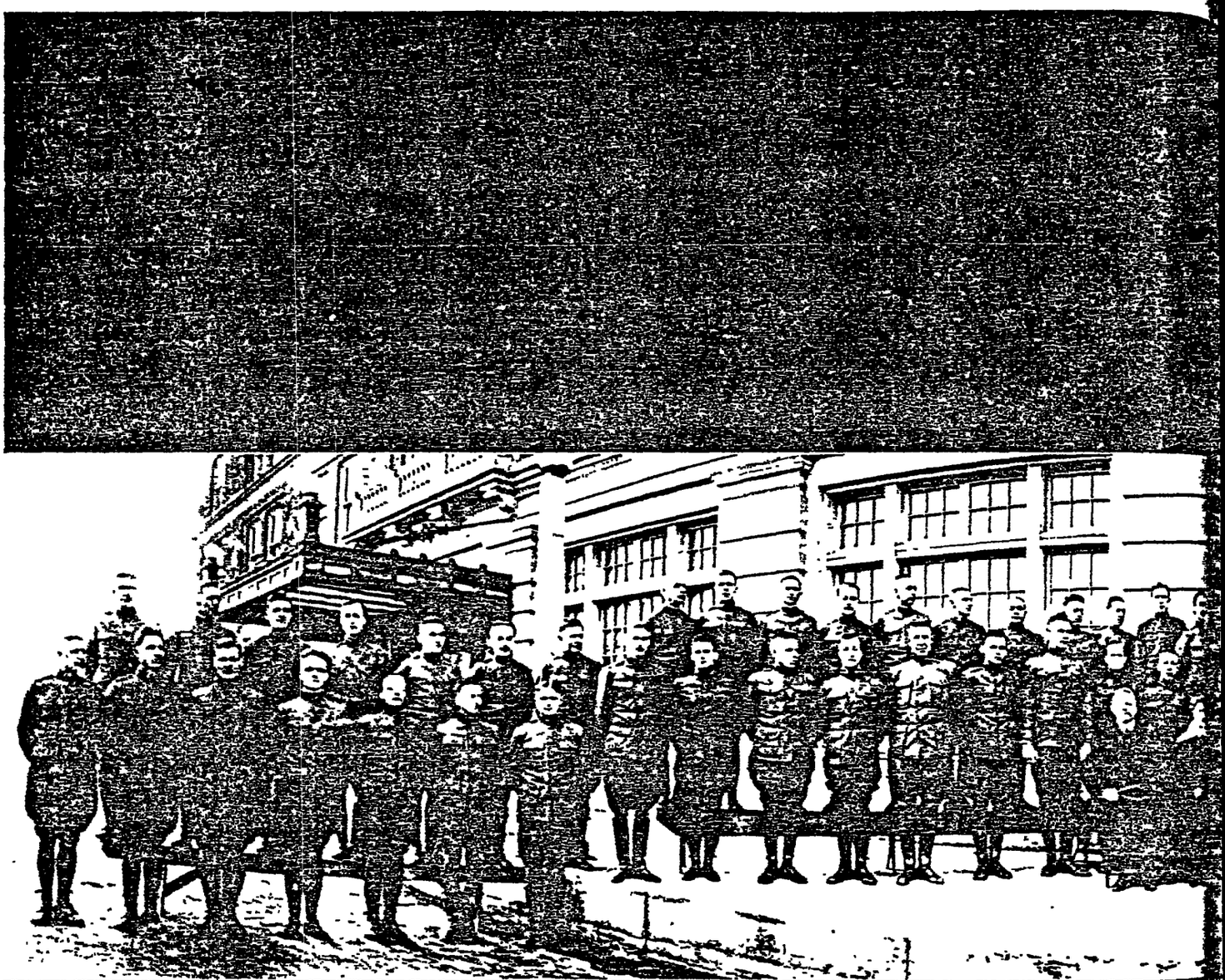


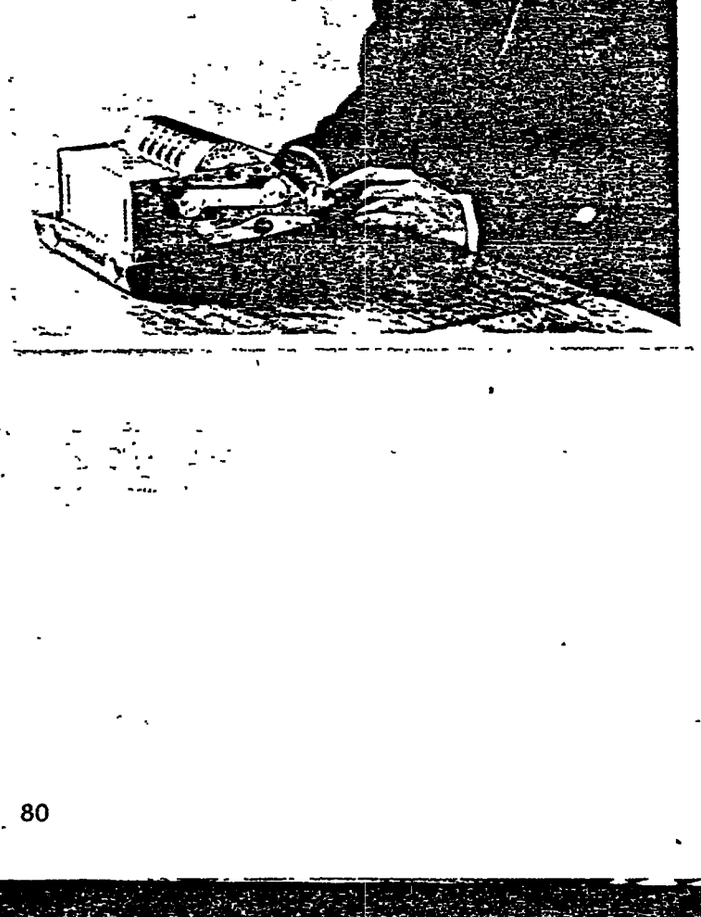
A PIONEER IN CRYPTOLOGY

Conveying a secret message, students and staff of the U.S. Army's cryptographic school in Geneva, Illinois, assemble for a graduation picture with their director, William F. Friedman (seated at center, right); in February of 1918, Friedman arranged his pupils and colleagues to form five-element groups that represent letters in a binary cipher—one using two elements in various combinations, as Morse code uses dots and dashes. In Friedman's human cipher, those whose heads face forward are equivalent to dots; those turned sideways represent dashes. The message reads from left to right, beginning in the back row, where the letter "K" is enciphered as "dot dash dot dot dash," and spells out "Knowledge is power," an aphorism of the 16th Century English philosopher Francis Bacon. Alas, Friedman had four fewer people than he needed and had to serve by himself as the final "r."

THE GENIUS WHO BUILT THE PURPLE MACHINE

To the men and women who worked with him, William Friedman's building of the Purple cipher machine to break the Japanese diplomatic code *(pages 56-57)* was no surprise. Since World War I he had been devising and unraveling codes with dazzling insight and a special imaginative flair, as the class picture on the preceding page suggests. While teaching classes of Army officers in 1917-1918, Friedman wrote a series of instruction manuals laying down mathematical principles that transformed cryptology from an intuitive craft into a full-fledged science. As the preeminent practitioner of that science, he trained a whole generation of cryptologists in the rigorously analytic techniques that enabled the United States to become the leading nation in the field by the eve of World War II.

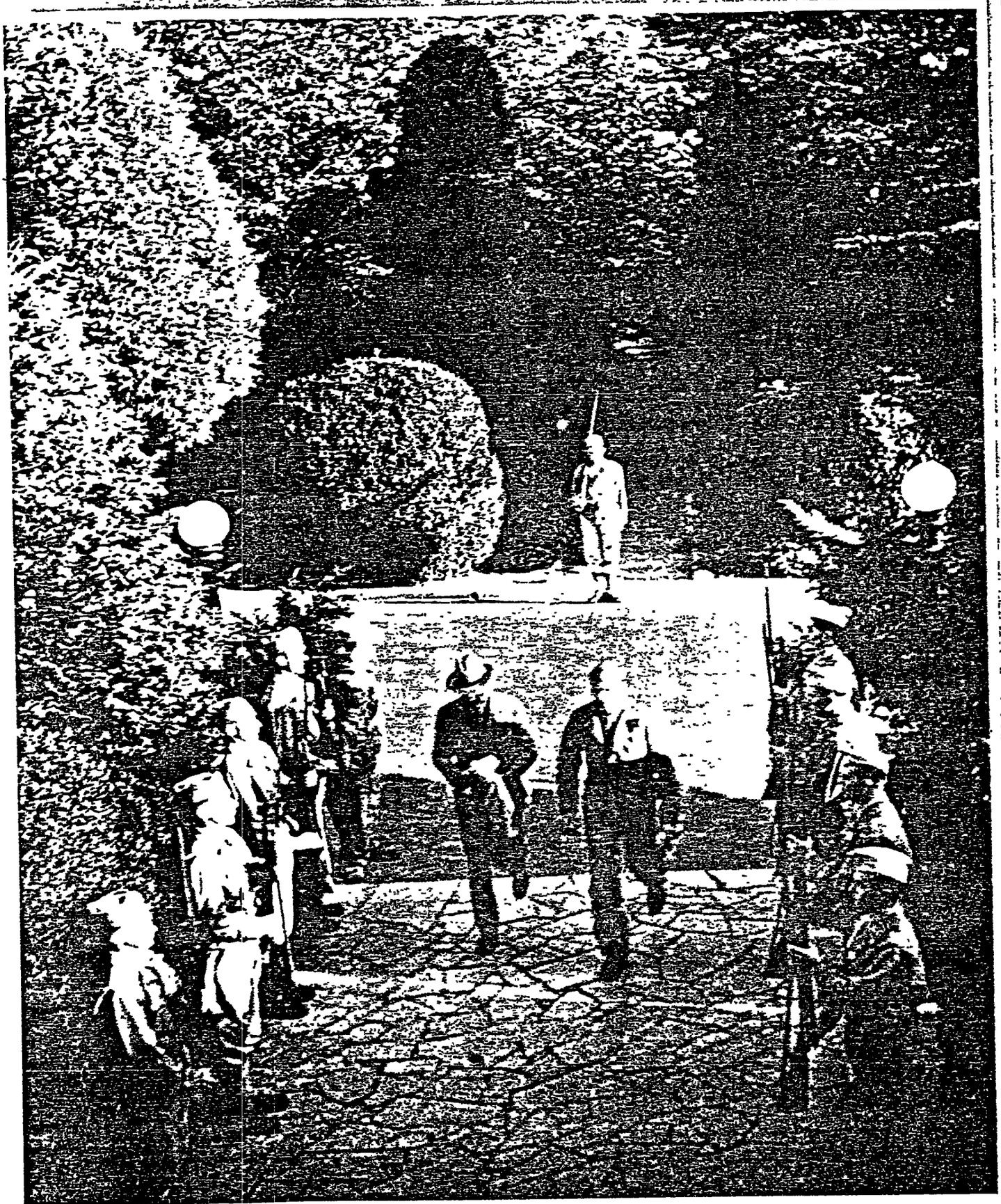
In a 1924 photograph, Friedman sits at a cipher machine that created random alphabets. Comparable machines were used widely in World War II.



Friedman started his career at a time when global rivalries and the advent of radiotelegraphy were increasing the traffic in encoded messages. The 1920s saw the introduction of a variety of electromechanical enciphering systems, most of them involving multiple-rotor machines that produced codes far more complex than any dreamed of before. As chief codebreaker for the Army Signal Corps, Friedman used mathematical inductive reasoning to reconstruct the new machines and crack their codes, thus laying the foundation for solving all modern rotor-machine puzzles.

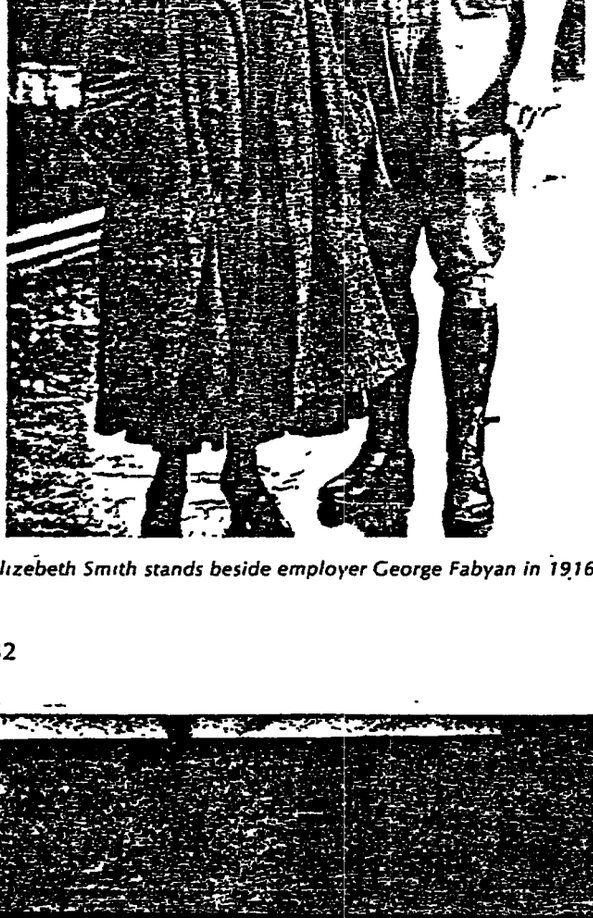
By the mid-1930s Friedman had become Chief Cryptanalyst of the War Department, charged with directing U.S. Army codebreaking efforts. His chief responsibility quickly became the breaking of the codes that the Japanese introduced in 1934, after the American press had revealed that the United States government was eavesdropping on diplomatic traffic from Tokyo.

When the War came, Friedman's staff outgrew its little office in the War Department and moved into the campus buildings at Arlington Hall, a former girls' school in Virginia. The work that went on there was unknown to the public, but Army Chief of Staff General George C. Marshall called it the determining factor in "the conduct of General Eisenhower's campaign and of all operations in the Pacific."

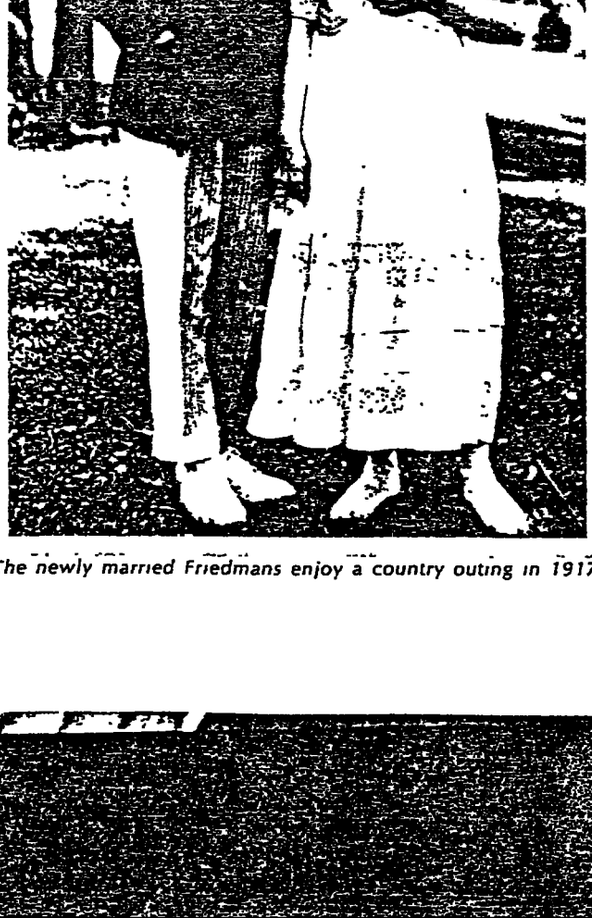


As civilian head of the Signal Security Agency of the U.S. Army, a felt-hatted Friedman arrives to take possession of Arlington Hall for the agency in 1942.

As a Cornell student, Friedman conducts plant-genetics studies in an insect-free hut at a Carnegie Institution experimental station in 1913.



Elizebeth Smith stands beside employer George Fabyan in 1916.



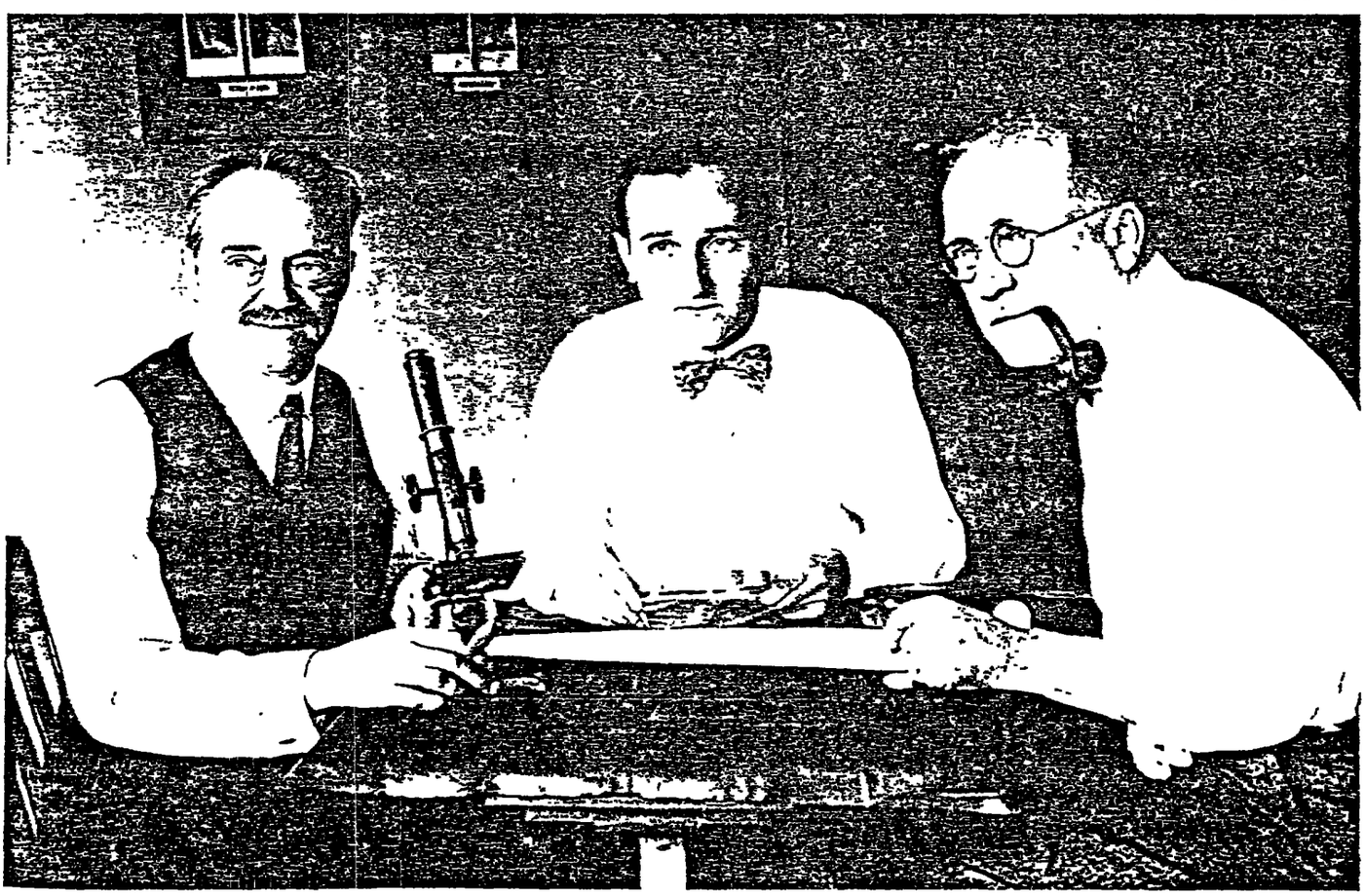
The newly married Friedmans enjoy a country outing in 1917.

FROM PLANT GENETICS TO SECRET CIPHERS

Friedman found his calling indirectly. He set out to be a botanist. But in 1915, as a fledgling scientist, he worked on the Illinois farm of an eccentric millionaire, Colonel George Fabyan. There he met Elizebeth Smith, who was hired to pore over Shakespeare's plays in search of a cipher that the colonel fancied would prove Francis Bacon the real playwright. That was labor lost. But Friedman fell in love with both Miss Smith and cryptology, marrying one and making the other his career.

In 1918 the American Telephone and Telegraph Company introduced a cipher machine that worked on the principle of the binary cipher—using as the two elements the presence or absence of perforations on a tape. Friedman cracked its system in six weeks, making himself famous. Six years later, when the U.S. Army mistook some radio signals for messages from Mars, Friedman was naturally the man the Army consulted to try to figure them out.

Friedman sits at the keyboard of an American Telephone and Telegraph cipher machine in 1919.



Friedman (center) and two colleagues try to decipher radio signals thought to have originated on the planet Mars, which came close to Earth in 1924.

who helped break the Japanese diplomatic code.

From: Tokyo
To: Washington
7 December 1941
(Purple-Eng)

#902 Part 14 of 14

(Note: In the forwarding instructions to the radio station handling this part, appeared the plain English phrase "VERY IMPORTANT")

7. Obviously it is the intention of the American Government to conspire with Great Britain and other countries to obstruct Japan's efforts toward the establishment of peace through the creation of a New Order in East Asia, and especially to preserve Anglo-American rights and interests by keeping Japan and China at war. This intention has been revealed clearly during the course of the present negotiations. Thus, the earnest hope of the Japanese Government to adjust Japanese-American relations and to preserve and promote the peace of the Pacific through cooperation with the American Government has finally been lost.

The Japanese Government regrets to have to notify hereby the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations.

JD-1:7143 SECRET (M) Navy trans. 7 Dec. 1941 (S-TT)

This deciphered message signaled the rupture of U.S.-Japanese relations in 1941.

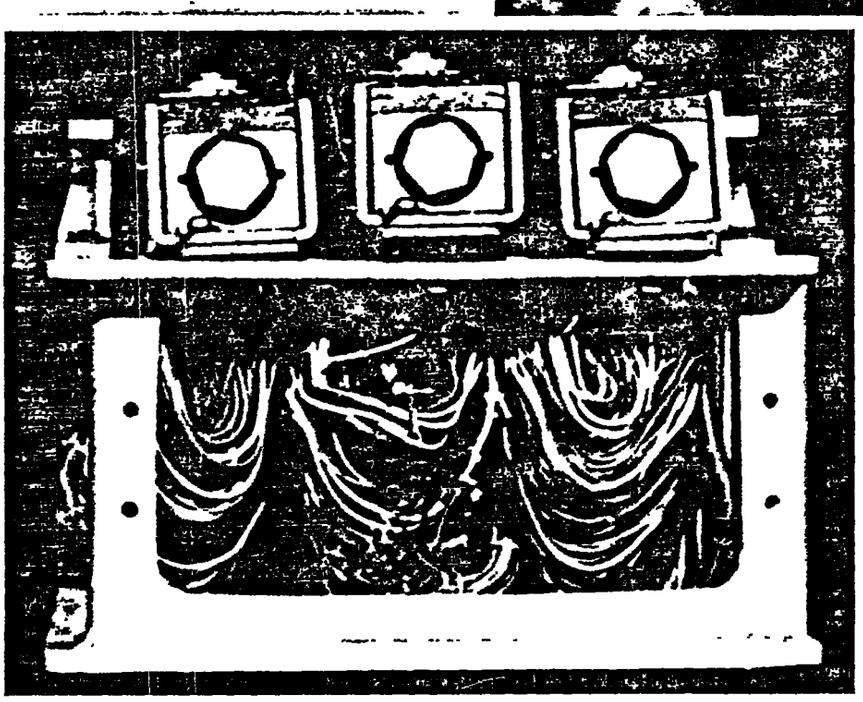
A MASSIVE ASSAULT ON A CIPHER MACHINE

By the 1930s, most industrial nations had some sort of electromechanical enciphering device. Among the most sophisticated of these was the one that from 1937 on transmitted the Japanese diplomatic code, nicknamed Purple by American cryptanalysts. Shortly after the Purple code was put into use, breaking it became William Friedman's top priority.

Supporting him was a superb team that he had started recruiting in 1930 from scholars in such disciplines as mathematics and linguistics. For 18 nerve-racking months, Friedman's team tried to duplicate the Japanese machine.

Instead of being based on rotors, the machine worked on the principle of a telephone switchboard, using plugs to shuffle arrangements of letters. When a replica Purple machine was finally hand-built in August of 1940, the United States had an instrument that enabled it to eavesdrop on such diplomatic fare as Germany's efforts to press Japan into war against Great Britain in March 1941.

The effort to build the machine told on everyone. It was, one cryptanalyst said, like being "engulfed in an interminable polar night." Friedman himself suffered a nervous collapse.



Built from readily available wires and screws, this American machine broke Japan's Purple code.

Friedman (center) is flanked in