Calendar

Code Crusher

An Exhibit of Encryption

It's the size of a clunky, old manual typewriter, circa 1940s. There's an ordinary keyboard and a carrying case that made it portable. The Germans manufactured many thousands of them for use on U-boats and elsewhere during World War II. There is a German word for it, but we and our allies called it the Enigma, and cracking its code is considered one of the most spectacular events in the history of cryptology. The spectacle came not only in the cracking but in the capturing of Enigmas and their code books from U-boats and elsewhere.

LOCAL EVENTS

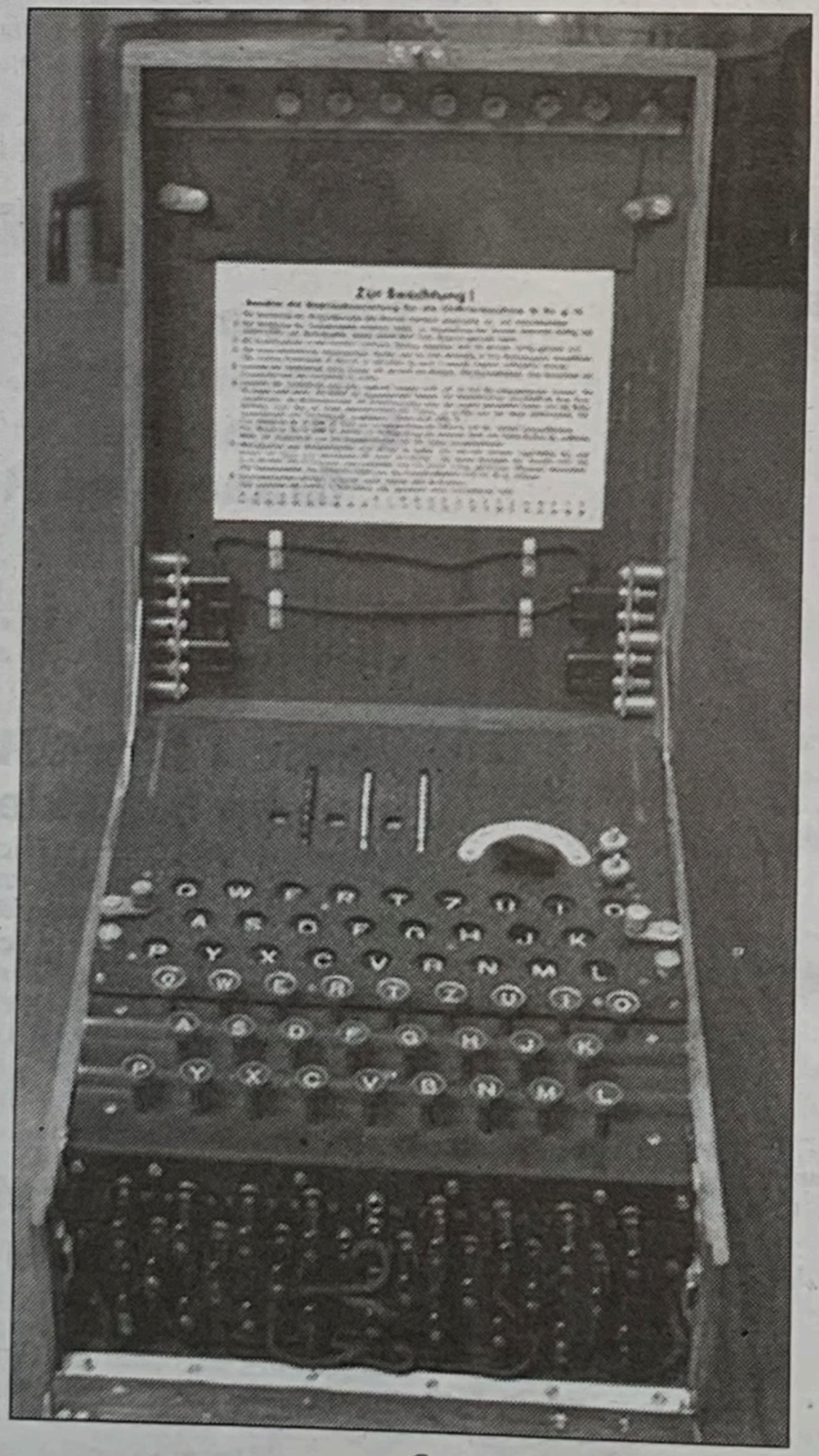
David Weil, curator and executive director of the Computer Museum of America, is host to an Enigma on loan from the National Security Agency in Fort Meade, Maryland. Great numbers of them were "acquired" by the United States after the war, says Weil.

By "acquired" he actually means "seized." The sweep was part of the "postwar salvage effort," he says. "These machines were obviously highly prized, but beyond that, we wanted to gather up as many of them as we could, so they couldn't be used again."

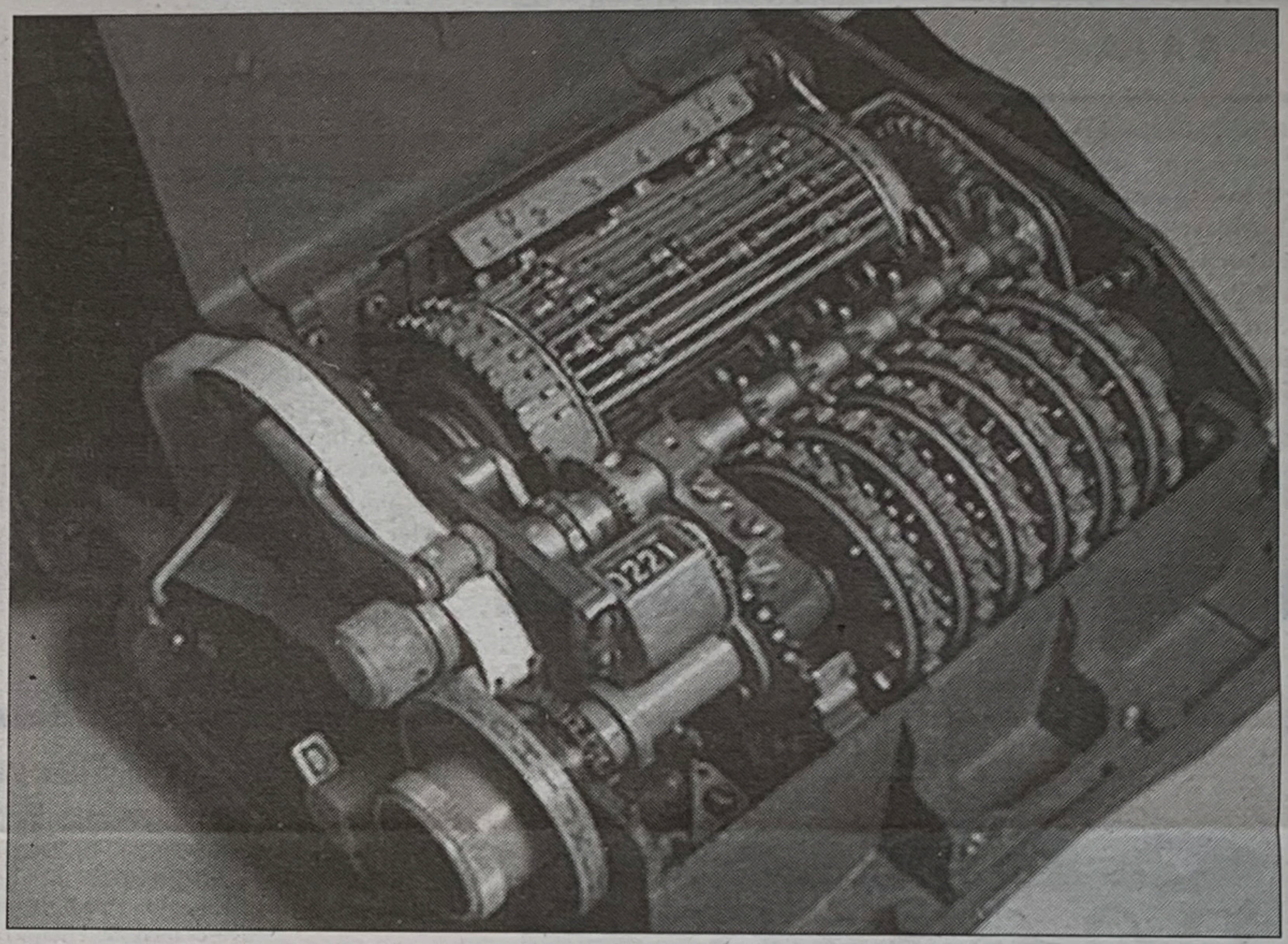
Assigned to decipher the Enigma code was a group of geniuses. Alan Turing, the British mathematician, was among them. Eccentric, to say the least, Turing is believed by some people to have been a high-functioning autistic — a savant of a sort. Later, he became one of the pioneers of computer science.

What made the Enigma so complicated? Weil explains that instead of merely replacing one letter of the alphabet for another, Enigma's multiple rotors assigned several substitutes to each letter on a revolving basis. Some Enigmas were more complicated than others, the degree depending on the number of rotors. (The Enigma at the museum has three rotors.) At its most daunting, the permutations multiplied "astronomically," says Weil. Even more confounding, the Enigma's operators could change the permutations *daily.*

The goal for the code-breakers was to figure out the system's base code. Turing, along with others (including chess players and crossword-puzzle experts), did it by inventing what they called a *bombe.* "*Bombes* were created first in Poland in the 1930s," says Weil. "Then some of the Polish mathematicians escaped to England and continued to help the British build these machines. Turing worked on one called the Colossus. *Bombes* were essentially computerlike. They may not have been called computers, but they functioned very similarly. They were probably the most advanced machines of their time. What they could do was run through all the permutations in less than two hours. So by ten o'clock every morning we could read all the German messages."



German Enigma code machine



Hagelin M-209-B rotor machine

Not all Enigmas are in museums. "Many are in private hands," says Weil. Sometimes you can see them for sale on eBay. A four-rotor Enigma was sold at a Sotheby's auction to Mick Jagger while he was producing a British-made movie called *Enigma,* which is set in Bletchley Park, Britain's wartime code-breaking headquarters. Jagger's Enigma was used as a prop in his movie, just being released here.

Don't mention an earlier Hollywood movie, *U-571,* to an Enigma aficionado. *U-571* portrayed Americans as the heroes, capturing an Enigma from a U-boat, when in reality the British made the crucial captures.

The National Security Agency has also lent to the museum what's called an M-209. The M-209 was an American-made machine of the World War II period. It was much less complicated but even more portable than the Enigma. "It would fit into a little canvas carrying case that you could strap to your belt," says Weil. They were issued by the Signal Corps for use by field units.

Writing and deciphering codes is still a challenge today, according to Weil. "Encryption is used every time you send an e-mail. There is voice encryption for telephones. And cryptologists continue to work on national security issues. As a nation we have tried not to export technology that might fall into the hands of the 'evil doers.' But at the same time we want instant communication. So it's a trade-off between wanting the whole world connected in some form and also wanting to make sure that some people don't use that technology for nefarious purposes."

The main focus of the exhibit is the connection between encryption and computers. But this summer Weil wants to invite one of the famous Native American "code talkers" to speak at the museum. "A couple of them live here in San Diego." Code talkers were employed by the military to use their own languages to encrypt voice communications. Choctaws were used as far back as World War I. For code work during the Second World War, they were joined by Kiowas, Winnebagos, Seminoles, Navajos, Hopis, Commanches, and Cherokees. "We want to get one of their radios here, too," says Weil. "We hope to borrow it from a local collector."

— *Jeanne Schinto*

"Secrets, Lies and Teletypes"
Exhibit on the history of
code-breaking from
ancient times to the present
Tuesdays–Sundays,
10:00 a.m.–5:00 p.m.
Through March 2003
Computer Museum of America
640 C Street, downtown
$2; seniors, military, students,
children 3 and over, $1;
children under 3, free
Info: 619-235-8222 or
www.computer-museum.org