the 79th Regiment. The response from the 79th Division went back to the 20th Division, then to the 78th Regiment. This cumbersome system was further complicated because each regiment had its own code.

(U) Ironically, higher-level Japanese army communications were less secure. Japanese area armies expanded rapidly and could not use low-power transmitters because of the distance that they covered. Rapid expansion made more communication necessary, which gave the Americans more to study.

(U) The U.S. read its first Japanese Imperial Army message in September 1943. By February 1944, the U. S. was decrypting 20,000 Japanese army messages per month. This was indeed a remarkable achievement.

(U) A Japanese Army codebook is on display in the National Cryptologic Museum.

Approved for Release by NSA on 06-27-2013, FOIA Case # 68827

(U) The photograph shows a training class for analysts at Arlington Hall Station, where much of the strategic Japanese traffic was worked.

(U) Like to blog? Want to discuss historical topics with interested -- and interesting -- folks? Visit the Center for Cryptologic History's blog, "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Comments/Suggestions about this article?