# Project Report

# On

# Cryptography

# (Minor)

**Submitted To : Teachnook**

**Dated : 21-03-2023**

# Table of Content


1. What is cryptography ? ..... 3

2. What is cipher ? ..... 3

3. Classical Ciphers : ..... 5

(i) Substitution cipher: ..... 5

(i) Substitution Cipher : ..... 6

(ii) Rot13 : ..... 7

(ii) Transposition cipher ..... 8

(i) Railfence : ..... 8

(ii) Column Transposition : ..... 9

4. Modern Ciphers: ..... 11

Types of Modern ciphers ..... 11

❖ Based on the type of key used ..... 11

(i) Symmetric Key Cryptography: ..... 11

(ii). Asymmetric Key Cryptography ..... 12

❖ Based on the type of input data ..... 14

(i) Block cipher: ..... 14

(ii) Stream cipher: ..... 14

## Topic :

**Make a report on different types Of Ciphers with examples & screenshots of the Implementation (You can use online tools to do Ciphering)**

### 1. What is cryptography ?

"Cryptography" comes from the Greek words kryptos, meaning "concealed, hidden, veiled, secret, or mysterious," and graphia, meaning "writing"; thus, **cryptography is "the art of secret writing.**

Cryptography is the study of data security through Encryption technique, which describe the encryption process and techniques used.

### 2. What is cipher ?

A cipher is an algorithm which is used to encrypt or decrypt the data. Plain text is converted in cipher text with help of this. The transforming process is performed using a key.

This key is like a pattern to encrypt the data. If we wanted to decrypt the data then we need to reverse the process.

**Example:**

Consider A is represented as D, and B is represented as E, it means all alphabets are replaced with the third subsequent alphabet. Then **Apple** will be written as:

A = D

P = S

P = S

L = 0

E = H

So, **apple** in plain text before encryption is **APPLE**.

This idea or algorithm to replace the alphabet with third subsequent alphabet is known as Cipher.

The third subsequent letter is used to encrypt the data, this secret is considered as a key.

If we want to use this above-mentioned cipher then we must know the rules and the key.

**Types of Ciphers :**

**Ciphers are of two main types: classical and modern.**

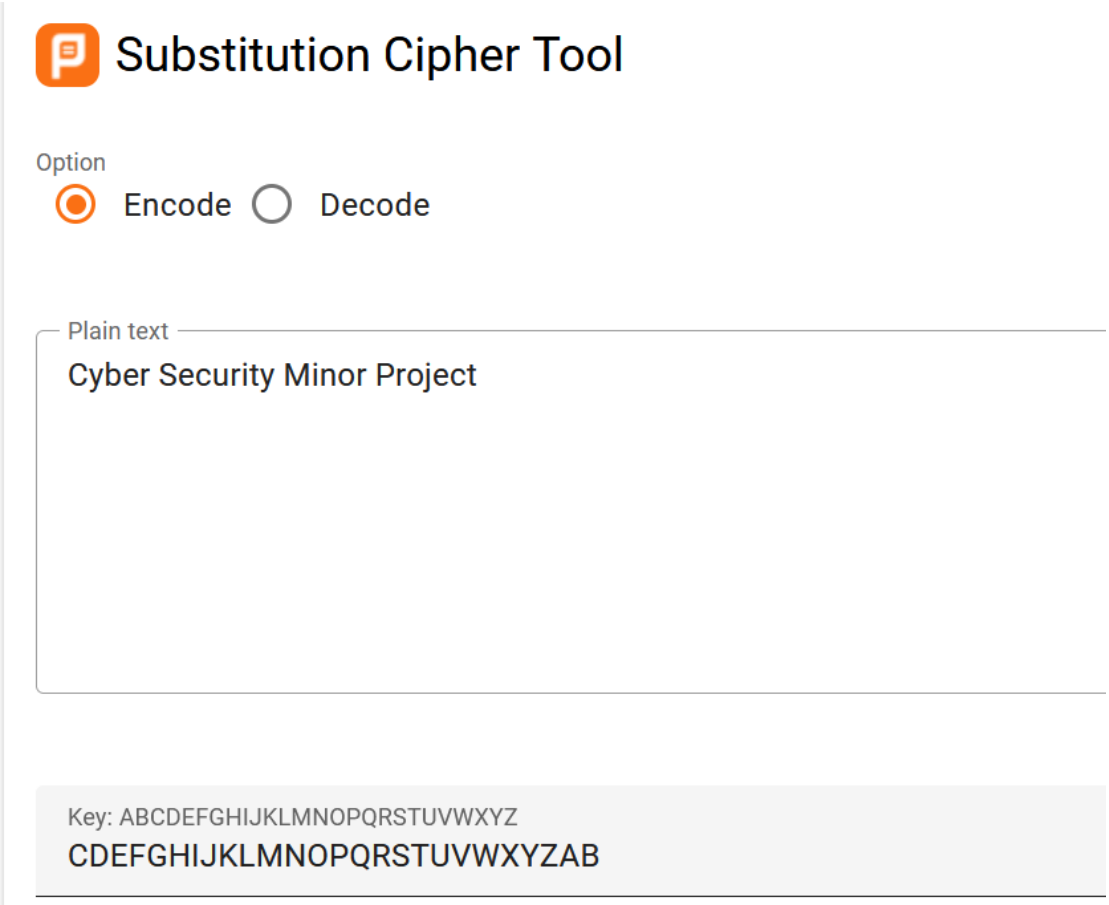
**3. Classical Ciphers :** Classical ciphers are the most basic type of ciphers, which operate on letters of the alphabet (A–Z). These ciphers are generally implemented either by hand or with simple mechanical devices. Because these ciphers are easily deciphered, they are generally unreliable

**(i) Substitution cipher:** The user replaces units of plaintext with ciphertext according to a regular system. The units may be single letters, pairs of letters, or combinations of them, and so on. The recipient performs inverse substitution to decipher the text. Examples include the Caeser cipher, Hill cipher and ROT13 .For example, "HELLO WORLD" can be encrypted as "PSTER HGFST" (i.e., H=P, E=S, etc.).

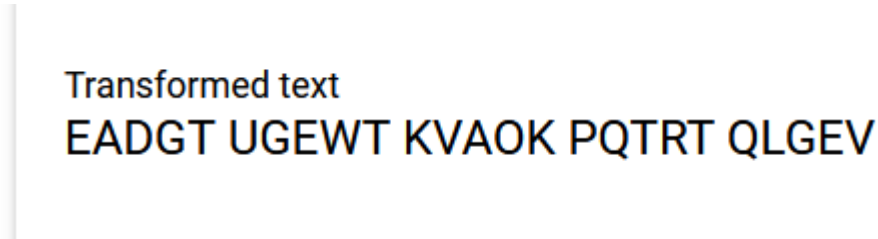
Following are the examples of substitution cipher:

## (i) Substitution Cipher :

Reference Link :https://planetcalc.com/7984/




**Output is :**



## (ii) Rot13 :

Reference Link : https://www.cryptool.org/en/cto/caesar

Input (plaintext)

```
Hello World
```

Encrypt Decrypt

Output (ciphertext)

```
Ifmmp Xpsme
```

Alphabets replaced with :

Plaintext alphabet

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
```

Ciphertext alphabet

```
BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzA
```

**(ii) Transposition cipher**: Here, letters in the plaintext are rearranged according to a regular system to produce the ciphertext. For example, “CRYPTOGRAPHY” when encrypted becomes “AOYCRGPTYRHP.” Examples include the rail fence cipher, route cipher, column transposition etc.

## (i) Railfence :

Reference Link : https://www.cryptool.org/en/cto/railfence

Plaintext:

```
Cyber Security Minor Project
```

Encrypted text:

```
Cuoty crnrcbei iPeeS tMrjryo
```

Rendering:

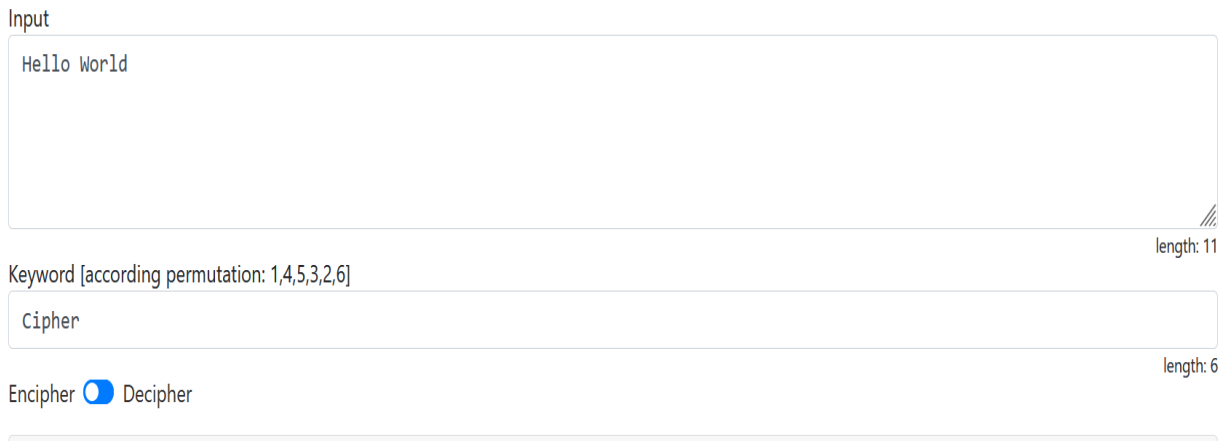
```
C       u       o       t
 y     c r     n r     c
  b   e   i   i   P   e
   e S     t M     r j
    r       y       o
```

---

## (ii) Column Transposition :

https://www.cryptool.org/en/cto/transposition

Column transposition uses a rectangular arrangement (also called a matrix or grid), consisting of several rows (as many as are necessary to enter the plain text).



| C | i | p | h | e | r |
|---|---|---|---|---|---|
| 1 | 4 | 5 | 3 | 2 | 6 |
| H | e | l | l | o | W |
| o | r | l | d | | |

</> Show / modify code

Output [2 non-alphabet characters have been deleted]

```
Hoolderllw
```

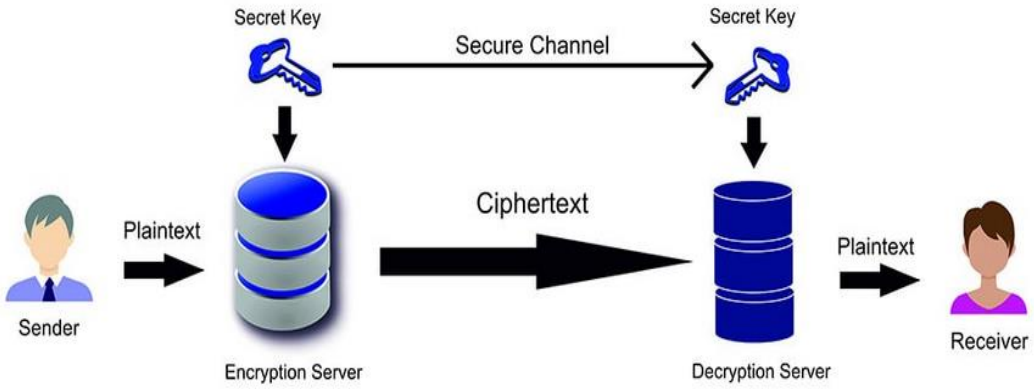
## 4. Modern Ciphers:

Modern ciphers are designed to withstand a wide range of attacks. They provide message secrecy, integrity, and authentication of the sender. A user can calculate a modern cipher using a one-way mathematical function that is capable of factoring large prime numbers.

## Types of Modern ciphers

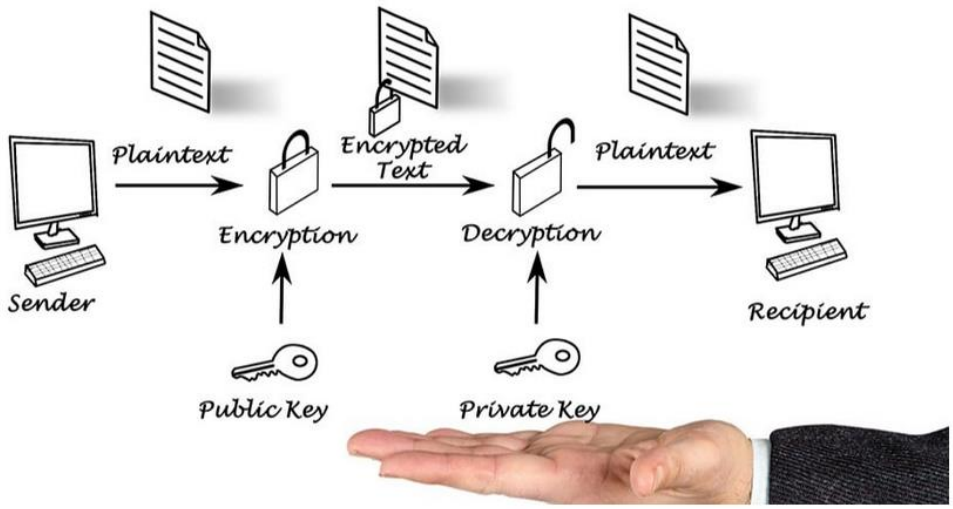
- **Based on the type of key used**

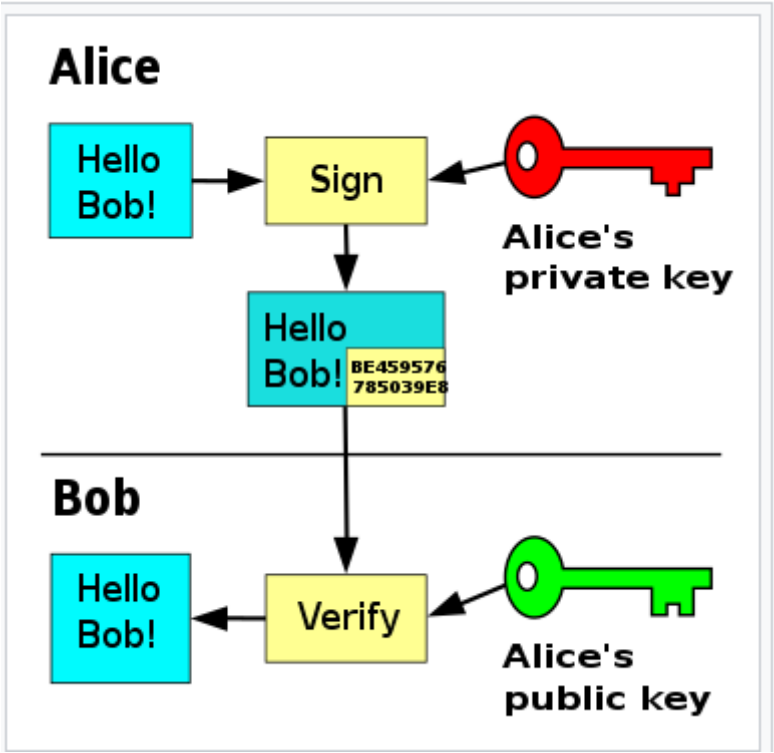
**(i) Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).




Symmetric Cryptography

**(ii). Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.




## Asymmetric Key Cryptography

❖ **Based on the type of input data**

**(i) Block cipher:** Deterministic algorithms operating on a block (a group of bits) of fixed size with an unvarying transformation specified by a symmetric key. Most modern ciphers are block ciphers. They are widely used to encrypt bulk data. Examples include DES, AES, IDEA, etc. When the block size is less than that used by the cipher, padding is employed to achieve a fixed block size.

**(ii) Stream cipher:** Symmetric-key ciphers are plaintext digits combined with a key stream (pseudorandom cipher digit stream). Here, the user applies the key to each bit , one at a time. Examples include RC4, SEAL, etc.