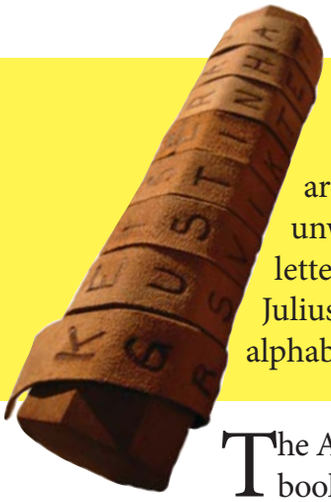
Fun Facts about Cryptology*

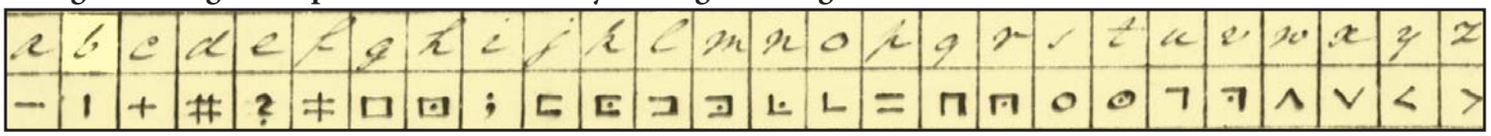
*the study of secret writing and codes



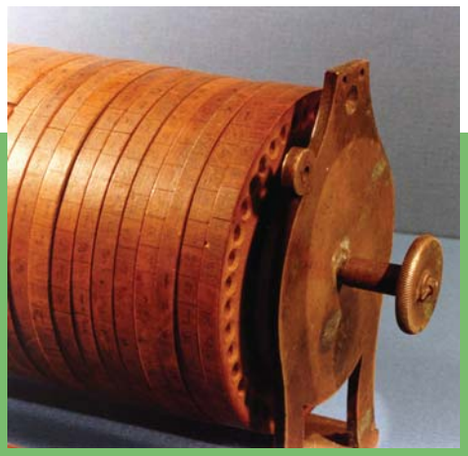
Cryptology began in the ancient world. The ancient Greeks used a ***scytale***, in which the person sending a message wound a strip of cloth around a stick, wrote the message vertically, filled in some random letters, unwrapped the strip, and sent it to the recipient. The message looked like random letters until wrapped around a stick the same size as the original. Roman emperor Julius Caesar is believed to have made a cipher that substituted the letters in one alphabet for another.

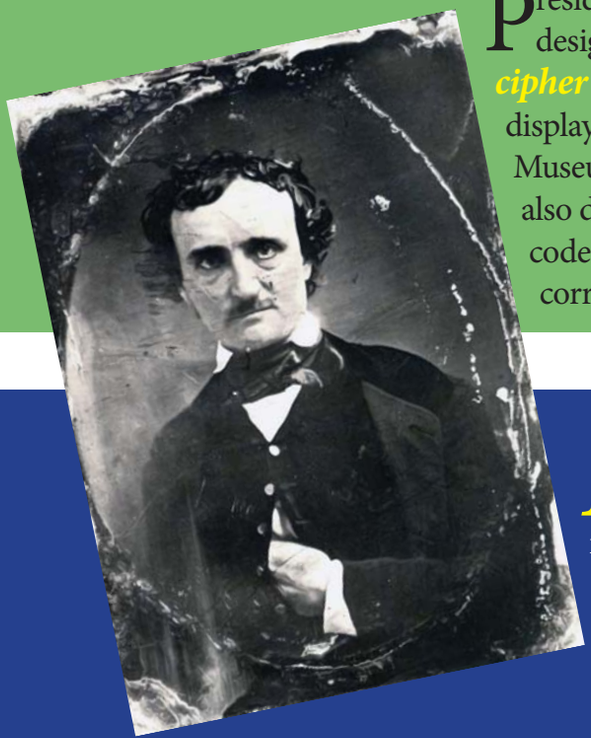
The Arab world also excelled in making and breaking ciphers. Arab authors published books on mathematical cryptology as early as (in Western dating) 1000 CE.

George Washington's alphabet code sheet. Try writing a message!



In the American colonies, some people used cryptographic systems for their personal mail—the postal system often was unreliable, and letters might go astray.





President Thomas Jefferson designed a ***wheel-based cipher machine***, which is likely on display in the National Cryptologic Museum (shown right). He also developed a mathematical code, or cipher, for his personal correspondence.

Edgar Allen Poe, author of dark and mysterious stories, edited a magazine in which he challenged readers to send him encrypted messages to solve. His success rate was 100%—he published only the messages he could solve!

In the 1920s, ***Elizebeth Friedman*** broke codes used by smugglers violating Prohibition laws, and helped the Coast Guard round up some criminal gangs. (Yes her name is spelled *Elizebeth*!)

In World War I and World War II, the United States recruited Native Americans as radio communicators or ***codetalkers***; their native languages served as a "living code" that was never "broken" (deciphered) by the enemy.

In World War II, the Japanese Navy set a trap for the American Navy centered around the island of Midway; US cryptanalysts solved a Japanese code and read the enemy's plans in advance, which allowed the US Navy to set its own trap. The ***Battle of Midway*** was long and close, but American forces dealt the Japanese a defeat from which they never recovered.

After World War II, many of the first computers were created to make or break codes.

Heard of Americans spying for the Soviet Union in the Cold War? US cryptanalysts solved a system for encoding and decoding messages, or cryptosystem, used by the Soviet espionage services, and gave the FBI hundreds of tips that enabled them to unmask dozens of these spies.

It is not true, as some books say, that NSA was a "secret" organization when it was established in 1952; however, there was little public awareness of its work, and some people joked that the initials stood for "No Such Agency."

To read more about these and other cryptologic subjects, visit the Center for Cryptologic History at **www.nsa.gov** or drop us a line at **history@nsa.gov**.