Doc ID: 6660671

UNCLASSIFIED

DAILY ENTERPRISE

(U) HISTORY TODAY - October 20 , 2015

FROM: CCH
Run Date(s): 10/20/2015

(U) A look back: World War II and German diplomatic communications -- FLORADORA

(U) During World War II, British and American cryptanalysts made limited breaks into a German diplomatic system known as FLORADORA. As German diplomatic communications began moving to use of one-time pads, unbreakable in theory, knowledge of FLORADORA helped in exploitation of the pads.
(U) The principal enabling factor behind the success in both the UK and the U.S. was the serendipitous acquisition of German keying material.

(U) A British landing party in Iceland in 1940 found that officials in the German consulate in Reykjavik had abandoned the city after burning secret documents. However, not all the documents had burned completely, and the landing party was able to recover remnants of a code book, additive keys, and documents on the indicator system. Study of these captured materials began about a year later.

(U) These materials gave promise of a break into the system, but the analysts at the Government Code & Cypher School (GC&CS) needed one additional item, daily indicator keys.

(U) A kind fate again came to their assistance.

(U) The director of the GC&CS team that analyzed German diplomatic traffic, Alastair Dennison, received a package from the British consul in Lourenco Marques, capital of Portuguese Mozambique. A cover letter stated that a sailor (presumably somebody hired to make a delivery for the Germans) had dropped the package at the British consulate, mistaking it for the German consulate. The package contained 90 days worth of daily indicator keys.

(U) Historical photo: The building at Berkeley Street in London, where the German diplomatic problem was worked by the Government Code & Cypher School (GC&CS) during World War II.

(U) Although it was expected the Germans would not use these keys once they discovered them missing, the keying material continued in use.

(U) In the assumption that FLORADORA traffic would never be exploitable, GC&CS had destroyed its files of intercept. However, Arlington Hall, the U.S. Army's cryptologic headquarters, had not disposed of its holdings, and the material was sent to GC&CS.

(U) This sharing led to fruitful cooperation between the two countries on this challenging problem, just as they were working together against other German and Japanese military communications. William Filby, a principal analyst on German diplomatic traffic at GC&CS, worked closely with Solomon Kullback from Arlington Hall. The British concentrated on Berlin's diplomatic messages to Dublin, while the U.S. worked on messages to Tokyo. When some breakthroughs were made, as Filby wrote years later, Kullback "flew over to join in the fun."

(U) Historical photo: The building at Berkeley Street in London, where the German diplomatic problem was worked by the Government Code & Cypher School (GC&CS) during World War II.

(U) GC&CS concentrated on Dublin because the German consulate there was running out of key, and the Germans believed it was too dangerous to try to send packages of new material. The Berlin-Dublin communications reused existing key by manipulating the order of the digits on the key sheets, but this was easier for analysts to exploit than continually new key.

(U) With these recoveries, the analysts solved messages with the same text that had been enciphered in FLORADORA for Dublin but on one-time pads for transmission elsewhere. After laborious effort, the analysts were able to determine that the Germans generated their one-time pads with a complex pattern -- but it was a pattern that could be analyzed, it was not truly random generation.

(U) At Arlington Hall Station, U.S. analysts were sorting German diplomatic traffic to isolate FLORADORA, which could be exploited, and disposing of the rest, which could not. One of the analysts hired in the wartime surge, Juanita Moody (who had dropped out of college to make the same wartime sacrifices her male friends were making), became curious about the rejects. She was told directly not to work on the non-FLORADORA intercept because it could not be solved and would be a waste of valuable time. She and a colleague, Thomas Wagner, decided, however, that it would not go against orders if they examined the material in their off-duty time.

(U) Once again, a lucky break abetted the analysis. Details differ, but the basic story was this: a courier from the German Foreign Ministry was sent to distribute one-time pads to diplomatic posts in Latin America. His ship transited the Panama Canal; when it was stopped for inspection, he claimed diplomatic immunity. However, his credentials were not in order, so he was detained, and while his status was being sorted out, the FBI examined his luggage and photographed the pads.

(U) When the photographs were sent to Arlington Hall, analysts, led by Solomon Kullback, began to use them to work out the pattern by which the printing machine generated the one-time pad numbers.

(U) In the meantime, the Wagner-Moody effort against the allegedly unbreakable German diplomatic messages had attracted a number of others who were willing to work on their own time. One of them had a husband who worked in the headquarters office, and the secret got leaked. Shortly after that, a colonel visited the unofficial project, apparently ready to discipline the workers who were violating orders. When they explained the progress they were making, his attitude changed and additional personnel were assigned to the problem.

(U) With this and the unexpected acquisition of the one-time pad photographs, the Americans also worked out the pattern by which the supposedly random numbers were generated.

(U) This article is based primarily on the recollections of the major participants. William Filby in 1995 wrote an article on this effort for the journal *Intelligence and National Security*. Juanita Moody recalled the story in an oral history interview given in 1994. While some details differ, Solomon Kullback and Frank Rowlett recall this effort in their earlier oral history interviews.

(U) Bill Filby, by the way, married an American assignee to GCHQ after the war, and came to the States. His wife, Vera Filby, was one of the most influential instructors in the National Cryptologic School.

(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]

[redacted]

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

[redacted]

Doc ID: 6660671

Information Owner
Page Publisher
Last Modified: October 16, 2015
Last Reviewed: October 16, 2015

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

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