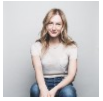
Ancient Uses of Cryptography: Four Examples that Pre-Date the Internet

medium.com/tokenring/ancient-uses-of-cryptography-four-examples-that-pre-date-the-internet-14679ae4f509

Melanie Shapiro

August 15, 2017



Melanie Shapiro

Aug 15, 2017

·

4 min read

·

One Greek tyrant hid messages on the scalps of his slaves' heads, Thomas Jefferson invented a cipher wheel, with about 1,000 letters that had to be lined up just the right way to be decoded, and in World War II, an extremely advanced machine at the time, the Enigma, helped the Nazis gain advantage, and then helped the Allies win once they cracked it.

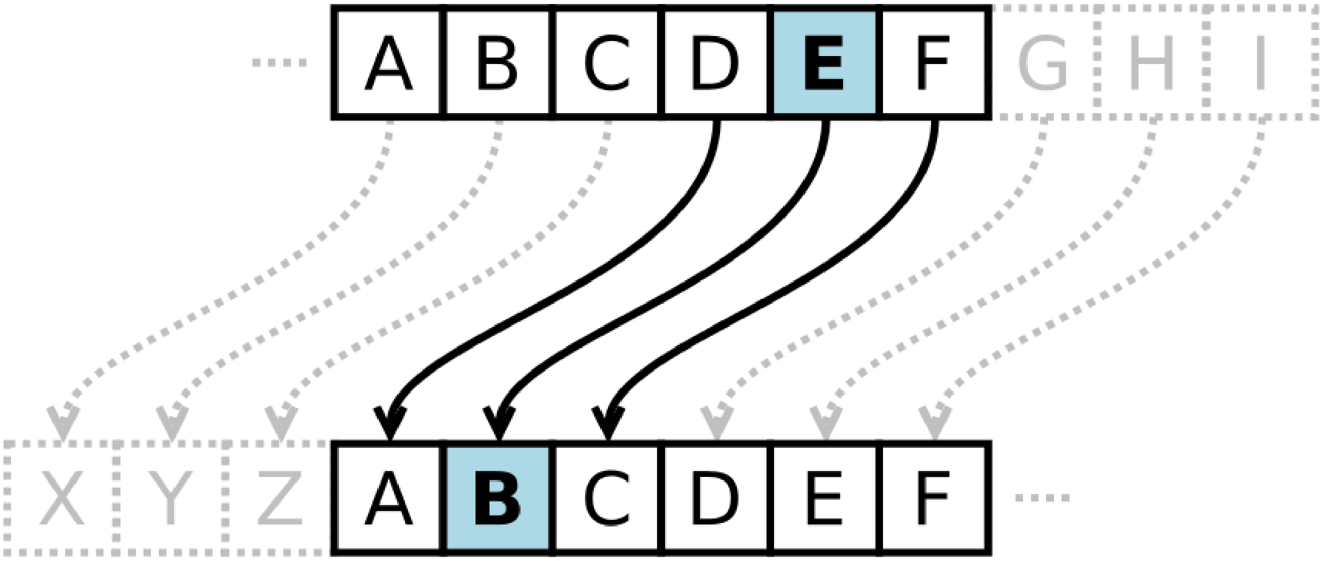
Since about 1900 BCE, when unusual hieroglyphics were written on a nobleman's tomb in Egypt, to today, we've been inventing new forms of cryptography, or the art and science of keeping information secure. It turns out protecting information has been extremely important to humans for a long time, and, because we now share our personal data more than ever before, it’s a good time to look back and understand a bit about how we got here.

Here are some highlights of cryptographic inventions over the past 2500 years:

The Scytale. Fighting wars has always been a big driver of innovation in cryptography. Around 500 BCE,Spartans who were trying to send secure messages during military campaigns wrapped a piece of parchment with a message around a certain kind of cylinder called a Scytale. To decrypt the message, the recipient had to have a cylinder of the same size. While it wasn’t the most sophisticated method by modern standards, it may have seemed pretty ingenious at the time.

Head tattoos. Around the same time, a cruel Greek leader seeking to revolt against the King of Persia, tattooed that conspiratorial message on a slave’s head, waited for his hair to grow back, and sent him to another rebellious leader with instructions to start a rebellion. Although the King ultimately beat back the attack, the message itself seemed to work! This is more an example of stenography than pure cryptography, as the message itself is hidden but readable when found, but highlights our thinking in early information security.

The Caesar cipher. A little over 2,000 years ago, Julius Caesar developed a simple system to send secure information to his troops. It was all about substituting certain letters for others, typically by shifting the letters by a predetermined number, according to researcher Nicholas McDonald. That algorithm is what we would call a cipher, and since Caesar’s invention, we’ve made cipher keys much more secure and advanced. Though it may sound obvious, if you want encrypt and decrypt information, you are going to have to choose a kind of cipher to do so.



The Caesar cipher

The Enigma Machines. The cipher machines, famous for their use by the Nazis in World War II, were made up of electronically-connected rotors. Although the messages, which were deciphered with a set of daily keys, were hard to crack, the whole operation proved breakable after a lot of hard work (British mathematician Alan Turing was a very important figure behind that effort). Because Germany's movements became predictable, that work helped turn the tide of the war and sped up the Allies' victory.

A Watershed Invention: Asymmetric Key Encryption.

All of the above inventions involved a concept called symmetric key encryption, which relied on shared secrets to crack open information. It means anyone looking to access the private information has to use the same key.

However, in the 1970s cryptologists Whitfield Diffie and Martin Hellman made a landmark invention: **Asymmetric key encryption.** It's the concept that both HTTPS (the popular protocol used to access a secure web server) and the secure element within Token rely on to keep your information completely private.

The principles behind it are genius. Instead of a shared key that codes and decodes information, the key for encrypting the information is different from the key that decrypts it — that way there is no longer a shared, secret key. With this invention, in order to share a secret message, you no longer even have to know the person you are sending it to. Most importantly, for people like us who care deeply about safe authentication and identity protection, the private key itself is never communicated at all, and that means no more shared secrets.

While the Diffie-Hellman protocol has been widely applied, at Token we believe its principles haven't been fully listened to. Across the globe, we are still using shared secrets to authenticate our identity when we type in passwords (read more about why shared secrets are so bad here). And in the US, we've only begun a major move to chip-enabled credit cards in the past few years (though the first version was introduced in Europe in 1994).

We've Built the Interface to Make Modern Cryptography Work

At Token we apply the lessons of history to today's advanced technology (like miniaturization and decentralization) to the Token ring. Each ring contains a secure element — a tamper-resistant, miniature chip that stores your private keys. We designed fingerprint and proximity sensors into the ring so that you're the only one who can authenticate your identity. And we integrate all this technology into one, single device inspired by natural movement and solely dedicated to authentication. This all means that, throughout your day, as you use Token, you are not communicating your personal, identifying data with anyone.

What to learn more about Token? It's all right here.

In the coming months, we will continue to initiate conversations — online and offline — about the importance of changing the way we safeguard our most valued data and the way we authenticate our identities. For alerts on how you help us build a secure digital future, sign up for our newsletter below.