ENCRYPTION

WHAT IS AN ENCRYPTION?

Method by which a text or data is converted from a readable form to an encoded version

The encrypted code can only be decoded by those who have access to a decryption key

Important method for data security

Commonly used on the internet to protect user information such as paswords, payment information

HISTORY OF ENCRYPTION

Comes from the Greek word KRYPTOS → hidden or secret

Used also in the ancient times (Egyptian)

Popular in military → the most famous encoding equipment was the ENIGMA machine

In 1976 → Whitfield Diffie and Martin Hellman invented the public key

Today → widely used both in the commercial and consumer realms

THE IMITATION GAME (2014)

HOW DOES ENCRYPTION WORK?

Plaintext is encrypted (encoded) using encryption (codes) algorithm and a key → generates the ciphertext (encoded text) which can only be viewed and decrypted (decoded) with the correct key.

TWO TYPES OF ENCRYPTION

Symmetric ➔ program genrates encrypted file which sent to the recipient + the decoding key (separately); the recipient decodes the message through the same app. Fast but not safe process; used for e-commerce transactions.

Assymetric ➔ two keys (public; private). Public key can encode the data; private key is used to decrypt the data. More secure but slower process.

QUESTIONS

What is the encryption?

Where does the word encryption come from?

What is the name of the most well-known encoding equipment?

Who invented the public?

When did Whitfield Diffi and Martin Hellmand invent the public key?

What is a plaintext?

What is a ciphertext?

What are the names of the two types of encryption?

Thank you for your attention!