Who Came Up With This Idea? March 1

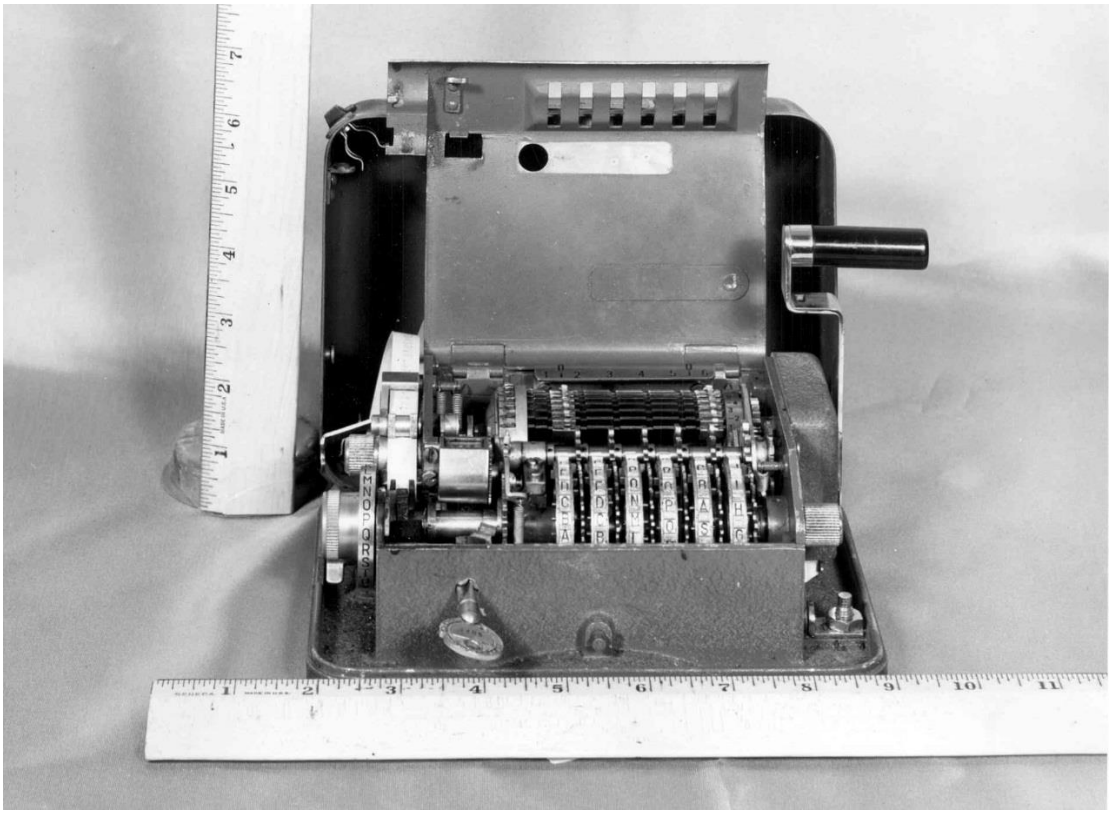
The principal tactical cryptographic device used by the Army in World War II was the M-209. This was the U.S. designation for a device manufactured under license from the Swedish cryptographic industrialist, Boris Hagelin.

The M-209 was considered fairly secure for a tactical device --- which usually needed to protect communications for 24 to 48 hours at most --- but it had an extensive list of disadvantages when using it. The encryption process was slow, and the device itself was hard to keep clean; it also was difficult under the best of circumstances to make changes to the cryptographic settings. And, of course, as a tactical device for deployment into combat zones, the M-209 was seldom used in the best of circumstances.

One additional disadvantage was the need to keep the device stable enough to use. This photograph shows the machine in use in a jungle setting on a South Pacific island.

This photograph shows the “textbook” method for using the M-209 in the field.

A look at the machine’s innards indicates how meticulous the process of changing the M-209’s settings had to be, and why they were time consuming. This view also allows us to imagine how difficult the cleaning process was.



Two things had to be done to determine the stepping pattern of the cipher wheels: first, each letter on each cipher wheel had a small pin through it; each pin had to be pushed either to the left or right of the letter. Second, in the back of the machine were parallel bars (sometimes called “the squirrel cage” by M-209 users); on each bar was a small lug, which had to be set in one of four positions along the bar.

Whose idea was it to use this machine? William Friedman recommended that the Army adopt the Hagelin device for tactical communications. Friedman had seen overseas service in World War I, but he did not see combat, and had never had to use a tactical cryptographic machine under fire or in dismal locales.

508 caption: photo 1 --- a soldier in the field bent over as he types a message on an M-209 which is balanced on a back pack; photo 2 --- a leg and hands, with an M-209 balanced on a knee, a strap running from the kneecap to the foot, running under the arch of the foot; hands are turning dials on the M-209; no other bodily parts are visible; photo 3 --- an open M-209 revealing 6 cipher wheels in the front and thin steel bars in the back; the machine is flanked by two rulers that measure its height and width.