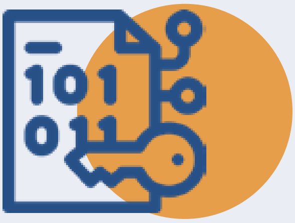
COLOMBIA POTENCIA DE LA VIDA

Timeline about the previous reading

TIC

Timeline of Cryptography History



1900 BC:

The first known evidence of cryptography appears in an inscription in Egypt's tomb of Khnumhotep II. Unusual hieroglyphic symbols are used for dignified representation.

100 BC:

Julius Caesar employs a substitution cipher known as the Caesar cipher. The shift-by-3 cipher is a historic mention, replacing each character with another three positions ahead.

16th Century:

Vigenere designs a cipher using an encryption key. Although easily breakable, it introduces the concept of encryption keys determining message secrecy.

19th Century:

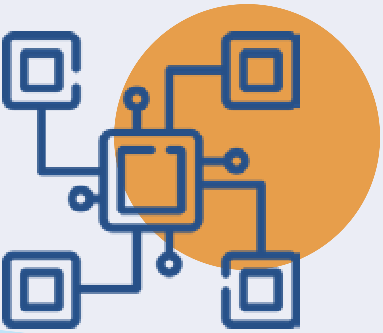
Hebern introduces the Hebern rotor machine, an electro-mechanical contraption using a rotating disc and letter frequencies.

World War I:

The Enigma machine, invented by Arthur Scherbius, is heavily used by German forces. It uses multiple rotors, and its cipher is eventually broken by Poland, leading to the transfer of technology to British cryptographers.

Post-World War II:

Cryptography gains commercial attention, with businesses seeking to secure data from competitors.



Early 1970s:

IBM forms a crypto group and designs Lucifer, a cipher later accepted as the Data Encryption Standard (DES) in 1973.

1997:

DES is broken by an exhaustive search attack due to its small key size. NIST requests proposals for a new block cipher, leading to the acceptance of Rijndael, known as the Advanced Encryption Standard (AES).

21st Century:

Advancements in quantum computers prompt considerations of Post Quantum Cryptography. NIST seeks public help for quantum-resistant algorithms, with four finalists announced in 2020.

TALENTO TECH
AZ | PROYECTOS EDUCATIVOS
UTP Universidad Tecnológica de Pereira