Doc ID: 6660639

UNCLASSIFIED

(U) HISTORY TODAY - April 14, 2016

FROM: CCH
Run Date(s): 04/14/2016

(U) **Captain Solomon Kullback, USA – Decrypting Japanese Army cryptosystems in WW II**

(U) In a rambling interview late in his life, Solomon Kullback, who had led the U.S. Army effort against Japanese Army cryptosystems in World War II, noted with great satisfaction how thoroughly the U.S. had penetrated Japanese Army codes and ciphers. (The U.S. Navy also had outstanding success against Japanese Navy systems, but Kullback was not conversant with those.)

(U) Kullback noted that toward the end of the war, the Japanese were sending details about their cryptographic procedures and changes to them in systems the U.S. could read.
(U) Both the Japanese Army and Navy used encryption methods that were already antiquated by the time of World War II. Both enemy services used some machine encryption devices, but, for most of their communications, depended on code books. Code books were nothing more than lists of words likely to be used in messages; next to each word in the code book was a substitute for the word, usually a four- or five-digit number. When encrypting a message, the Japanese code clerk would substitute the number for the actual word, then disguise the number through use of an additive table or an enciphering square.

(U) Kullback noted: "[T]owards the end I think they were changing the enciphering square every five days or maybe they got it down to changing it every day. [T]hey were beginning to get more and more concerned about the security of their system, [but] they had so many isolated units that they couldn't distribute information [by submarine] so that they were sending them these messages. That was a big help to us."

(U) CPT Solomon Kullback, USA

(U) Throughout the war, Japanese messages often reported the movement of cryptographic systems to outposts in the central and south Pacific. Sometimes U.S. forces were able to interdict the material, as in the case of the *Yoshino Maru*, reported in this *History Today* of February 11, 2016.

(U) Messages often gave the dates when codebooks, additive groups, and discriminant values would go into effect. U.S. cryptanalysts were well forewarned. Messages also sometimes included instructions on encoding and decoding procedures. This indicated to the U.S. analysts that some Japanese units were forced to use untrained personnel, or that there had been many mistakes committed by deployed Japanese units using the systems to report to their headquarters. Ann Caracristi, a cryptanalyst during the war, noted in an interview that U.S. understanding of the Japanese systems was so thorough that U.S. Army analysts could reconstruct a garbled message and gain the intelligence, whereas the intended recipient, a Japanese commander, had to ask for a retransmittal of the message.

(U) In December 1944, Central Bureau, the cryptologic bureau that supported Allied efforts in the Southwest Pacific, noted in a wrap-up report that in early December they had solved an encrypted message that contained actual additive values for Japanese cryptographers. The message contained

a complete additive square for encrypting messages. Another Japanese message gave instructions for future construction of encryption squares.

(U) Analysts at Arlington Hall and at Central Bureau were painstaking in their reconstruction of Japanese codebooks and additive tables. It paid off.

(U) Kullback recalled another example. “I remember on one occasion they wanted to change the key book, a 500-page book with squares [of] 10 four-digit groups across the row, with scrambled up numbers on the side... but they had difficulties in distributing it.... [W]hat they were told to do was to compile a new key book out of their existing key book by adding; for example, [taking] page one and page two, add[ing] the digits, and get[ing] a new page one. [T]hen they take page two and three and add the digits and get a new page two, and go through the key book, so it would end up, in effect, a new key book. [I]f nobody knew what the old key book was, it would, in effect, be a problem of solving it all over again. But, fortunately, we had the old key book, we read what they were doing, [and] we were able to compile [the new one], so when they changed the key book, there was no problem....”

(U) The reports issued by Arlington Hall and Central Bureau on all these cryptanalytic bonanzas were of great benefit to U.S. and British cryptanalysts working Japanese traffic at all other locations.

(U) In peacetime, Captain Solomon Kullback was a civilian employee of the Army with a commission in the reserves. He was called to active duty during World War II and rose to lieutenant colonel.

(U) To discuss historical topics with interesting folks, visit the Center for Cryptologic History's blog, History Rocks ("go history rocks").
(U) Have a question or comment on *History Today*? Contact us at DL cch or [redacted]

Information Owner [redacted]
Page Publisher [redacted]
Last Modified: April 13, 2016
Last Reviewed: April 13, 2016

~~DERIVED FROM: NSA/CSSM 1-52, DATED: 20130110, DECLASSIFY ON: 20430110~~
UNCLASSIFIED

(b)(3)-P.L. 86-36

[redacted]