

April 95

Museum Lifts Veil of Secrecy From Code-Making and Breaking

National Security Agency displays history of cryptography - sort of

By **Simson L. Garfinkel**
Special to The Christian Science Monitor

FORT MEADE, MD.

FOR more than 40 years, it was one of the United States government's most secret organizations, hidden in the Maryland countryside midway between Baltimore and Washington, D.C. People who worked there joked that its initials, NSA, stood for "No Such Agency." Their spouses and children, on the other hand, claimed the true meaning of the initials was "Never Say Anything."

But today at Port Meade, Md., home of the world's foremost military intelligence organization, the National Security Agency, there is a new openness - sort of.

Last year the NSA opened the doors to a new annex, the National Cryptologic Museum. Looking more like a bunker than the Smithsonian, the mu-



THE ENIGMA OF **CRYPTOGRAPHY** machines were used by the Germans in World War II to encrypt messages. Visitors to the cryptologic museum can try out this one.

seum is housed in a one-story building that's ringed with a 12-foot chain-link and barbed-wire fence. And it's less than a mile from the agency's office complex, where it is a federal offense to so much as make a pencil sketch of the buildings from the parking lot.

The National Cryptologic Museum purports to chronicle the history of the NSA. But it's a necessarily sanitized history. Indeed, most of the museum's cryptographic treasures actually predate the NSA, which came into existence on Nov. 4, 1952. Instead, the museum has a rare books collection, including a second edition of "Polygraphiae" (1518), the first book on cryptography ever published. There is also

an impressive exhibit on the the native American "code talkers," who confounded German and Japanese code-breakers during World Wars I and II by speaking in their native tongues.

Many visitors feel that the museum's most impressive exhibit is a collection of 13 German Enigma machines, the standard military cipher used by Hitler during World War II. Covered with buttons, dials, and lights, the machines look like children's toys from an earlier age, but they were actually the basis for the Germans' most secret military code. To encrypt a message, the German code officer would type each letter onto the machine's keyboards; each button would cause a different light to illuminate, and the officer would write down the enciphered message. The machine could be used in reverse to decrypt the corresponding message.

"I hadn't realized there were so many (Enigma) models," says Phil Karn, a computer programmer visiting from San Diego. "One case had several prewar Polish and German versions along with disassembled components and a schematic diagram showing how a rotor machine operates. The other case had the different models used by the different German forces - Air Force, Navy, Army, and submarine service."

But for Mr. Karn, the best part of the exhibit is the Enigma machine located on a pedestal, where museum visitors can try it out to encrypt messages of their own. "Having read quite a bit about Enigma, I had no trouble making it work," he says.

Neither did the Allies. During the war, a top-secret effort headed by English mathematician Alan Turing figured out a way to decrypt the Germans' communications. The resulting military intelligence dramatically shortened the war. An exhibit standing next to the machines shows how it was done.

Other exhibits hint at the role of cryptography and eavesdropping during the cold war. In the back of the museum is a two-foot wooden seal of the United States - a replica of one presented to US Ambassador Averell Harriman by Soviet school children in 1946. The ambassador was so impressed with the seal that he hung it in his office. Six years later, intelligence agents discovered that the seal contained a hidden microphone and radio antenna. By beaming a radio signal at the instrument, the Soviets could listen in on the ambassador.

Most recently, the museum's curator, Jack Ingram, has built a new exhibit around a fragment from Francis Gary Powers's U-2 spy aircraft, which the Soviet Union shot down on May 1, 1960. The fragment was presented to Mr. Ingram last October, when a delegation from Moscow's Central Armed Forces Museum came for a visit.

What's missing from the National Cryptologic Museum is information about modern advances in cryptography. A piece from a Cray 1 supercomputer hints at the use of high-speed thinking machines for code-making and code-breaking. But the museum does little to chart the unseen role that the NSA has had in shaping the development and growth of the nation's entire computer industry.

"I would have liked to have seen more examples of actual breaks and successes of cryptanalysis and traffic analysis, but that might be more boring for others than the kind of exhibits they had," said Jim Gillogly, a computer scientist at the BAND Corporation. "I would, of course, like to see a great deal about specific cryptanalysis methods, with examples... but I understand why that would be inappropriate."

•The Motional Cryptologic Museum is open weekdays from 9 a.m. to 3 p.m. and Saturdays from, 10 a.m. to 2 p.m.