Secret Code Machines: The Inside Story

The Eerie World of Espionage Has Created Some Truly Strange Hardware!

BY A.E. FELDMAN

About the author: Mr. Feldman is an avid collector of cryptographic equipment. Per-

The M-209, A Sturdy Contender

The most frequently encountered device is the American M-209, and what a wonderful and complex machine it is! It's less than 7-inches square, and the actual mechanism is reminiscent of old time mechanical adding machines.

A cursory look inside the M-209 reveals very complex workings. There are six internal keywheels, each with attched moveable tabs, providing a cryptographic *period* (the number of letters the device must consecutively produce from plaintext before enciphering routines are repeated) or more than one hundred million!

The military manual goes on to exquisitely describe the M-94, saying that it "consists of the following parts: (1) A central shaft, the left end of which terminates with a projecting shoulder, the right end of which is threaded. (2) A set of 25 alphabet disks, on the rim of each of which there is stamped a different, completely disarranged alphabet. (3) A guide-rule disk, consisting of a blank or unlettered disk from which projects a guide-rule. (4) A retaining plate, consisting of a thin disk upon one surface of which is stamped the name and type number of the device. (5) A knurled nut."

Get the idea? This description gives new meaning to the aphorism of a picture being worth 1,000 words. Still, the M-94 is remarkably easy to use, although the simplicity is a trade-off at the expense of signal security. Given the state of the art of cryptanalysis even before 1922, this device offered little (if any) security. Not at all surprising that the reason the M-94 was nicknamed the *Jefferson Wheel* was because it had been invented in the Seventeenth Centruy by Thomas Jefferson!

It's remarkable that our pre-WWII military was using for "secret communication" a device whose basic principle was undoubtedly even older than the 150 year period that had passed since Thomas Jefferson first proposed the device and its actual adoption by our armed forces! Nevertheless, it is a noteworthy historical item.

As impressive as all of this sounds, supposedly by the middle of WWII the German intercept stations were routinely deciphering M-209 messages in as little as three hours. So much for any really serious secrets sent out via an M-209 network. But the M-209 was a tactical device, and for some tactical operations, three hours clearance may be an acceptable time frame.

The basic mechanism dates from the late 1930's, being credited to Boris Hegelin, a Russian-born Swiss citizen. While Hegelin's brilliance can't be denied, it does appear that the M-209 was actually a refinement of earlier devices. Legend has it that in 1940, Hegelin secured passage on one of the last European ocean liners and visited American authorities with samples and prototypes of the M-209. David Kahn's *Code Breakers* book reports that more than 140,000 M-209's were made by L.C. Smith and Corona Typewriters, Inc. Reportedly a Cyrillic (Russian) alphabet version was also made. One source states that the Italian Navy used a device identical to the M-209.

The military manual for the M-209 was entitled, "Technical Manual TM 11-380, Converter M-209, M-209-A, M-209B (cipher)" and is dated 1944. It describes the M-209 as being used in military units of division level and below. The enciphered text appeared as five-letter groups.

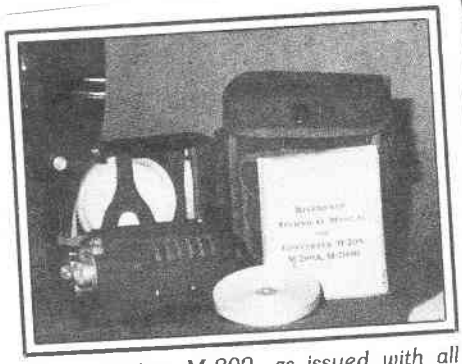
It was a sturdy little unit with a top lid that folded down to protect the mechanism. Perhaps its basic ruggedness is why so many seem to have survived and still turn up at gun shows, antique shows, and flea markets. A few I've seen appear to look unused, or even brand new in factory condition with all manuals and accessories.

M-209 legends abound. One is that Turkey adopted 500 or 1,000 of them after WWII. Another story is that our government dumped thousands of M-209's into the ocean rather than sell them as surplus. An alternate legend claims they were first "steam rolled" or torched into junk and *then* dumped into the ocean.

Mr. Hegelin went on to start a Swedish company called Crypto-Aktien Gesellschaft A.G., devoted entirely to manufacturing cipher devices and systems. Presently the company is located in Zug, Switzerland and is known as Crypto AG Zug.

The Heyday

During the heyday of mechanical cipher devices (from WWII to the late 1960's when electronics took over), Crypto AG was active in marketing their crypto equipment. Since the large world powers develop their own crypto systems, chances are that the company primarily sold them to the smaller nations. The products were reasonably effective if the instructions were carefully followed, and it was still less expensive for a Third World nation than doing its own research, development, and production.



The complete M-209, as issued with all manuals, tape, and accessories.

An interior look at the M-209 with its cover lifted.