

WILLIAM FRIEDMAN: A LIFE IN CRYPTOLOGY

"When it came to the cryptology, something in me found an outlet."

William Friedman (The Codebreakers, David Kahn)

William F. Friedman was more than a cryptologic pioneer; he is deemed the father of modern American cryptology. Throughout his adult life, he dedicated himself to the art and science of cryptology: making codes and breaking codes. "The legendary figure is with us still – in the works he left behind, in the science he created, and in the inspiration he bequeathed to his colleagues and friends," wrote Friedman's student and friend, Lambros Callimahos.

Throughout his career, William F. Friedman wrote notes, training manuals, reports, and books, leaving his legacy for future generations. The first of these works were training manuals he used to teach soldiers in World War I. After serving in a cryptanalytic unit in France during the First World War, he wrote a report on the codes used by the Germans. He followed this with a seminal work, *The Index of Coincidence and its Applications in Cryptography*. David Kahn, author and cryptologic historian, says this work "must be regarded as the most important single publication in cryptology." Later, in the 1950s Mr. Friedman wrote and presented six lectures on cryptologic history to teach new students in the field. His experience and insights passed to future generations of cryptologists and continue to inspire today.

William Friedman also devoted himself to working with others in the Army to build machines to protect the communications of the United States. Among them was the precursor to the SIGABA machine, which created cipher that was never solved by the enemy throughout World War II.

William Friedman's achievements in cryptanalysis are also noteworthy. "Time and again he shouldn't have been able to solve a particular message or cryptosystem, but he did," remembered Lambros Callimahos. Although Mr. Friedman was not a mathematician, he recognized the mathematical principles behind cryptanalysis and actively recruited mathematicians into the field, a practice that continues to this day. Lambros Callimahos noted, "Because of Mr. Friedman's foresight and pioneering efforts in cryptanalysis, cryptanalytic training, data processing machine utilization, and cryptanalytic organization, the U.S. Army was fully prepared to meet the cryptologic challenges of World War II."

"Friedman's major lasting contribution was the concept that cryptology had to move from a craft to an industrial process, and devised ways to make that happen."

Dr. David Hatch, NSA Historian