

William F. Friedman



<http://www.nsa.gov/gallery/photo/photo00057.jpg>

Once, when asked how he happened to become the father of American cryptology, William F. Friedman smiled and said, "I was seduced." This dapper little man with the mustache was a writer, teacher, inventor, and above all a cryptologist. Known as Mr. Friedman to his face, "Uncle Willie" behind his back, William Friedman was a leader in American cryptology for half a century and still significantly shapes the business today, over thirty years after his death.

Wolfe Frederick Friedman was born on 24 September 1891 in Kishinev, then part of imperial Russia, now Chisinau, capital of Moldova. His father, an interpreter for the Czar's postal service, emigrated to the United States the following year to escape increasing anti-Semitic regulations; the family joined him in Pittsburgh in 1893. Three years after that, when the elder Friedman became a U.S. citizen, Wolfe's name was changed to William.

After receiving a B.S. and doing some graduate work in genetics at Cornell University, William Friedman was recruited by "Colonel" George Fabyan for work in his department of genetics at Riverbank Laboratories, what would today be termed a "think tank," outside Chicago. Fabyan was an "honorary colonel" and a millionaire who could indulge his interest in science and industry.

In addition to the work being done in genetics and other industrial and agricultural topics, there was a cipher department at Riverbank studying the "Baconian Cipher." (Colonel Fabyan was convinced that Francis Bacon, rather than William Shakespeare, had written the plays credited to the latter.) Friedman became interested in the study of codes and ciphers, thanks to his concurrent interest in Elizebeth (sic) Smith, who was doing some of the "Baconian Cipher" research. When Riverbank was asked to train the military in the use of codes, Friedman was assigned as the principal instructor. As preparation, he made a thorough study of historical and present-day cryptology. Friedman served as a lieutenant in G6A2, the crypt unit of the American Expeditionary Forces (AEF) during World War I.

He returned to Riverbank until 1920, when he went to Washington, DC, to work in the Office of the Chief Signal Officer where, in 1922, he was made head of the Codes and Compilation Section. In 1929 he was selected to be the head of the newly organized Signal Intelligence Service (SIS). Throughout the early and middle 1930s, he created the organizational foundations of a cryptologic structure which evolved into the Army Security Agency (ASA) in World War II. In the process, he led the transition from paper and pencil cryptology into the modern era characterized by the application of machines to both cryptography and cryptanalysis.

The SIS/ASA is primarily famous as the group that "broke PURPLE"--PURPLE was the American code name for a Japanese diplomatic cryptosystem. A distinguished team trained and led by Friedman was responsible for this, one of the major cryptologic breakthroughs of World

War II, commensurate with the Polish solution of the German Enigma cipher. However, they didn't concentrate solely on breaking cryptosystems. Friedman and the members of the team also cooperated with Navy cryptographers to develop the most secure cipher machine of the World War, SIGABA. The major players on the team-- Rowlett, Sinkov, Kullback, Snyder, and Rosen-- went on to be major influences in the development of the Armed Forces Security Agency (AFSA) and NSA.

After the war, Friedman served as director, Communications Research (1947-1949); cryptologic consultant, Armed Forces Security Agency (1949-1951); research consultant, NSA (1952-1954); special assistant to the director, NSA (1954-1955); member of the NSA Scientific Advisory Board (1954-1960); and special consultant to NSA (1955-1969).

His services did not go unrecognized. He received the War Department Medal for Exceptional Civilian Service in 1944, the Presidential Medal for Merit in 1946, the Presidential National Security Medal in 1955, and a congressional award of \$100,000 for inventions and patents in the field of cryptology held secret by the government.

Perhaps Friedman's greatest achievements were introducing mathematical and scientific method into cryptology and producing training materials used by several generations of pupils. His work affected for the better both signals intelligence and information systems security, and much of what is done today at NSA may be traced to William Friedman's pioneering efforts.

William F. Friedman died in November 1969 of a heart attack. He is buried at Arlington National Cemetery.