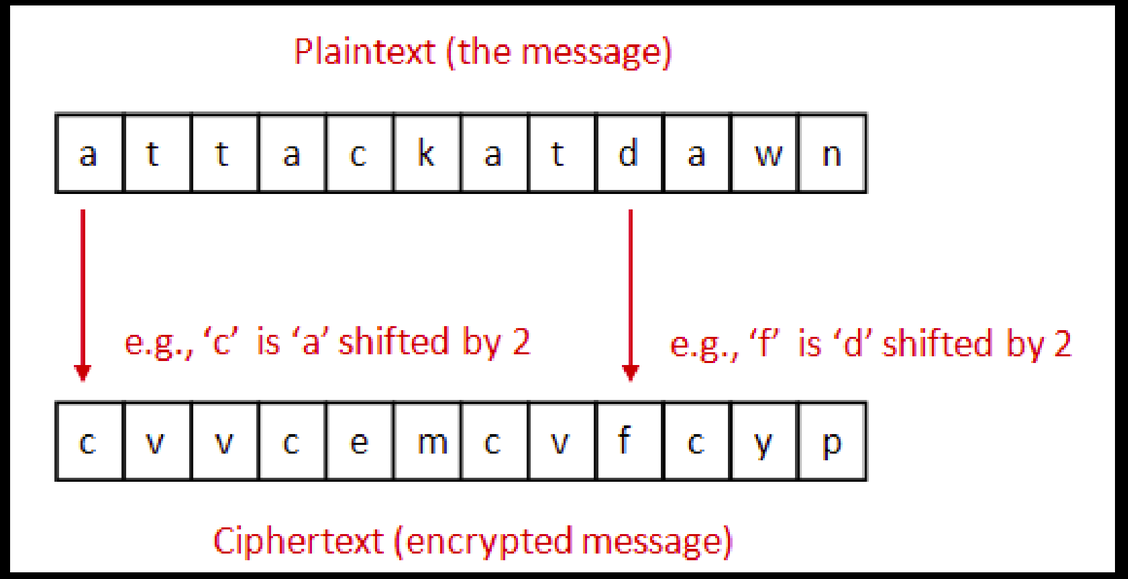
Cryptography :

the study of Secure Communication Techniques

Cryptography - Yesterday

- The evolution of human civilizations as different tribes and kingdoms demanded secret communication methods.
- With the evolution of mode of communication [from pictorial representations to electronic] the feel and depth of cryptography has evolved .

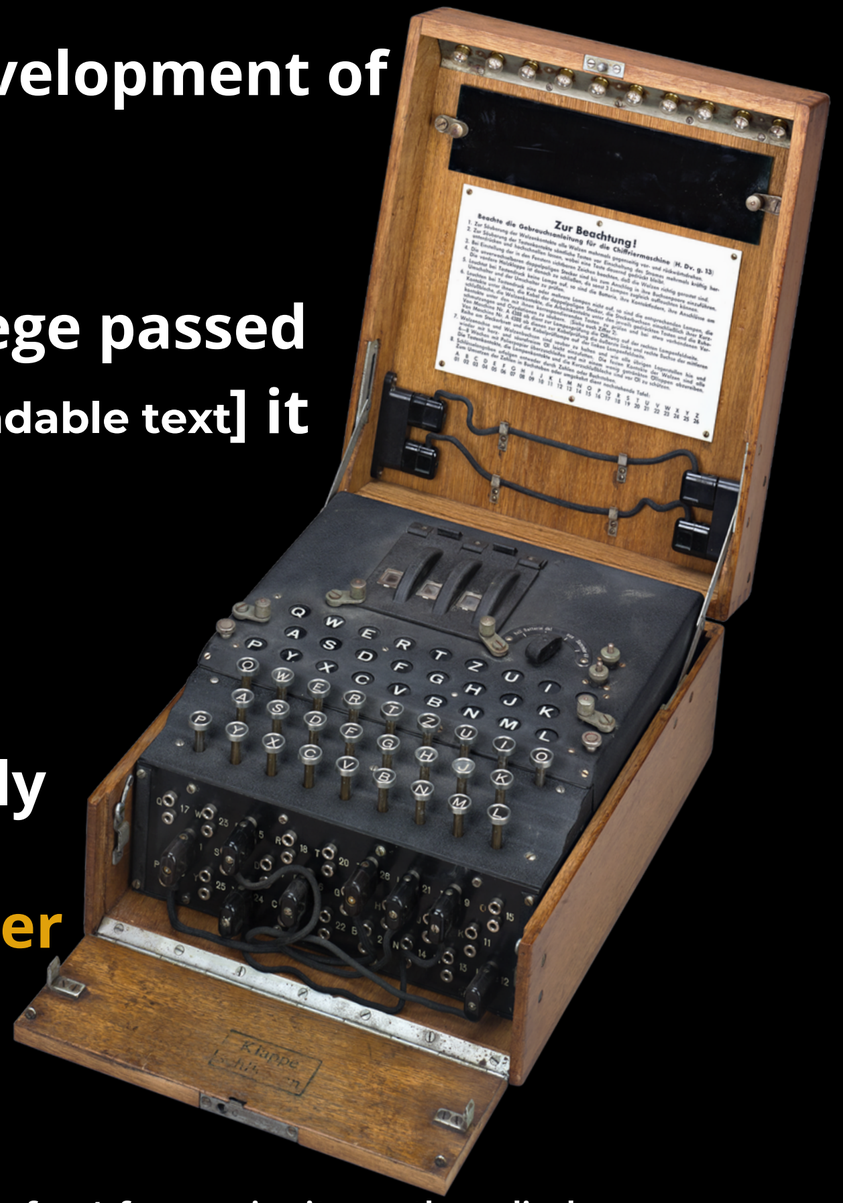


(In the slide you can see an Egyptian hieroglyph which is a method of pictorial scripting were only extensively educated privileged like Pharaoh could read. And the 2nd image is a demo of Caeser cipher which is considered the 1st of its kind where alphabets are shifted in an particular pattern.)

- The World Wars played a significant role in the development of Cryptography into a field of extensive research.

- Encrypting [converting into a non-readable code] the messege passed over the Radio and Decrypting [converting back into readable text] it back on the other end decided the victories.

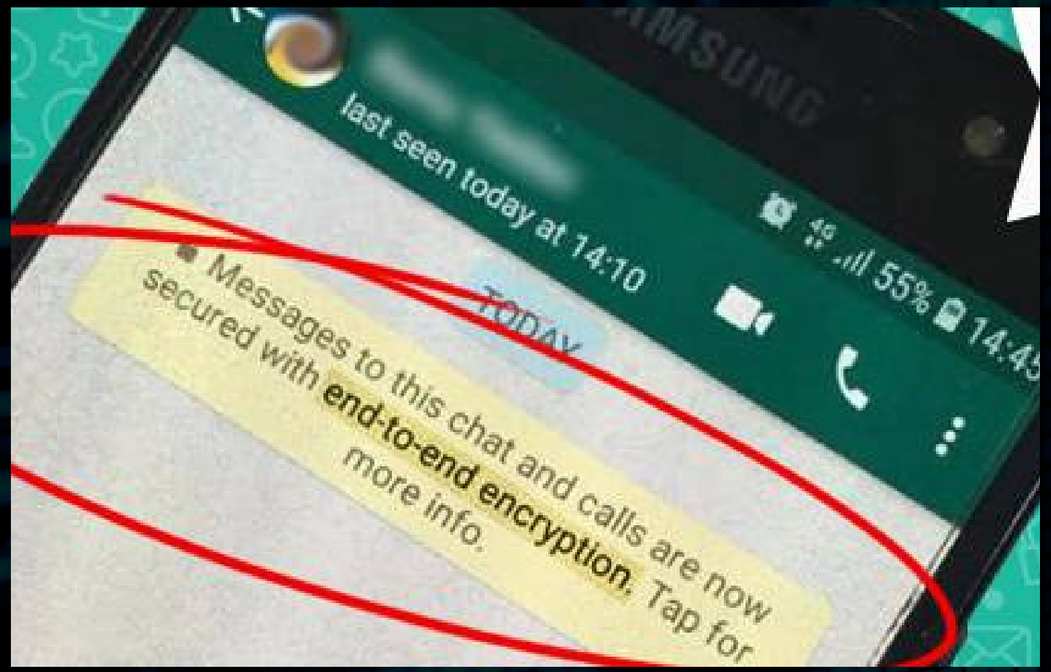
- By that time rather than being just linguistically tricky, cryptography started to be more extensively mathematical, making use of information theory, compuational complexity, abstract algebra, number theory, finite mathematics & statitics.



[The image in the slide is of an Enigma machine. This device was used to encrypt & decrypt the message before/after passing it over the radio, becasue radio interception were very easy. So even if the enemies get the radio signals, they can only make use of the info only if they have an Enigma machine with exactly the same setup.]

Modern Cryptography

Today, Privacy and security we are bothered about much is backed by cryptography.



We can roughly classify the modern cryptogtraphy into:

- Symmetric-key cryptography
- Public-key cryptography
- Cryptographic Hash Functions

Symmetric-key cryptography

A single secret key is used for both encryption and decryption functions.

Public-key cryptography

- The public key is used to encrypt and the private key is used to decrypt.
- Very popular today

Hash Functions

A mathematical function that converts every input it recieves into a unique output of fixed lenth.

Cryptography & Blockchain

- Modern computing itself has no ways out of Cryptography.
- And the fair share of the entire blockchain concept is deep-rooted on Cryptography.
- Public-key, Private Key, Hash values, merkle roots, etc shows how blockchain and cryptography are closely related.

Future

More computational power demands more complex security measures.

Quantum computing

(which is still in the cradle) is capable of entirely uprooting all the norms of Cryptography we have today.

Such a disruption will affect all the technology domains.