UNITED STATES AIR FORCE ACADEMY

Timeline of Codes and Ciphers

This is an incredibly brief timeline of some ciphers and codes used to protect information throughout the ages.

~500 BCE—Spartans with the Scytale

A strap of leather that had to be wound around a specifically carved staff to form the correct message.

A

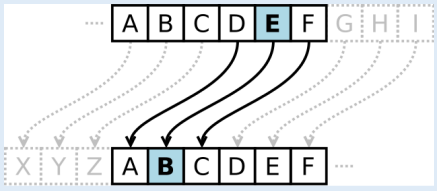
~440 BCE—Greeks with Steganography

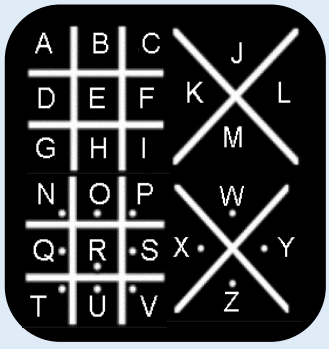
A slave had their head shaved and the message to be concealed was tattooed onto the scalp. The "messenger" was sent on their way once their hair grew back to cover the message.

~100 BCE Caesar Cipher

One of the earliest known ciphers used by Julius Caesar to communicate with generals in the field.[1] This shift cipher moves or shifts letters down by a selected number of characters. The message "easy" with a shift of three is encoded as "BXPV."

e	a	s	y	← Plain text
B	X	P	V	← Cipher text





Ancient times, resurfaced in 18th Century—

Freemason or Pigpen Cipher

This cipher was believed to have originated with Hebrew rabbis in ancient times, and evidence that the Knights Templar using one during the Christian Crusades in the Middle Ages. It disappeared and resurfaced when some Freemasons used the cipher to keep records and rites private.[2]

A. CC SSA 3.0: https://commons.wikimedia.org/wiki/File:Skytale.png, 1. https://ghostvolt.com/articles/cryptography_history.html, 2. https://www.freemason.com/what-is-masonic-cipher/

UNITED STATES AIR FORCE ACADEMY

Timeline of Ciphers and Cryptography

1467— Cipher disk from Leon Battista Alberti

This is a polyalphabetic cipher system that uses two mobile concentric disks which can rotate. The disk has two alphabets, one fixed (stabilis) one moving (mobilis). By rotating a disk, it shifts an alphabet to the next letter.

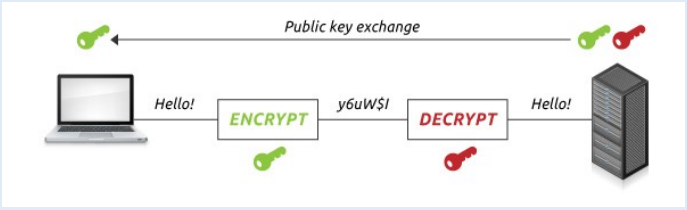
B

~1923—German Enigma Cipher Machine

Used in the early- to mid-20th century to protect commercial, diplomatic, and military communication. It was famously used by Nazi Germany during World War II to obscure military information, messages and troop movements. Alan Turing and the team at Bletchley Park helped decode or crack the Enigma.

1970's — Asymmetric Encryption

Also known as public key cryptography, this uses separate keys for encryption and decryption: a public and a private key. The keys are typically two large strings of numbers paired together. One key is public, can be shared with anyone and they can use it to encrypt a message. The other is the private key which is kept secret. The private key is needed to decrypt the message encrypted with the public key.[3] This is secure because it is mathematically "hard" to solve for current computers.



C

Next Gen and Post-Quantum Cryptography (PQC)

A current concern is as quantum computers grow in power, they will be able to break traditional asymmetric encryption. Cryptographers are actively developing "post-quantum asymmetric cryptography algorithms" or PQC algorithms. These algorithms are based on mathematical problems that are "hard" for quantum computers as well. The US Federal agency NIST has an on-going competition for developing quality PQC algorithms that can securely used, even as quantum computers grow in power and usefulness.

B. CCSA2.0 Generic Arnold Reinhold; C. Image from https://www.digicert.com/faq/ssl-cryptography.htm; Point of contact: Dr. Shannon Beck - Shannon.Beck@afacademy.af.edu