William Friedman, Geneticist Turned Cryptographer

Irwin L. Goldman¹

Department of Horticulture, University of Wisconsin–Madison, Wisconsin 53706

ABSTRACT William Friedman (1891–1969), trained as a plant geneticist at Cornell University, was employed at Riverbank Laboratories by the eccentric millionaire George Fabyan to work on wheat breeding. Friedman, however, soon became intrigued by and started working on a pet project of Fabyan's involving the conjecture that Francis Bacon, a polymath known for the study of ciphers, was the real author of Shakespeare's plays. Thus, beginning in ~1916, Friedman turned his attention to the so called "Baconian cipher," and developed decryption techniques that bore similarity to approaches for solving problems in population genetics. His most significant, indeed pathbreaking, work used ideas from genetics and statistics, focusing on analysis of the frequencies of letters in language use. Although he had transitioned from being a geneticist to a cryptographer, his earlier work had resonance in his later pursuits. He soon began working directly for the United States government and produced solutions used to solve complex military ciphers, in particular to break the Japanese *Purple* code during World War II. Another important legacy of his work was the establishment of the Signal Intelligence Service and eventually the National Security Agency.

KEYWORDS cryptogram; cryptanalysis; Baconian cipher; Riverbank Laboratory

A code is a rule that governs how one piece of information is converted into a different representation of that information. Both language and writing are elegant examples of codes developed to transmit complex concepts using symbols. Humans have used codes for millennia to communicate and to prevent communications from being discovered. The scientific approach to secret communications is a field known as cryptography. Modern cryptography makes use of complex mathematical algorithms, rather than symbols, to transform messages into encrypted forms. Decoding cryptograms requires intelligence and creativity, and this type of expertise is of great value in military strategy and tactics.

The science of genetics is intertwined with the science of coding, since genetic material itself contains a code that is ultimately translated into proteins by cells. One could argue that our understanding of heredity was, in part, a process of decoding nature. Beginning in the early 1960s, the nature of the genetic code could, at last, be investigated directly and the precise relationship between nucleotides and protein synthesis was established. Preceding this, however, geneticists had long been accustomed to using codes for the loci that control the presence or absence of traits and the various allelic forms

of a gene. Thus, codes and coding have long been a part of understanding modern genetics and may be an important part of the allure of this field of science.

William Friedman (1891–1969) was a plant genetics student at Cornell University between 1912 and 1916. During this time, he taught introductory and advanced genetics and conducted research on maize with Rollins Emerson at Cornell and George Shull at Cold Spring Harbor, both pioneers in the field of genetics and breeding. Hired as a geneticist at Riverbank Laboratories in Geneva, IL while still in graduate school, Friedman began applying the type of thinking one would use for genetics problems to solve the ciphers and cryptographs that were sent to Riverbank for decoding by the United States military's cipher division. Friedman eventually left the field of genetics and developed a series of approaches to encryption that were to revolutionize the field of cryptography. His critical pathbreaking work relied on statistical approaches to languages, focusing on analysis of the frequencies of letters in language use. Eventually working for the War Department in the United States government, Friedman's many solutions to complex military ciphers led to large improvements in national security, including the breaking of the Japanese *Purple* code during WWII. Friedman is considered the father of modern cryptography. This essay traces the arc of Friedman's career from geneticist to cryptographer, and points to the parallels between problem solving approaches in these two fields.

William Friedman's Early Years

Wolfe Frederic Friedman, later William F. Friedman, was born in 1891 in Kishinev, which is now part of the Republic of Moldova. At the time of Friedman's birth, Kishinev was the Bessarabian capital of czarist Russia. His father Frederic was from Bucharest and worked as a translator and interpreter in the Russian postal service. His mother, Rosa Trust, was from Kishinev. By the time of William's birth, more than half the population of Kishinev were Jews. Restrictions imposed by Russian authorities following the assassination of Alexander II in 1881, however, made life difficult for Jews, and many thousands began emigrating. The Friedmans followed this path and came to Pittsburgh, PA in 1892, where Frederic worked for the Singer sewing machine company and Rosa worked for a clothing company (Clark 1977). The family was in near-constant debt and struggled to make ends meet. Nevertheless, America provided a welcome refuge and they became American citizens in 1896.

William Friedman was a precocious child with interests in science and agriculture. He was also drawn to puzzles and was taken with Edgar Allen Poe's *The Gold Bug*, a famous story published in 1843 in which Poe uses an encrypted message that must be decoded in order to find a buried treasure (Clark 1977). A detailed description is provided in the story for the solution of a substitution cipher that employed the frequencies of letters. This episode foretells Friedman's lifelong interest in codes and ciphers (Rosenheim 1997), but the field of genetics intervened before Friedman could devote himself to that pursuit.

At Pittsburgh Central High School, Friedman was part of a debating society known as the "Emporean Philomath" (Clark 1977). There, among other topics, the members debated the merits of Zionism, the nationalistic movement that espoused the reestablishment of a Jewish homeland in Palestine. Zionism had sprung up in the 19th century as a reaction to anti-Semitism in Europe. The movement had an agrarian emphasis, whereby collective farms would be established so that a people who had largely been displaced from agriculture for thousands of years could return to work the soil. Friedman was passionate about these ideas, and this became part of his inspiration to enroll in Michigan Agricultural College in Lansing, MI in 1910 to study agricultural genetics. Leaving Michigan after 6 months, Friedman enrolled at Cornell University in Ithaca, NY, where he was a student of the newly developing science of genetics. He spent his summers working at Cold Spring Harbor with C. B. Davenport and G. H. Shull. Shull was a pioneer in plant genetics concerned with the relationship between inbreeding and outbreeding, as well as the development of hybrid corn (Murphy and Kass 2007). Davenport was a biologist and leader of the eugenics movement in the United States, founding the International Federation of Eugenics Organizations in 1925. Friedman graduated from Cornell in 1914 with a bachelor's degree and enrolled in Cornell's graduate program in plant breeding, with Rollins Emerson as his major professor. Friedman also served as an assistant in undergraduate courses, including

genetics and advanced genetics in 1915 (Murphy and Kass 2007). Emerson had been a student of Edward Murray East, a geneticist at Harvard's Bussey Institute (Sax 1966; Goldman 2002), and was among a cohort of newly trained faculty bringing applied genetics to land-grant institutions throughout the United States.

In May 1915, Emerson received an unsolicited letter from Colonel George Fabyan of Chicago, asking him if he might be able to recommend someone who could head up his new genetics department at Riverbank Laboratories in Geneva, IL, located ~30 miles west of downtown Chicago on Fox River. Emerson recommended Friedman. In trying to convince Friedman to join the work at Riverbank, Fabyan wrote him a letter encouraging him to use genetics to improve crop adaptation and productivity: "I want the father of wheat, and I want a wife for him, so that the child will grow in arid country. Where did I get this problem? I got it from one of my wealthy Jewish friends, and if I can beat him to it, he will foot the bills and be damned glad to" (cited in Munson 2013). Given Friedman's interests in Zionism and agriculture, this could hardly have failed to appeal to him. Leaving Cornell, Friedman joined Fabyan at Riverbank. He did not publish any scientific articles from his graduate work at Cornell or produce a graduate thesis.

George Fabyan and Riverbank Laboratories

George Fabyan (Figure 1) was a scion of Boston-based Bliss, Fabyan & Company; one of the country's most prosperous textile firms. After a stint working in the Chicago office of that firm, the independently wealthy Fabyan decided to develop a laboratory to fund his pet scientific pursuits, among them the new science of genetics. Fabyan hobnobbed with many influential people both in the United States and abroad. For his public service work, the governor of Illinois awarded him an honorary title of colonel, by which he was known throughout his life. Colonel Fabyan said "Some rich men go in for art collections, gay times on the Riviera, or extravagant living, but they all get satiated. That's why I stick to scientific experiments, spending money to discover valuable things that universities can't afford. You never get sick of too much knowledge" (Clark 1977).

Fabyan began buying up land on the Fox River near Geneva in 1905 (Munson 2013). Eventually employing 150 workers and covering 350 acres, Fabyan's research complex, which became known as Riverbank, was one of the most unusual and important private research laboratories in the history of the United States. Featured in the September 1923 issue of *Scientific American*, the Riverbank scientists were seen to be "pegging away at the secrets of nature, sooner or later break down existing barriers, open the way to a new field, and we are soon confronted with brand new opportunities for explorations." Fabyan built a large engineering laboratory at Riverbank, a radiation laboratory with stored radium where cancer research took place, an acoustics laboratory, a veterinary laboratory where hoof-and-mouth disease was investigated, a

Figure 1 Colonel George Fabyan in one of his suspended armchairs.

laboratory for fire-retardant materials, and a cryptography group. Fabyan also added a genetics research laboratory, including experimental fields and greenhouses.

The other plant geneticist hired at Riverbank to complete the genetics department was Karl Sax (1892–1973). Sax was likely identified as a candidate for Riverbank through some of the same Harvard connections by which Fabyan found Friedman. Sax was an undergraduate at Washington State College when he married his cytology teacher, Dr. Hally Jolivet, a native of Wisconsin. Jolivet took a position at Wellesley College in Massachusetts in 1916 and Sax began his studies at the Bussey Institute, at that time under the direction of Edward Murray East. After working briefly at the University of California, Berkeley, Sax was hired at Riverbank in 1919 to work in plant breeding. Sax and Jolivet found Riverbank to be fascinating but also unnerving, as Fabyan had taken a romantic interest in Jolivet. As a result, the Saxes fled Riverbank for Orono, ME, but later went back to Boston where Sax worked as a professor at the Bussey Institute. He became a prolific researcher and horticultural plant breeder; developing new strains of apples, magnolias, cherries, and forsythias, and his work on X ray-induced mutagenesis was pioneering in plant breeding and plant genetics. He served as director of the Arnold Arboretum, where the Bussey Institute had been located, from 1947 to 1954.

Riverbank Laboratories was an eccentric place. Fabyan's pet gorilla roamed the grounds. All of the chairs, beds, and furniture were hung from the ceilings with chains to facilitate the cleaning of the floors (Munson 2013). Fabyan wore knickerbocker suits, as if he were an equestrian (which he was not). A giant Dutch windmill was transported to Riverbank at great expense, where it sat on a nearby island in Fox River. Fabyan worked with world-famous designers and architects on the property, including Frank Lloyd Wright, whom Fabyan hired in 1907 to remodel the farmhouse into a stately villa (Munson 2013), and a landscape gardener from Japan who was presented to Fabyan by the Japanese royal family. Fabyan had served as informal consul to the Japanese government before the official consulate in Chicago was developed (Munson 2013). Over the years, Fabyan hosted many Japanese dignitaries and built an expansive formal Japanese garden. Fabyan delighted in giving tours to academics and politicians; he had a friendship with Theodore Roosevelt and hosted a visit to Riverbank by Albert Einstein. He was also successful in convincing the father of acoustical science, Paul Sabine, dean of Harvard's Bussey Institute, to design the acoustics laboratory at Riverbank. But Fabyan's primary pursuit at the time Friedman joined the laboratory was codes and ciphers.

The Baconian Cipher

Fabyan had long used codes in his cotton business dealings as a way to disguise the meaning of communications and telegrams (Kranz 1970). Late in the 19th century, a controversy had raged about the authorship of William Shakespeare's plays. Delia Salter Bacon (1811–1859); who was born in Tallmadge, OH and raised there and in Hartford, CT; may have originated the idea that Sir Francis Bacon and others were the true authors of William Shakespeare's plays. Delia Bacon published her work in 1857 but suffered a mental breakdown shortly thereafter and died in 1859. Orville Ward Owen (1854–1924), a physician from Detroit, MI, wrote a six-volume treatise called *Sir Francis Bacon's Cipher Story* (Owen 1893–1895), published between 1893 and 1895, adding to the notion that Sir Francis Bacon had not only written Shakespeare's plays but also embedded ciphers in these texts. Owen claimed proof in these texts, via a device he had concocted called a cipher wheel, of a host of Elizabethan conspiracies including that Bacon was Queen Elizabeth's son and that *Romeo and Juliet* was the story of Bacon's romance with the Queen of France, Margaret of Valois.

Others also became intrigued by the story of the Bacon-Shakespeare connection. Elizabeth Wells Gallup (1848–1934), together with her sister Kate Wells, worked on solving the Baconian ciphers while working as a high school principal. Bacon, as Lord Chancellor to the Queen of England, had borne responsibility for government's oversight of book printing. He was thus perhaps in a position to influence the text of Shakespeare's printed works. But critics noted how unlikely it might be that Bacon would go to all that trouble to write

some of the most famous works of literature in the English language simply as a vehicle for passing along encoded messages; nevertheless the notion of a secret embedded in these great works captivated the imagination of many, including Fabyan and Gallup.

Because of Fabyan's interest in this subject, the cryptography group at Riverbank was dedicated to solving the alleged Baconian cipher. Fabyan hired Elizabeth Gallup to lead this effort. She believed that the differing fonts in the First Folio were part of a bilateral cipher, where each slightly differing font would symbolize a particular substitution of a letter. Such ciphers were commonplace at the time and used to protect official communications from prying eyes. Bacon had developed a bilateral cipher, described in one of his famous works known as *De Augmentis Scientiarum*. In this cipher, the letter "a" would be represented by the code "aaaaa," the letter "b" would be represented by the code "aaaab," and the letter "c" would be represented by the code "aaaba." The letter "d" was represented by "aaabb," the letter "e" by "aabaa," the letter "f" was "aabab," and "g" was "aabba." Clark (1977) has described this cipher's operation through the phrase "good news," which would be represented by:

G O O D N E W S

aabba abbaab abbaab aaabb abbaa aabaa babaa baaab

To send a message with this sort of cipher, one would first create a sentence with five times as many letters as those in the original message. Then, marked letters would be indicated with a different font, such as italic, which would contrast with the normal font of the other letters. A coded letter would be indicated with a "b" font, such as an italic font, while all the rest of the letters would be indicated with an "a" or normal font. In this way, the message "good news" could be delivered through the phrase "We will see you Sunday or some other proper day," if the phrase was written in the following way as described by Kahn (1967):

"We will see you on Sunday or some other proper day."

Each italicized letter would be the location of a "b," which would give the code:

aabba abbaab abbaab aaabb abbaa aabaa babaa baaab, or
"good news."

Students of genetics will immediately realize a similarity of such cipher problems to problems in genetics. The abstract nature of genetics problems, in which a letter stands for a particular purine or pyrimidine base, a set of letters for a codon, and a string of letters as a DNA sequence, attracts those who have a natural fondness for codes and ciphers.

William Friedman and Cryptography

Genetics, however, was also a particular interest of Fabyan's: he felt it represented a key to life's code. Edward Sax, son of geneticist Karl Sax who worked on wheat breeding with Friedman, recorded his father's recollections about Riverbank. The elder

Sax commented: "The Friedmans lived in a cottage next to ours. They did their work in the Villa. Fabyan's real reason for hiring me soon became evident in our conversations. He had the idea that the secret of life was contained in a genetic code, and that with the help of the Friedmans, who had by now established a leading reputation for their deciphering abilities, we could ultimately break that code and discover the secret of life" (Sax 2002). Interestingly, in 1954, after completing his service at the Arboretum, Sax took occupancy of an office on the second floor of the Harvard biological building on Divinity Avenue in Cambridge, MA. One of his floor mates was the newly hired assistant professor James D. Watson.

Shortly after his arrival at Riverbank, Friedman was conscripted by Gallup to apply his self-taught photography skills to the Baconian cipher problem. Friedman photographed and enlarged images of Shakespeare's First Folio to more easily study the text. Gallup's helpers included Elizebeth Smith, who had been raised in Huntington, IN and who had studied English literature. She had viewed the First Folio at Newberry Reference Library in Chicago in 1916 and it was there where an introduction was made to Colonel Fabyan. Later, Elizebeth joined Gallup at Riverbank and began working with Friedman, whom she eventually married in 1917 (Figure 2). Elizebeth Smith (1892–1980) became a prominent cryptographer in her own right, working often with her husband on complex military ciphers. From this point, Friedman largely left the field of genetics and both he and Elizebeth dedicated themselves to developing the science of modern cryptography. About this departure, Friedman said he felt as though he had been seduced to leave an honorable profession (genetics) for one with a slight odor (cryptography). In an ironic twist, decades later, after they retired, William and Elizebeth wrote the definitive work irrefutably demonstrating that the Baconian ciphers of Owen and Gallup were printing errors due entirely to worn and damaged type or even ink spread during the printing process, and therefore had nothing to do with codes of any kind (Friedman and Friedman 1957).

During World War I, Riverbank became a leading center of cryptographic work due to the work of Friedman, Smith, and others in their circle. Because Riverbank had assembled such a well-known working group in the area of codes and ciphers, the United States Government offices sent them messages that needed to be decrypted. Their success in doing so led Fabyan to ask the intelligence office of the War Department if Riverbank staff could be of help in the war effort. The United States found itself highly unprepared to deal with encrypted messages during the war, and Riverbank provided much-needed assistance for the allied war effort. During this time, a cipher bureau known as Military Intelligence 8 was set up in Washington, DC under the direction of Herbert Yardley, and Riverbank became a training ground for recruits to the bureau. The course was directed by Friedman and began his lifelong passion for organizing and assembling key information about cryptography which would be used worldwide.

In 1919, Friedman wrote a revolutionary article called *The Index of Coincidence and its Applications in Cryptography*

Figure 2 William and Elizebeth Friedman at Riverbank Laboratories, undated photograph.

(Friedman 1919), which explained how statistical techniques could be used in cryptanalysis. In this approach, two cryptograms are placed side by side and counts are made of the number of times the same letters occur in the same place in both texts. The degree to which they coappear is called the index of coincidence. The technique is a probabilistic approach to solving codes and is similar to using correlation analysis to understand biological phenomena. No such approach to breaking codes had ever previously been attempted. The quantitative reasoning Friedman applied to codes transformed cryptography into something resembling a science. Friedman wrote: "It will be shown in this paper that the frequency tables of certain types of ciphers have definite characteristics of a mathematical or rather statistical nature, approaching more or less closely those of ordinary statistical curves."

To understand the index, Kahn (1967) encourages imagining two urns, each containing one each of the 26 letters of the alphabet. The chance of drawing identical, paired letters out of each urn would be $(1/26\text{th} \times 1/26\text{th})$, and the chance of drawing any pair of letters from these urns would be the sum of all 26 such probabilities, which is equivalent to 0.0385. If we also assumed two urns with a collection of letters where each letter was present in the same frequency,

Figure 3 In-house Riverbank plant diagram on Bacon's cipher technique by William Friedman, ca. 1916, where even the drawing's legend contains a bilateral cipher.

and we chose letters from each urn and superimposed the string of texts one on top of the other from each of the urns; we would find a similar probability that the letter in one string was the same as a letter in the other string in the same position: 0.0385. This is known as the "random" constant.

Assume another urn with a set of 100 letters, where the frequency of each letter is based on how it is used in normal text, such as the one in this manuscript. We can call these plaintext urns. The chance of drawing a letter is proportional to its frequency in the language. If you had two such urns, the chance of drawing a pair of English letters would be a product of their frequencies, and the probability of drawing any pair of identical letters is the sum of these probabilities, which is equivalent to 0.0667.

Finally, if we have two plaintext urns containing strings of plaintext, and we draw letters from them and superimpose the two strings, the probability that two identical letters will

Wreath and Cipher Key from Seventeenth Century Cryptographer.

Figure 4 Cipher figure embedded in article by Jensen, attributed to the cryptographer Friderici: a single rose represents the letter "E," a pair of roses represent the letter "N," a single tulip is "I," a pair of tulips is "R," etc. The bouquet is meant to be read clockwise starting at 12 o'clock. A spray of lilies of the valley separates each word. From *The Florist's Review* (Jensen 1920).

coincide in the same position is also 0.0667. This means that for every two plaintext English phrases we compare, we would expect about seven coincidental pairs of letters to line up if we superimposed one phrase on top of the other. This can be called the "plaintext" constant.

These two probabilities, known as κ_r (0.0385) for the random situation and κ_p (0.0667) for the plaintext situation, are of great importance to cryptography. Each alphabet will have its own specific values for these random and plaintext probabilities. For example, the Cyrillic alphabet with its 30 characters will have a κ_r of 0.0333 and a κ_p of 0.0529; values for κ_p for French are 0.0778; and for German, 0.0762.

Knowing the κ_p values for a particular alphabet provides a key for deciphering codes because it provides a statistical basis for comparing strings of text. When two cryptograms are properly juxtaposed, the coincidences that exist in the original plaintext show up. This mathematical approach allows one to assess the probability that two letters are the same and gives constants for each language that can be used

Figure 5 Jensen describes the use of a bilateral cipher (note the key in the top left of the figure) to encrypt the message "love accomplishes all things" using red and white roses and the bilateral cipher key used by Sir Francis Bacon. From *The Florist's Review* (Jensen 1920).

to check against. Kahn (1967) says that this is like shifting, a small distance at a time, two identical picket fences with very narrow slits at irregular intervals. From time to time, there will be a small amount of light shining through two slits when they overlap by chance from each fence, but there will be a very large amount of light shining through when all of the slits are properly juxtaposed.

In addition to the very serious business of military ciphers, Friedman clearly must have enjoyed exploring his horticultural and botanical interests (Figure 3, Figure 4, and Figure 5). In a remarkable essay in *The Florist's Review* in 1920, a horticultural trade magazine published in Chicago, an author named Cora J. Jensen from the Riverbank Laboratory Department of Ciphers—who is clearly writing information collected by William Friedman—described how floral arrangements can be used as encryption devices. Revealing the Baconian bilateral cipher in the article, the author explains how messages can be encrypted using different flower colors or different combinations of flowers in a bilateral arrangement. One of the figures shows how the message "love accomplishes all things" can be encrypted in a landscape arrangement with red and white roses (Figure 4 and Figure 5; Jensen 1920).

Genetics and Cryptography

Reginald Punnett, an English geneticist, was the first to figure out a way to calculate the probability of offspring with particular genotypes from a cross of parents with known genotypes (Edwards 2012). The Punnett square, named after his approach, is a summary of possible allelic combinations from the maternal and paternal sides. One can also think of the

Figure 6 Frequency distribution of letters in English usage based on a sample of 40,000 words.

Punnett square as a coded representation of the laws of heredity where alleles are assigned letters and the various allelic combinations, or genotypes, can be predicted based on their contributions from the parents.

Friedman would have no doubt learned about the Punnett square at Cornell University and most likely taught this newly discovered concept to his genetics students. The representational aspect of letters symbolizing alleles, allelic combinations symbolizing genotypes, and genotypes symbolizing phenotypes bears a certain similarity to the sort of codes and puzzles found in cryptography. It is therefore tempting to propose that Friedman's cryptographic genius was in part motivated by his penchant for genetics.

As a modern science, Mendelian heredity was only beginning to be understood by the turn of the 20th century. Still, the notion that contrasting alleles at a genetic locus, which were understood to physically reside on chromosomes, could be represented by letters that symbolized their similarities and differences has some commonality with the ideas behind a code or cipher. If, for example, we allow *A* to represent the wild-type allele and *a* to represent the mutant allele, we create a code where we can describe the physical characteristics of an organism carrying one of each of these alleles via the letter code *Aa*. And, like for many codes and ciphers, a set of rules (dominance, codominance, etc.) is constructed to interpret the code. It is perhaps most similar in the sense that letters are used as representative symbols in a code; much like the way a code or cipher uses letters or sets of letters as representative symbols that carry the code in a particular language.

Furthermore, the remarkable insight provided by Mendel was fundamentally a way to apply statistical models to biological phenomena. Friedman's insight similarly took from statistics and mathematics and applied it to a frequency problem with languages. Friedman's revolutionary index of coincidence has parallels to problems in population genetics. The frequency of letters in typical English language speech or writing has been quantified and represents a distribution like the one depicted below. The letter "e" is used most frequently, at >12% (Figure 6), followed by "t," "a," and "o." Problems in

Figure 7 William Friedman.

population genetics often focus on the sampling of alleles from a population, leading to consideration of the frequency of a given allele. In this way, Friedman's index of coincidence is reminiscent of the type of frequency calculations one might employ when studying an allele or genotype in a population.

Kahn (1967) wrote that "Before Friedman, cryptology eked out an existence as a study unto itself, as an isolated phenomenon, neither borrowing from nor contributing to other bodies of knowledge. . . . Friedman led cryptology out of this lonely wilderness and into the broad rich domain of statistics. He connected cryptology to mathematics." In a fitting twist to the spirit of Friedman's efforts, cryptographic problems have recently been solved with genetic algorithms. Genetic algorithms make use of the process of natural selection, using the rules of heredity, to solve problems. Substitution ciphers and other types of ciphers have been solved with such algorithms (Morelli and Walde 2003; Morelli *et al.* 2004).

Friedman's Career in Cryptography

Friedman became Chief Cryptanalyst to the War Department in 1921 and then later Director of Communications Research in the Army Security Agency (Figure 7). He wrote the book *Elements of Cryptanalysis*, which became the United States Army's main cryptographic reference. Friedman went on to have a remarkable career. He provided key evidence in the Senate hearings for the Teapot Dome scandal of 1924,

testifying before a congressional committee on coded telegrams concerning the leasing of federal land containing petroleum reserves to private developers in exchange for bribes. Friedman decoded the telegrams that provided key evidence for the conviction of Albert Bacon Fall, United States Secretary of the Interior, as well as the Secretary of the Navy and the Attorney General.

Friedman was a delegate to many important international conferences on behalf of the United States government. Eventually Friedman was to be put in charge of the Signal Intelligence Service, which was the forerunner to the National Security Agency. During World War II, Friedman and his group were responsible for the breaking of the Japanese *Purple* code, one of the most sophisticated ciphers ever developed. He was awarded the Medal for Merit in 1946 by Harry Truman, and the National Security Medal in 1955 by Dwight Eisenhower. Friedman is considered a national hero and is buried in Arlington cemetery. Bacon's dictum "knowledge is power" appears on his headstone. His revolutionary approach to codes and ciphers, which bears similarity to approaches used by geneticists, has changed the landscape for modern warfare and national security.

Literature Cited

- Clark, R. W., 1977 *The Man Who Broke Purple: The Life of the World's Greatest Cryptologist Colonel William F. Friedman*. Weidenfeld and Nicolson, London.
- Edwards, A. W. F., 2012 Reginald Crundall Punnett, first Arthur Balfour Professor of genetics, 1912. *Genetics* 192: 3–13.
- Friedman, W. F., 1919 *The Index of Coincidence and its Applications in Cryptography*. War Department. Government Printing Office, Washington.
- Friedman, W. F., and E. S. Friedman, 1957 *The Shakespearean Ciphers Examined: An Analysis of Cryptographic Systems Used as Evidence That Some Author Other Than William Shakespeare Wrote the Plays Commonly Attributed To Him*, Ed. 2. Cambridge University Press, London.
- Friedman, W. F., 1924 *Elements of Cryptanalysis*, U.S. Government Printing Office, Washington, D.C. 157.
- Goldman, I. L., 2002 The intellectual legacy of the Illinois long term selection experiment. *Plant Breed. Rev.* 24: 61–78.
- Jensen, C. J., 1920 "Saying It" In *Cipher*, pp. 17–19 in *The Florist's Review*, Vol. XLVI. Chicago.
- Kahn, D., 1967 *The Codebreakers: The Story of Secret Writing*. Scribner, New York.
- Kranz, F. W., 1970 Early history of Riverbank Acoustical Laboratories. *J. Acoust. Soc. Am.* 49: 381–384.
- Morelli, F., and R. Walde, 2003 A word-based genetic algorithm for cryptanalysis of short cryptograms. *Amer. Assoc. Artificial Intelligence*, 229–233.
- Morelli, R., R. Walde, and W. Servos, 2004 A study of heuristic approaches for breaking short cryptograms. *Int. J. Artif. Intell. Tools* 13: 45–64.
- Munson, R., 2013 *George Fabyan: The Tycoon Who Broke Ciphers, Ended Wars, Manipulated Sound, Built a Levitation Machine, and Organized the Modern Research Center*. CreateSpace Independent Publishing Platform, MO.
- Murphy, R. P., and L. B. Kass, 2007 *Evolution of Plant Breeding at Cornell University*. The Internet-First University Press, Ithaca, NY. Available at: <http://ecommons.library.cornell.edu/handle/1813/62>.
- Owen, O. W., 1893–1895 *Sir Francis Bacon's Cipher Story*. Vol. 1–6. Howard Publishing Company, Brentwood, TN.
- Rosenheim, S. J., 1997 *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet*. Johns Hopkins University Press, Baltimore.
- Sax, E., 2002 *Personal Letter to Irwin Goldman, June 3*.
- Sax, K., 1966 The Bussey Institution: Harvard University Graduate School of Applied Biology. *J. Hered.* 57: 175–179.

Communicating editor: A. S. Wilkins