REF ID:A4045962

WILLIAM F. FRIEDMAN (1891-1969)

When I joined the U.S. Army to enter the cryptologic service of my adopted country on February 11, 1941, William F. Friedman, the man who became the dean of modern American cryptologists, was already a legendary figure in my eyes. I had read two early papers of his, "L'indice de coïncidence et ses applications en cryptographie" and "Application des méthodes de la statistique à la cryptographie," when I was living in Paris in 1934, concertizing as a flute soloist throughout Europe while privately pursuing serious studies in cryptology, in anticipation of eventual military service. I was therefore properly impressed when I first met Mr. Friedman, the dapper figure with the Adolph Menjou moustache, the cryptologic giant who asked the most searching questions and understood the answers even before the explanations were finished. After a tour of duty in Washington I went to New Delhi as an Assistant Theater Signal Intelligence Officer, and when the war ended Mr. Friedman requested my reassignment to Washington as his principal Technical Assistant.

My respect and admiration for the man for whom I worked increased with every contact and discussion. Mr. Friedman was superb in his work habits, thinking our the problem in broad outlines, and mapping out points a, b, c,...n in logical progression with clarity of exposition and greatest attention to detail. He wasted but little time or motion, and knew instinctively when he was on the wrong track--a splendid attribute for any cryptanalyst. He had immense drive, and knew how to organize his colleagues for the most effective teamwork to achieve maximum efficiency of effort.

Mr. Friedman was blessed by phenomenal luck throughout his entire career as a cryptanalyst--everything he touched turned to plain text, a sort of latter-day

Approved for Release by NSA on 05-12-2014 pursuant to E.O. 13526

Midas. Time and again he shouldn't have been able to solve a particular message or a cryptosystem, but he did: the odds were against him, but luck was for him. That is, luck tempered by logical insight and remarkable intuition. Mr. Friedman was not a mathematician, but he had superb mathematical feeling and insight, inventing techniques that were missed by mathematicians working on the problem. A classic example of his innovative abilities was in his solution in 1923 of an exceedingly complex cipher machine. He postulated that there were 91,000,000,000 alphabets involved when there were really only 45,000,000,000, and--in spite of his modest mathematical background--originated an important theory of coincidence and, with only ten messages, arrived at a solution of the machine.

A typical example of his unbelievable luck occurred in 1917 when Mr. Friedman was at Riverbank Laboratories in Geneva, Illinois, where he was employed as a geneticist and cryptologist by a wealthy eccentric named Colonel George Fabyan who had a quasi-official relationship with the Government. The British had proposed the use of a geared disk cipher device for U.S.-British communications which was regarded as absolutely indecipherable if the sequences for both plain and cipher components were unknown. But somebody in Washington suggested that perhaps it might be wise to have the device tested by William Friedman at Riverbank. Accordingly, five very short test messages--a most unrealistic test--were sent to Friedman, and by a process that remains a mystery to this day he was able to scrounge out from the cipher texts the sequence for the cipher component based on the key word CIPHER. But now he was stumped, as he didn't quite know what to do next, since it wasn't until 1923 that he discovered an important principle which would have made the problem a very simple one. But he called in one member of his staff, his wife Elizebeth, told her he was going

to give her a certain word, and asked her to give him the first word that occurred to her. He said "cipher," and she replied "machine." Sure enough, the plain component was based on the key word MACHINE. (One of the messages read "This cipher is absolutely undecipherable."!) The solution went back to the British and, although 11,000 of the devices had been manufactured, they were never used.

Mr. Friedman returned to Riverbank Laboratories after the war from France, where he had been a member of the Code and Cipher Solving Section, G2 GHQ AEF. He now solved, among others, a supposedly unsolvable machine system proposed by the AT&T Corporation. On January 1, 1921, he entered government service as a cryptologist. The entire cryptologic organization of the U.S. Army consisted only of Mr. Friedman and one clerk-typist until April 1930, when three young high school mathematics teachers were recruited by Mr. Friedman, picking the three persons from the civil service list who had made the highest scores on the mathematics examination. These three, Solomon Kullback ('59), Frank Rowlett, and Abraham Sinkov, were to remain in cryptologic work, making notable contributions for over three decades and rising to high positions.

In 1933 a challenge message was submitted to the Signal Corps by a New York lawyer representing a client who had bought, for $100,000, the North American rights to a cipher machine invented by a German. The machine was touted by the inventor as absolutely indecipherable, and a German mathematician had demonstrated that the number of ways in which a message could be enciphered was 2.29×10^{82}, a figure 100 million times as large as the number of atoms in the universe. The message was received on February 24, and was date-stamped "Feb 24 AM 11:12," with the notation in Friedman's handwriting, "Commenced work. W.F.F." On another part of the messages was the pixie-ish observation, "Time out during lunch period,

50 minutes. W.F.F." And then over the date-time stamp "Feb 24 PM 2:43," was the cryptic notation, "Solved. W.F.F." Elapsed time: 3 hours and 31 minutes, less 50 minutes for lunch--2 hours and 41 minutes, and this without any machine aids whatsoever! A letter with the decipherment and the keys was sent to the lawyer that afternoon.

Mr. Friedman studied many proposals for cryptographic systems, solving everything that came his way. One cipher teleprinter machine that was studied had a period of 8.65×10^{14}, and the inventor and his sponsors (the IT&T Corp.) claimed that cryptograms produced by the machine were practically, if not absolutely, indecipherable without the key. It took almost four years to construct the machine, at a cost of approximately $100,000--but it took Friedman and his staff less than three hours to break it. In addition to his ability to destroy everyone else's ciphers, Friedman was able to invent a number of cryptographic systems for his country that would withstand sophisticated attack by enemy cryptanalysts. For his inventions Congress in 1956 awarded him $100,000 in compensation for profits he might have realized if the patents had not been held secret by the Government.

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 cryptographic challenges of World War II. Friedman took part in all these aspects during the war and continued to make notable contributions. After the war a most spectacular role of cryptanalysis was revealed in the hearings held by the joint congressional committee on the investigation of the Pearl Harbor attack. At that time it was made public that, shortly before the war, the U.S. in a brilliant stroke of

cryptanalysis had been able to reconstruct the Japanese cipher machine which was used for the highest-level diplomatic communications, enabling this traffic to be read throughout the war. The successful solution of this machine, known by its cover name as the PURPLE machine, represented 18 months of intensive study by a group of U.S. Army cryptanalysts under the direction of William F. Friedman.

Mr. Friedman continued his brilliant work until he retired from the National Security Agency in 1955, after over 35 years of service with United States cryptologic activities. We had become the closest of friends, and the bond between us is indicated by the warm inscription on his portrait which he gave to me in 1958, reading as follows:

> "To my disciple, colleague, and friend, Lambros Demetrios Callimahos--who, having at an early age become one of the great flautists of the world, deserted the profession of musician, in favor of another in which he is making noteworthy contributions--
>
> From
>
> William F. Friedman--
>
> who, having at an early age aspired to become noted in the field of biology, deserted the profession of geneticist, in favor of another, upon which he hopes he had left some impression by his contributions.
>
> In short: from deserter to deserter, with affectional greetings:
>
> W.F.F.
>
> Washington, 21 November 1958"

It was a great honor and privilege to have known him and to have been his collaborator, and to have been counted as one of his intimate friends.

William Friedman, dean of modern American cryptologists, was the most eminent pioneer in the application of scientific principles to cryptology who laid the foundation for present-day concepts. His inventions and many achievements won for him the nation's highest awards and a reputation as one of the world's leading cryptologists. In 1944, he was presented the War Department's

highest decoration, the Exceptional Civilian Service Award; in 1946, he was awarded the Presidential Medal for Merit; and in 1955, Mr. Allen Dulles, then Director of Central Intelligence, presented the National Security Medal, the country's highest award for contributions to the national security. He was the author of many classified publications, of articles in scholarly journals, and of the articles on cryptology in the 1927 and 1954 editions of the Encyclopaedia Britannica. With his wife (who was for years a leading cryptologist with the Treasury Department), he authored the book, The Shakespearean Ciphers Examined. For this book they were awarded the Folger Shakespeare Literary Prize and the Fifth Annual Award of the American Festival Theater and Academy. He was listed in Who's Who in America and in American Men of Science, and was a member of the Cosmos Club since 1946.

On Sunday, November 2, 1969, at the age of 78, William Frederick Friedman died quietly at his home in Washington, D.C., and was buried with full military honors in Arlington Cemetery. 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.

Lambros D. Callimahos ('72)

(1728)