**CRYPTOGRAPHY**

Encryption is a process for converting the source text into encrypted text with a particular key. Reversed process, decryption, allows you to read encrypted data if you have the key.



Since there is civilization, there is a need for encrypting messages. Thus, the Spartans used a stick around which parchment is ribbed, scytale, to encrypt their messages. A secret message was written on the parchment. In this example of encryption, the key is the shape of the stick.

**CAESAR CIPHER**

Gaius Julius Caesar used the message encryption method in which each letter in the message is replaced by a letter three places after it in the alphabet (A to D, B to E, etc.). To encrypt Caesar's cipher, we can also use Caesar's disk so that the letters in the upper circle are replaced by corresponding letters from the lower circle.

Although Caesar was a great military general, he did not seem to be very good in math, as his encryption could be broken in up to 26 attempts. Today, Caesar’s cipher is any encryption method where the number 3 is replaced by a number smaller than 25.

**ENIGMA**

The Enigma machines are a series of electro-mechanical rotor cipher machines, mainly developed and used in the early to mid-20th century to protect commercial, diplomatic and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War II. Alan Turing, a Cambridge University mathematician and logician, provided much of the original thinking that led eventually to breaking the Enigma in the mid-20th century.

INSTRUCTIONS FOR ENIGMA ENCRYPTION MACHINE:

1. Define an initial gear order.
2. Define the initial key, 3 characters long. Once gear order is set, the key defines the gear orientations.
3. Write the text that you wish to encode. Do not use spaces or punctuation.
4. The right side gear is the Text wheel. To begin encryption, find the 1st letter of your message and align it with the arrow next to this wheel. Read the corresponding letter that appears at the top arrow of the gear 1, which is the left gear on the board. Write this letter right below the letter you just encoded. Next set the Test wheel to the second letter of your message. Read the encoded letter on the 2nd (middle) gear. Repeat this process of going from the left gear (1) to the center gear (2).

**VISUAL CRYPTOGRAPHY**

How to hide or safely encrypt a picture? Is it possible to share a secret amongst a group of friends, each of whom is allocated a share of the secret in such way that the secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own?

Visual encryption is the method of sharing the secret image to the corresponding number of participants so that no participant can independently detect the secret. Visual encryption was introduced by Adi Shamir and Moni Naor in 1994, after which it is rapidly evolving.

**PUBLIC KEY CRYPTOGRAPHY**

When encrypting with public key cryptography, Alice has a pair of keys: the public key *E*Alice which other users use to encrypt messages to Alice and the secret key *D*Alice which Alice uses to decrypt the received messages. A public key is available to everyone, and the secret key is only available to the owner. We can imagine that every person has their own key and lock. Its lock is available to everyone, and the key is just for her/him. When Bob wants to send a message to Alice, he puts it in the box, locks with Alice's lock and sends it. Only Alice has her secret key and only she can unlock the box and read the message that is intended for her.

Today, when using public key cryptography, they use procedures based on NP-difficult mathematical problems.

INSTRUCTIONS FOR MICRO:BIT
Micro:bit for encryption

1. Button B: Select the public key of the person you want to send the message
2. Button A: Choose the letter you want to encrypt
3. Key A and B key: encrypt the selected letter
4. Repeat steps (ii) and (iii) until you encrypt all the letters of the text

Micro:bit for decryption

1. Button B: Choose your secret key
2. Button A: Choose the letter you want to decrypt
3. Key A and B key: decrypt the selected letter
4. Repeat steps (ii) and (iii) until you decrypt all the letters of the text