

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DAILY ENTERPRISE



(U) Genevieve Grotjan Feinstein (Part One) - HISTORY TODAY: April 22, 2019

FROM: (U) Center for Cryptologic History (CCH)

Run Date(s): 04/22/2019



(U) Many Cryptologic Hall of Honor members have contributed a lifetime of service to the cryptologic mission. Genevieve Grotjan Feinstein's cryptologic service spanned only eight years. Why was this early cryptomathematician awarded NSA's highest recognition, membership in the Cryptologic Hall of Honor?

(U) Genevieve Grotjan was born on April 30, 1913, in Buffalo, New York. She showed early academic promise, graduating as the salutatorian of her high school class — and delivering her graduation address in Latin, no less! Upon graduating from the University of Buffalo with a mathematics undergraduate degree in 1936, she hoped to teach mathematics at the university level but did not obtain a position. She later moved to Washington, DC, to work as a statistician with the Railroad Retirement Board.

(U) Genevieve enjoyed her work. Eventually seeking to qualify for a promotion, she sat for a mathematics exam. Her exam results came to the attention of William Friedman, who was ever on the lookout for talented mathematicians to join his workforce at the Signal Intelligence Service (SIS), the U.S. Army's cryptologic organization. SIS recruited Genevieve, telling her only that she would be working in the code section. There was no hint that she would soon be working on Japanese codes.

(U) Many decades later, Genevieve described her SIS work to interviewer David Kahn in a way that later cryptanalysts would certainly recognize: "I would be writing, shuffling papers, sitting and staring, taking various counts — by hand at first . . . figuratively I scratched my head (if not literally)."



(U) Genevieve Grotjan's photograph in NSA's Cryptologic Hall of Honor

(U) On February 20, 1939, Japan began operational use of a new diplomatic encryption system, known within SIS as the "B" machine and eventually as the cover term PURPLE. Based on SIS's understanding of an earlier Japanese system ("RED"), the team knew that the twenty-six (26) letters appearing in the cipher were divided into two components of six letters and twenty letters. The cryptanalytic team had successfully diagnosed PURPLE's component of six, which they called "the sixes." Later in 1939, Leo Rosen (another future Cryptologic Hall of Honor member) devised a way to use telephone switches and other parts to build a machine eventually dubbed the "Six Buster." By mimicking the action of the PURPLE machine, Rosen's device took over the painstaking manual cryptanalytic work previously required to exploit the sixes.)

(U) This was to be the last real breakthrough on PURPLE for another year. During that year, the team focused on the component of twenty letters, which proved much more difficult to understand than the sixes had been. The next significant breakthrough came in the fall of 1940, on "September 20, at about 2:00 P.M.," as meticulously recorded by Friedman. On this day, Genevieve found consistent relationships between the ciphertext and plaintext in the messages she had been examining. In her own words to David Kahn: "This was the first real entering wedge except for the sixes we had because it confirmed something about the encipherment." She also cautioned: "There was still an awful lot to do."

(U) The team and its supervisors, including Friedman and Frank Rowlett, took a moment to celebrate Genevieve's discovery. In his book *It Wasn't All Magic*, Rowlett later described cheering cryptanalysts literally jumping for joy. Additional personnel were quickly added to the effort, and the team worked day and night to completely understand the PURPLE machine.

(U) Within days Leo Rosen, working for and with Rowlett, began to design a new machine to duplicate what was now known about the working of the PURPLE machine. Today, the new machine is referred to as the PURPLE analog (as in "analogous"). Remarkably, it had been built without the team's ever seeing an actual PURPLE device or any part of one. To this day, no intact PURPLE device has been recovered. The National Cryptologic Museum has on display an actual PURPLE fragment recovered later and two PURPLE analogs.

(U) Why was PURPLE, a diplomatic system, so important to the war effort? The major reason is that the Japanese ambassador to Berlin, General Oshima Hiroshi, was given broad access to German military and industrial information by officials of the Third Reich. General Oshima faithfully reported this information — encrypted by PURPLE — back to Japan and, as it turned out, also to the Americans who were able to decrypt the messages.

(U) Genevieve's flash of insight was critical to this success, as were the contributions of the other cryptanalytic team members who were able to build upon her findings. Friedman summed up the teamwork thus: "The successful solution of the B-machine is the culmination of 18 months of intensive study by a group of cryptanalysts and assistants working as a harmonious, well-coordinated and cooperative team. Only by such cooperation and close collaboration of all concerned could the solution possibly have been reached." And the overall success was not solely cryptanalytic: collectors made the data available; linguists were critical to the cryptanalytic effort and also in translating the decrypts;

and eventually the US military responded to the intelligence gained from PURPLE.

(U) In September 1943, William Friedman documented his award recommendations for individuals in his organization. He prefaced his PURPLE recommendations with these words: "I regard the Japanese 'Purple' machine and the underlying system to have been by far the most difficult cryptanalytic problem successfully handled and solved by any signal intelligence organization in the world" Among the list of his five "principal assistants" on this project was Genevieve Grotjan Feinstein, alongside Frank Rowlett, Robert Ferner, Albert Small, and Samuel Snyder. (Rowlett and Snyder are also Cryptologic Hall of Honor members.)

(U) Genevieve Grotjan's contribution to the solution of PURPLE is a significant part of her cryptanalytic legacy. But it is not the only problem in which she played a key role. Come back tomorrow to read about her contributions to an equally critical encryption problem.

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

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

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

- "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>)
- Genevieve Grotjan Feinstein, oral history with David Kahn (National Cryptologic Museum library, DK 181-14), May 12, 1991
- William Friedman, Preliminary Historical Report on the Solution of the "B" Machine (SRH-159), <https://www.nsa.gov>, especially 1, 8
- William Friedman, memorandum for Colonel Corderman, "Recommendations for Legion of Merit and Medal for Merit Awards,"

September 27, 1943, <https://www.nsa.gov>, 2

- William Kvetkas, "Genevieve Grotjan," CCH reference files
- Frank Rowlett, *It Wasn't All Magic*. Aegean Park Press: 151 and following

(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.

Information Owner P2 Strategic Comms, P2, 963-5901, (email)

Page Publisher P21 Web Staff, P2, 963-5901, (email)

Last Modified: April 22, 2019

Last Reviewed: April 22, 2019

DERIVED FROM: NSA/CSSM 1-52, DATED: 20180110, DECL
UNCLASSIFIED//~~FOR OFFICIAL USE ON~~