

# PROJECT NAME: CYBER SECURITY MINOR PROJECT.

SUBMITTED BY: BASIT SHAMEEM

## Report on Different Types of Ciphers with Examples

Ciphers are cryptographic techniques used to secure the confidentiality of information by transforming it into an unreadable format. Throughout history, various types of ciphers have been developed, each with its own method of encryption and decryption. In this report, we will explore some common types of ciphers, along with examples for each.

### 1. Caesar Cipher

The Caesar Cipher is one of the simplest and oldest known ciphers. It involves shifting each letter in the plaintext by a fixed number of positions down or up the alphabet.

#### Example:

- **Encryption:** If the shift is 3, "HELLO" becomes "KHOOR."
- **Decryption:** To decrypt, shift the letters 3 positions up, turning "KHOOR" back into "HELLO."
- In the example below I have used shift 11.

VIEW	ENCODE DECODE	VIEW
Plaintext ▼	Caesar cipher ▼	Ciphertext ▼
My name is Basit and this is the minor project for cybersecurity with teachnook	SHIFT - 11 a→l + ALPHABET abcdefghijklmnopqrstuvwxyz CASE STRATEGY Maintain case ▼ FOREIGN CHARS Include Ignore → Encoded 79 chars	Xj ylxp td Mldte lyo estd td esp xtyzc aczupne qzc njmpcdpnfctej htes eplnsyzzv

## 2. Substitution Cipher

Substitution ciphers replace each letter in the plaintext with another letter, number, or symbol. The most common form is the Monoalphabetic Substitution Cipher, where each letter is replaced by a single corresponding character.

**Example:**

- **Encryption:** Using a key, "HELLO" might become "FOLLE."
- **Decryption:** With the same key, "FOLLE" can be decrypted back to "HELLO."


VIEW	ENCODE DECODE	VIEW
Plaintext ▼	Alphabetical substituti... ▼	Ciphertext ▼
My name is Basit. This is an example for substitution cipher.	PLAINTEXT ALPHABET abcdefghijklmnopqrstuvwxyz CIPHERTEXT ALPHABET zyxwvutsrqponmlkjihgfedcba CASE STRATEGY Maintain case ▼ FOREIGN CHARS Include Ignore → Encoded 61 chars	Nb mznv rh Yzhrq. Gsrh rh zm vcznkov uli hfyhgrrgfrlm xrksvi.

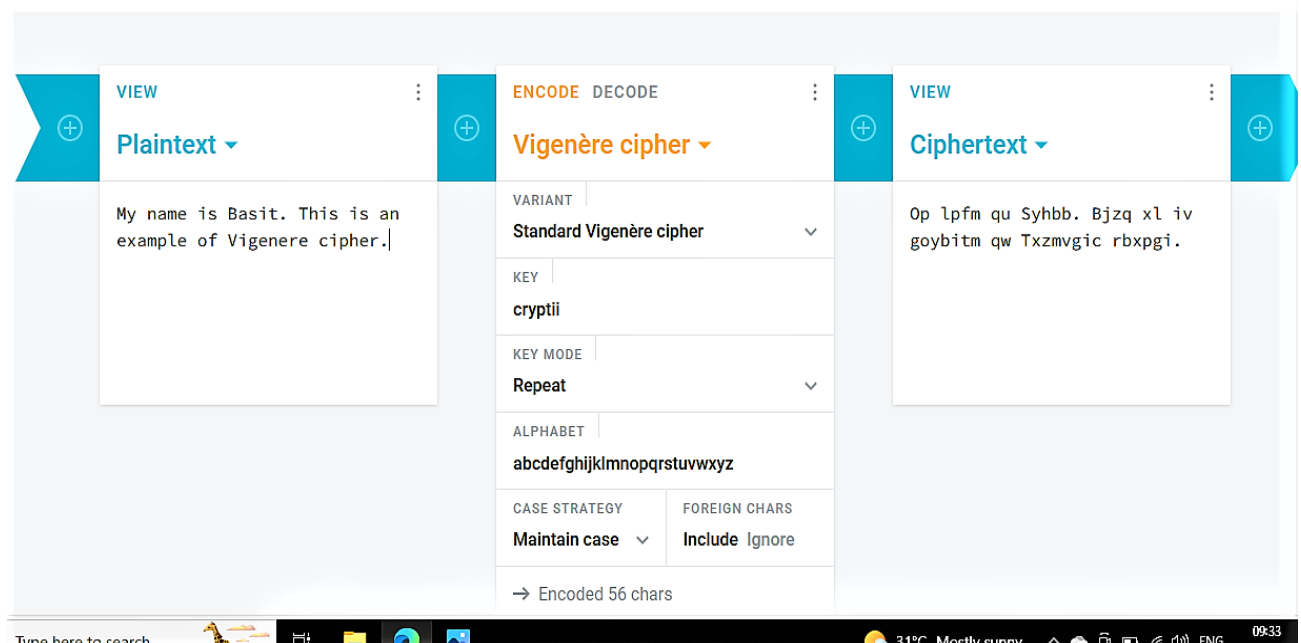
### 3. Vigenere Cipher

The Vigenere Cipher is a polyalphabetic substitution cipher. It uses a keyword to shift letters in a more complex pattern, creating a more secure encryption.

**Example:**

- **Encryption:** Using the keyword "KEY," "HELLO" becomes "RIJVS."
- **Decryption:** By knowing the keyword, "RIJVS" can be decrypted back to "HELLO."

 cryptii



The screenshot shows the cryptii Vigenere cipher tool interface. It has three main panels: Plaintext, Vigenère cipher settings, and Ciphertext. The Plaintext panel contains the text "My name is Basit. This is an example of Vigenere cipher." The Vigenère cipher panel has settings for Variant (Standard Vigenère cipher), Key (cryptii), Key Mode (Repeat), Alphabet (abcdefghijklmnopqrstuvwxyz), Case Strategy (Maintain case), and Foreign Chars (Include). The Ciphertext panel shows the encrypted text "Op lpfm qu Syhbb. Bjzq xl iv goybitm qw Txzmvigic rbxpgi." The interface is in English and shows the system time as 09:33.

### 4. Transposition Cipher

Transposition ciphers rearrange the order of characters in the plaintext without altering the characters themselves. The Rail Fence Cipher is a simple example, where characters are written in a zigzag pattern.

**Example:**

- **Encryption:** "HELLO" in a Rail Fence Cipher becomes "HOLEL."

- **Decryption:** Knowing the pattern, "HOLEL" can be decrypted back to "HELLO."

The screenshot shows the dCode website's interface for the Transposition Cipher tool. On the left, there's a search bar with the text "e.g. type 'random'" and a "Results" section displaying "my\_name\_is\_basit\_this\_is\_an\_example\_for\_tranposition\_cipher". The main right-hand section is titled "TRANSPOSITION CIPHER" and includes a "TRANSPOSITION DECODER" and a "TRANSPOSITION ENCODER". The decoder section has a text input field containing "ya\_s\_iaemeotnsi\_prmnesath\_\_alf\_aotnie\_mibitssnxp\_rrpioch", a checkbox for "KEEP SPACES, PUNCTUATION AND OTHER CHARACTERS" which is checked, a dropdown for "PLAINTEXT (PRESUMED) LANGUAGE" set to "English", and a "DECIPHER METHOD" section with two options: "KNOWING THE ENCRYPTION KEY OR PERMUTATION" (selected) and "TRY ALL PERMUTATIONS (BRUTEFORCE UP TO SIZE 6)". The key input field shows "KEY" and a permutation "(2,1,3) ⇌ (2,1,3)<sup>-1</sup>". The encoder section has a "MODE" dropdown set to "Write by rows, read by columns (by default)". At the bottom, there are social media share buttons and a Windows taskbar.

## 5. Playfair Cipher

The Playfair Cipher encrypts pairs of letters at a time using a 5x5 matrix of letters. It involves specific rules for handling duplicates and the positions of letters in the matrix.

**Example:**

- **Encryption:** Using a matrix and key, "HELLO" becomes "DPEMT."
- **Decryption:** With the same matrix and key, "DPEMT" can be decrypted back to "HELLO."
- 
-

BOXENTRIQ

TOOLS

### Playfair cipher

Encrypt

Decrypt

HI I AM BASIT. THIS TEXT IS AN EXAMPLE OF PLAYFAIR CIPHER

Clear

Options

### Result

EB B PH DYQDN. QMCN NMZS CN PQ KUFHLAG NP LAYFPPBB DEIKGCV

### Encryption key

PLAYFAIR

Translate this letter 

J

 into 

I

## 6. Enigma Machine

The Enigma machine is an example of a rotor cipher machine used by the Germans during World War II. It employed a complex system of rotors and wiring to encrypt and decrypt messages.

### Example:

- **Encryption:** By setting the rotors and plugboard correctly, "HELLO" would become a seemingly random string.

- **Decryption:** Only with the precise rotor settings and wiring information can the message be decrypted.

The screenshot shows a web-based Enigma machine simulator. It is divided into three main sections: Ciphertext, Enigma machine settings, and Plaintext.

**Ciphertext Section:** Labeled 'VIEW' and 'Ciphertext', it contains the encrypted message:
   
gtbhh xdjrs cowew ppbac rvqgq
   
xosoq suuzt wnHPq ylbjt

**Enigma machine Section:** Labeled 'ENCODE' and 'DECODE', it shows the machine configuration:
 

- MODEL: Enigma M3
- REFLECTOR: UKW B
- ROTOR 1: VI, POSITION: - 1 A +, RING: - 1 A +
- ROTOR 2: I, POSITION: - 17 Q +, RING: - 1 A +
- ROTOR 3: III, POSITION: - 12 L +, RING: - 1 A +
- PLUGBOARD: (empty)

**Plaintext Section:** Labeled 'VIEW' and 'Plaintext', it shows the decrypted message:
   
hi my name is Basit. This is
   
an example of enigma machine

## Conclusion

Ciphers have played a crucial role in the history of cryptography. They range from simple and easily breakable methods like the Caesar Cipher to more complex and secure systems like the Enigma machine. Understanding these ciphers helps us appreciate the evolution of cryptography and the importance of encryption in protecting sensitive information. In modern times, cryptographic algorithms like AES and RSA have replaced many of these classical ciphers due to their increased security and complexity.