DAILY ENTERPRISE

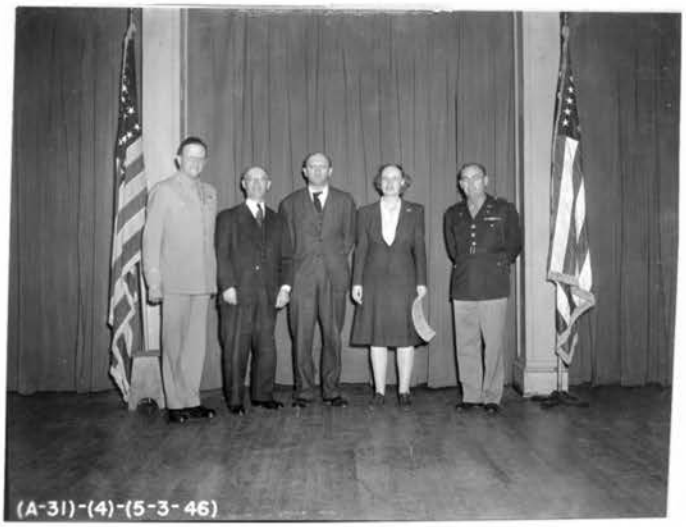
(U) Genevieve Grotjan Feinstein (Part Two) - HISTORY TODAY: April 23, 2019

FROM: (U) Center for Cryptologic History (CCH)
Run Date(s): 04/23/2019

(U) On February 1, 1943, the Army Signal Security Agency at Arlington Hall Station began its effort to study and exploit a particular set of Russian messages, thought at the time to be diplomatic communications. At that time, Arlington Hall's cryptanalysis effort was divided into two sections, headed respectively by Major Solomon Kullback and Major Frank Rowlett. The Russian diplomatic problem initially was assigned to Kullback's organization.

(U) The two-person team first assigned to this project began by imposing some sort of order on a large amount of back traffic dating mostly to 1940, with a few 1939 messages. More people, including several women who were former schoolteachers, were brought on board to join the Russian diplomatic problem in the summer and early fall of 1943.

(U) In the fall of 1943, the cryptanalysis effort reorganized: Kullback's section now was focused on Japanese army communications, and Rowlett's covered everything else. By this time, the team understood that the Russian diplomatic communications involved an enciphered codebook. The encipherment layer over the code was presumed to be a secure one-time pad system.



(U) Genevieve Grotjan Feinstein after receiving her Exceptional Civilian Service Award. Major General Chamberlain, Army Director of Intelligence (G-2), is on the left and Colonel Hayes, Chief, Army Security Agency, is on the right. Presumably the others are Genevieve's family members. (Center for Cryptologic History photograph collection)

(U) Not all was as it seemed. The

diplomatic communications were not all diplomatic, and the secure one-time pad was, in some instances, neither one-time nor secure. There were actually five user sets: diplomatic, lend-lease, and three Soviet intelligence services (KGB, GRU, and GRU-Naval). By mid-October 1943, the team had made the first break: all of the painstaking sorting and testing of messages paid off when they found instances of the one-time pad's being used twice. This allowed the effects of the encipherment layer to be removed, leaving the code groups.

(U) It was probably after this initial discovery that Genevieve Grotjan Feinstein (now married to chemist Hyman Feinstein), moved onto the team working the Russian problem. By now Genevieve was a senior cryptanalyst. Her expertise would have been well known to section head Rowlett, with whom she had worked on the PURPLE success. Notes by one Lieutenant Hallock, who previously had made the discovery that the one-time pad wasn't always one-time, showed Genevieve's ongoing influence, both in her personal analytic contributions and also in her mentoring and advising of the cryptanalytic staff.

(U) After the excitement of the discovery about the non-one-time pads, the team soon experienced a setback. May 1, 1944, did indeed turn out to be a Mayday: the format of the message indicators changed. These indicators had enabled the identification of pairs of messages using the same one-time-pad pages. Without knowing the location of the indicators, the team could no longer remove the encipherment layer and expose the code groups. Ironically, May 1 was also the day when the brilliant young cryptanalyst Cecil Phillips joined the team.

(U) For most of the rest of 1944, team members studied messages to try to find the new location of the indicators. Genevieve, the section's senior cryptanalyst, was kept apprised of ongoing work. When Phillips and his colleague Lucille Campbell found statistical irregularities in the messages, it was Genevieve who recognized that parts of the messages might be displaying actual information from the one-time-pad pages — "in the clear," as it were. If this were true, the team could once again search for duplication between messages by matching these glimpses into the actual one-time pads. As recorded by Phillips (who was there) and Robert Benson (who later documented the project with Phillips), the "results were quick and dramatic." Immediately, the team regained the ability to identify pairs of messages using the same one-time-pad page (per pair) and quickly found hundreds of instances of this insecure use of encrypted communications. At the same time, the cryptanalytic team had also found the first example of exploitable communications from the data set that would eventually

be identified as KGB.

(U) Once again, Genevieve had contributed critical insight that resulted in regaining progress on an analytical effort. And once again, her personal contribution was within the context of a wider cryptanalytic team and an even broader cryptologic effort. It would be several more years until the communications were fully exploitable: after the encipherment had been removed, the code groups still had to be solved by intensive linguistic analysis. And after the code groups began to be understood, the identities of the plaintext code meanings had yet to be associated with real-life actors. These identifications took place through collaboration with the FBI and other partners.

(U) The cryptographically vulnerable messages appeared only for a few years in the 1940s and were not exploited until several years after they had been sent. However, the information was so important that these 1940s messages continued to be worked by NSA for many decades. Why? The project, covername VENONA, revealed the extent of Soviet infiltration of America, from major businesses to sensitive scientific endeavors to the highest levels of government. Along the analytical road to this final outcome, Genevieve's realization of the significance of her team members' findings and her ability to leverage that information was deemed by the authors of NSA's official VENONA account to be "the most important single cryptanalytic break in the whole history of VENONA."

(U) Although Genevieve is best known for her contributions to these major discoveries, Arlington Hall records in the NSA Archives give occasional other insights into her day-to-day contributions. In mid-1942, she, alongside two other cryptanalysts, developed solutions to a set of Enigma traffic and also the German Kryha machine. And in late 1942, as part of a team of instructors she taught "an intensive course in machine cryptanalysis" to cryptanalysts who had been identified to work the German Enigma.

(U) In 1946, Genevieve was recognized with the Exceptional Civilian Service Award. That same year, the Feinsteins' son Ellis was born. And on May 4, 1947, after eight years of stellar public service, she resigned from the Army Security Agency.

(U) Eventually, Genevieve realized her early dream of becoming a mathematics professor. She taught at George Mason University (GMU) in Virginia, where her husband was a chemistry professor. Hyman, who predeceased her, established the Genevieve G. Feinstein Award in Cryptography at George Mason; it is awarded

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

annually. And in 2006, when Genevieve died, a $1 million legacy from her estate started the Ellis F. Feinstein Endowed Scholarship, in memory of their son, for GMU students with financial need.

(U) Genevieve Grotjan Feinstein was inducted into the NSA/CSS Cryptologic Hall of Honor in 2010. In her eight-year career of government service, her pivotal cryptanalytic insights directly contributed to U.S. national security, both during World War II and in the threatening atmosphere of the early Cold War. As a technical leader, she mentored other cryptanalysts, showing through her personal example the rewards of persistence and hard work, the joy of creative discovery, and the power of collaborative teamwork.

(U) The author of this article is [redacted]

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

(U//~~FOUO~~) Sources for today's article:

- *History of the Signal Security Agency: The General Cryptanalytic Problems (vol 2), 1946, 244-245, NSA Archives, Ref ID A2141776, Doc ID 6554247 (redacted)*
- *Benson and Phillips, History of VENONA, vol. 1 (NSA), 8, 13, 18, 24-28, 38-41, NSA Archives, Ref ID A2141776, Doc ID 4322341 (redacted)*
- *"An American Hero," At Buffalo, Spring 2018. See this article on the external Internet for more detail on Genevieve's early life and her years after leaving government service (http://www.buffalo.edu/atbuffalo/past-issues/spring-2018.html)*
- *George Mason University web pages (accessed in 2018) referenced the two Feinstein scholarships*
- *Mason Experimental Geometry Lab's external web page (accessed in January 2018) lists recent winners of the Genevieve G. Feinstein Award in Cryptography (through 2018). See http://meglab.wikidot.com (external Internet)*

(U) Discuss historical topics with interesting folks on the Center for Cryptologic History's blog: "go History Rocks!"

(U) Have a question or comment on History Today? Contact us at: DL cch or [redacted]

(U//~~FOUO~~) While the new CCH website on NSANet is being built, you can find all CCH publications on the CCH Intellipedia page on Intelink.

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

Information Owner P2 Strategic Comms, P2, 963-5901, (email)
Page Publisher P21 Web Staff, P2, 963-5901, (email)
Last Modified: April 23, 2019
Last Reviewed: April 23, 2019