

***Name:***

Talha Abid

***Roll No:***

192400002

***Subject:***

Information System

***Submission Date:***

13 April, 2022

***Submitted To:***

Prof. Aleem Awan

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***Cryptography***

Cryptography is an information security tactic used to protect enterprise information and communication from cyber threats through the use of codes.

***Types Of Cryptography*** with the passage of time new tactic and methods are developed as the previous were hacked as well as for enhancing security of information.

**Caesar’s Cipher**

In this each letter in the [plaintext](https://en.wikipedia.org/wiki/Plaintext) is replaced by a letter some fixed number of positions down the [alphabet](https://en.wikipedia.org/wiki/Alphabet) depending upon key.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P.T | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| C.T | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |

* Encryption (Key 3)

Plain Text: TALHA

Cipher Text: QXIEX

* Decryption (Key 3)

Plain Text: QXIEX

Cipher Text: TALHA

**Mono Alphabetic Substitution**

A Substitution for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption and Decryption Process.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P.T | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| C.T | T | R | E | W | Q | Y | U | I | O | P | A | S | D | F | G | H | J | K | L | Z | X | C | V | B | N | M |

* Encryption

Plain Text: TALHA

Cipher Text: ZTSIZ

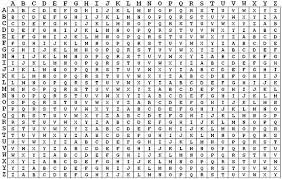
* Decryption

Plain Text: TALHA

Cipher Text: ZTSIZ

**Vigenere Cipher**

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of [polyalphabetic substitution](https://en.wikipedia.org/wiki/Polyalphabetic_cipher). A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the [Vigenere square.](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#/media/File:Vigen%C3%A8re_square_shading.svg)



* Encryption Key:xyz

Plain Text: TALHA

Cipher Text: QYJEZ

* Decryption

Plain Text: TALHA

Cipher Text: QYJEZ

**Rail Fence Cipher**

The rail fence cipher is a form of transposition cipher. It derives its name from the way in which it is encoded.

* Encryption Key:2

Plain Text: TALHA

Cipher Text: T L A => TLAAH

A H

* Decryption

Plain Text: T L A => TALHA

A H

Cipher Text: TLAAH

**One Time Pad**

[Encryption](https://en.wikipedia.org/wiki/Encryption) technique that cannot be [cracked](https://en.wikipedia.org/wiki/Cryptanalysis), but requires the use of a single-use [pre-shared key](https://en.wikipedia.org/wiki/Pre-shared_key) that is not smaller than the message being sent. In this technique, a [plaintext](https://en.wikipedia.org/wiki/Plaintext) is paired with a random secret [key](https://en.wikipedia.org/wiki/Key_(cryptography)).

* Encryption Key:ABCD

Plain Text (+): TALHA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | A | L | H | A |
| 20 | 1 | 12 | 8 | 1 |
| A | B | C | D | A |
| 1 | 2 | 3 | 4 | 1 |
| 21 | 3 | 15 | 12 | 2 |

Cipher Text: UCOLB

* Decryption

Plain Text(-): TALHA

Cipher Text: UCOLB

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| U | C | O | L | B |
| 21 | 3 | 15 | 12 | 2 |
| A | B | C | D | A |
| 1 | 2 | 3 | 4 | 1 |
| 20 | 1 | 12 | 8 | 1 |

**Column Transposition**

A columnar transposition cipher is an encryption method that swaps the columns of a table containing the plain message to obtain an encrypted message.

* Encryption Key:22850

Plain Text: TALHA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 2 | 8 | 5 | 0 |
| T | A | L | H | A |

Cipher Text: ALATH

* Decryption

Plain Text: TALHA

Cipher Text: ALATH

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 2 | 8 | 5 | 0 |
| A | L | A | T | H |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_