
MARYAM VULIS, Maryam Vulis

William Friedman's Contributions to American Cryptology.

William Frederick Friedman (1891-1969) is rightfully called the father of American cryptology, William Friedman was born in the Russian Empire, and was fortunate to grow up in Pittsburg, where his family settled after escaping Russian atrocities. Studying Electrical Engineering was not affordable, and he turned to genetics studies at Cornell University. The degree in Genetics brought him to the Riverbank Laboratories thus to cryptology where he met his future wife Elizebeth Smith, herself an outstanding cryptologist. William Friedman (WFF) started his career as an Army Cryptologist in 1917 when the US entered WWI and was eventually put in charge of the research division of the Army's Signal Intelligence Service (SIS). For over 30 years William Friedman was instrumental in providing cryptological security to the US Government. Friedman shrewdly saw the mathematical foundations in the science of deciphering and the necessity of involving trained mathematicians in his Army cryptological group. In 1920s, William Friedman introduced a clever use of the Index of Coincidence, a particular formula from probability One cannot about talk about William Friedman, and the success of breaking the Japanese diplomatic code Purple. Friedman's group successfully decrypted the Japanese Navy communications and reconstructed the Japanese cipher machine Purple giving cryptanalysis the decisive role in the victory at Midway in 1942. After WWII, William Friedman joined the NSA, whose existence was not even known to the public at the time and became chief NSA cryptologist. The 2015 declassification of his work brought in the recognition that William Friedman deserved.