PROJECT NAME: CYBER SECURITY MINOR PROJECT.

SUBMITTED BY: BASIT SHAMEEM

Report on Different Types of Ciphers with Examples

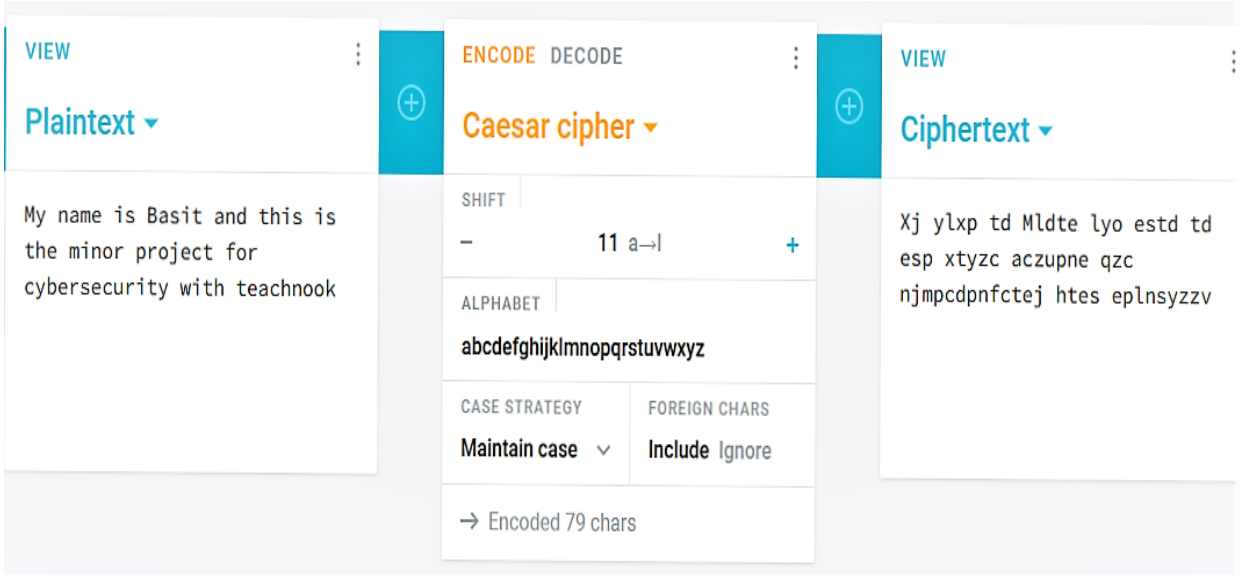
Ciphers are cryptographic techniques used to secure the confidentiality of information by transforming it into an unreadable format. Throughout history, various types of ciphers have been developed, each with its own method of encryption and decryption. In this report, we will explore some common types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

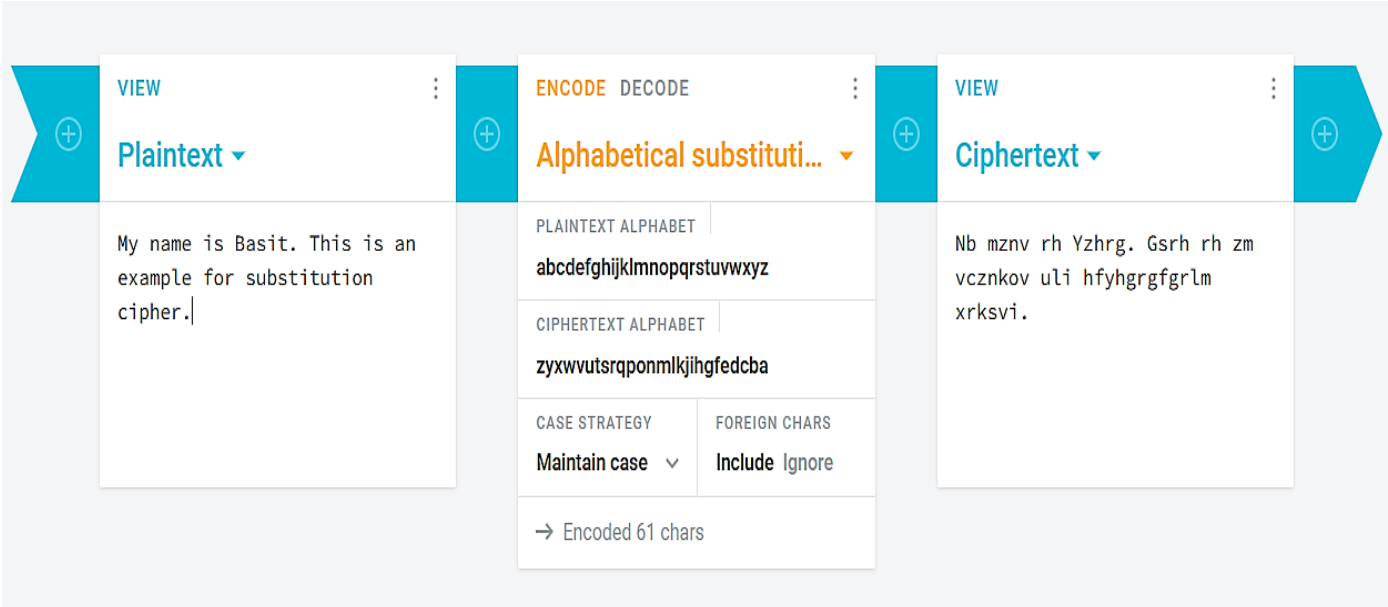


2. Substitution Cipher

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."

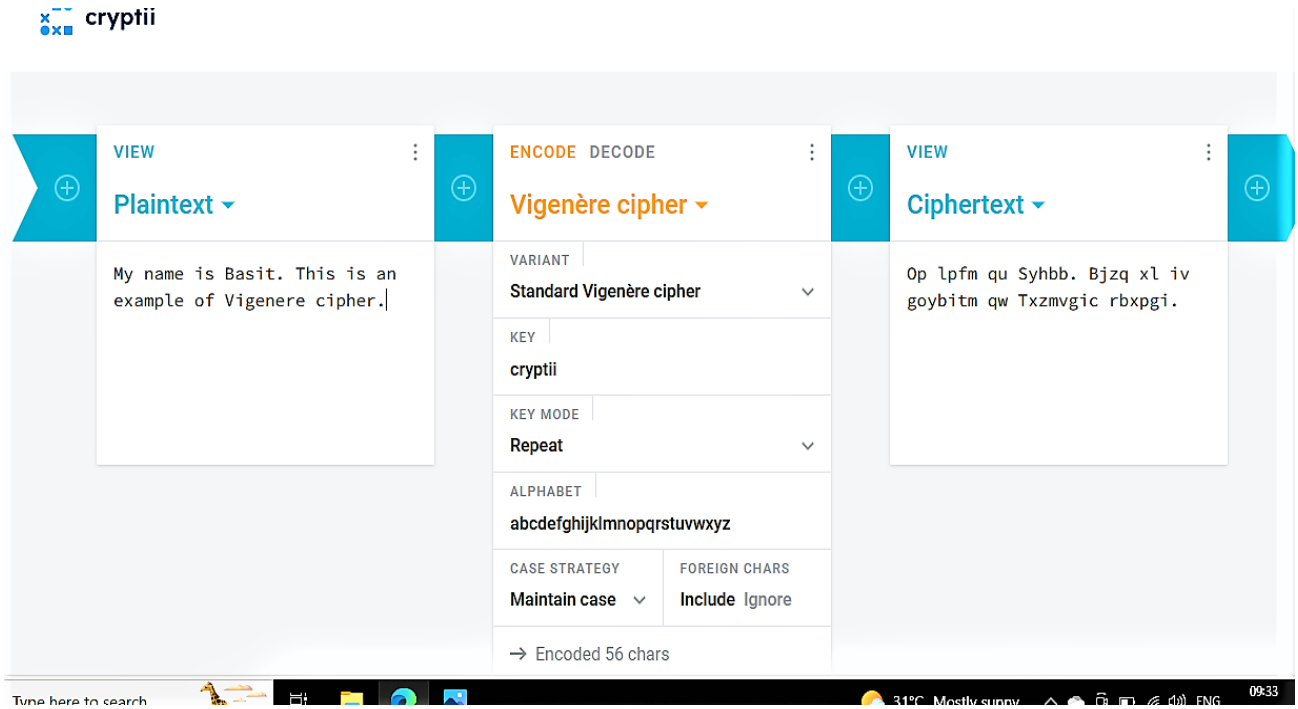


3. Vigenere Cipher

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."



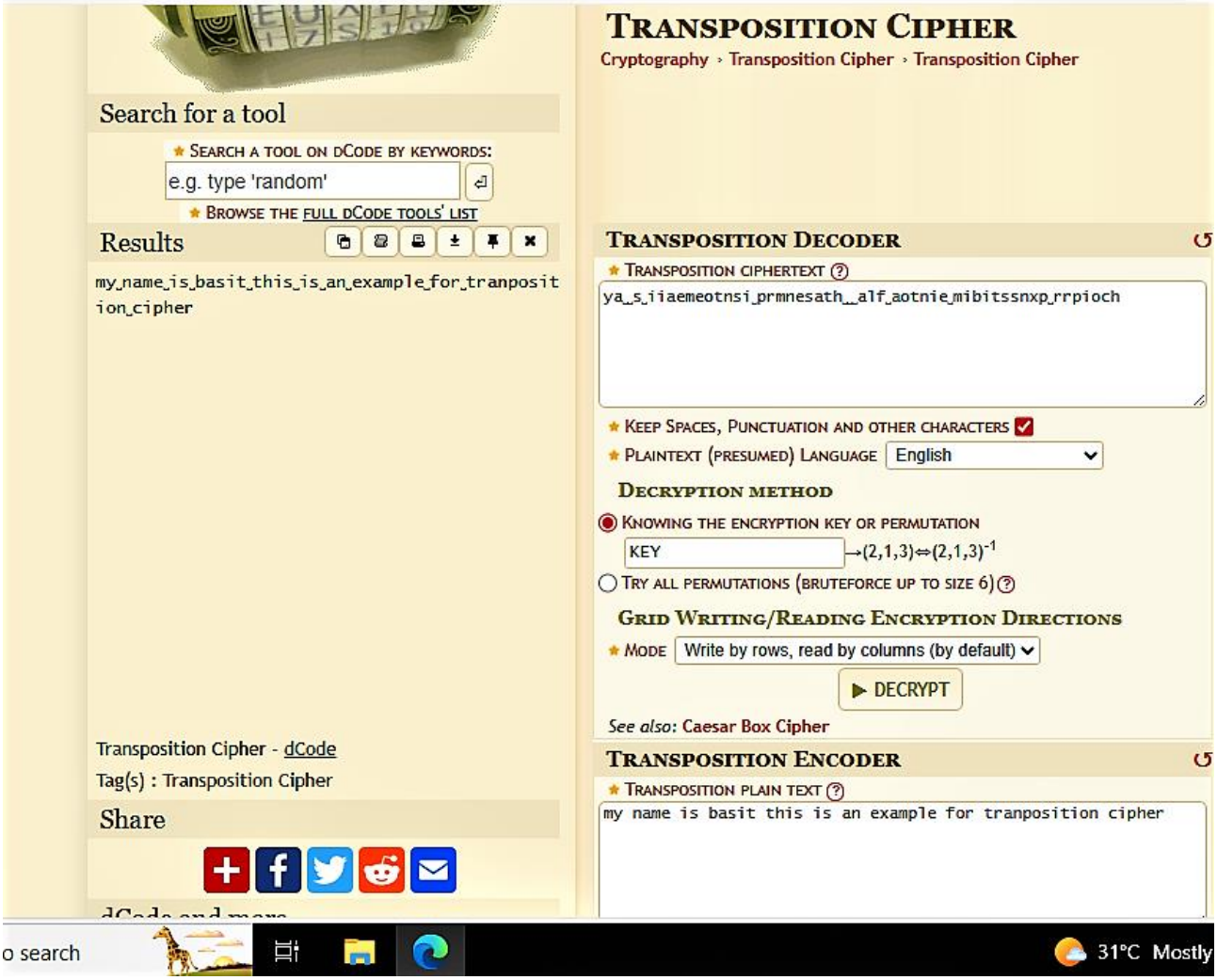
4. Transposition Cipher

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."

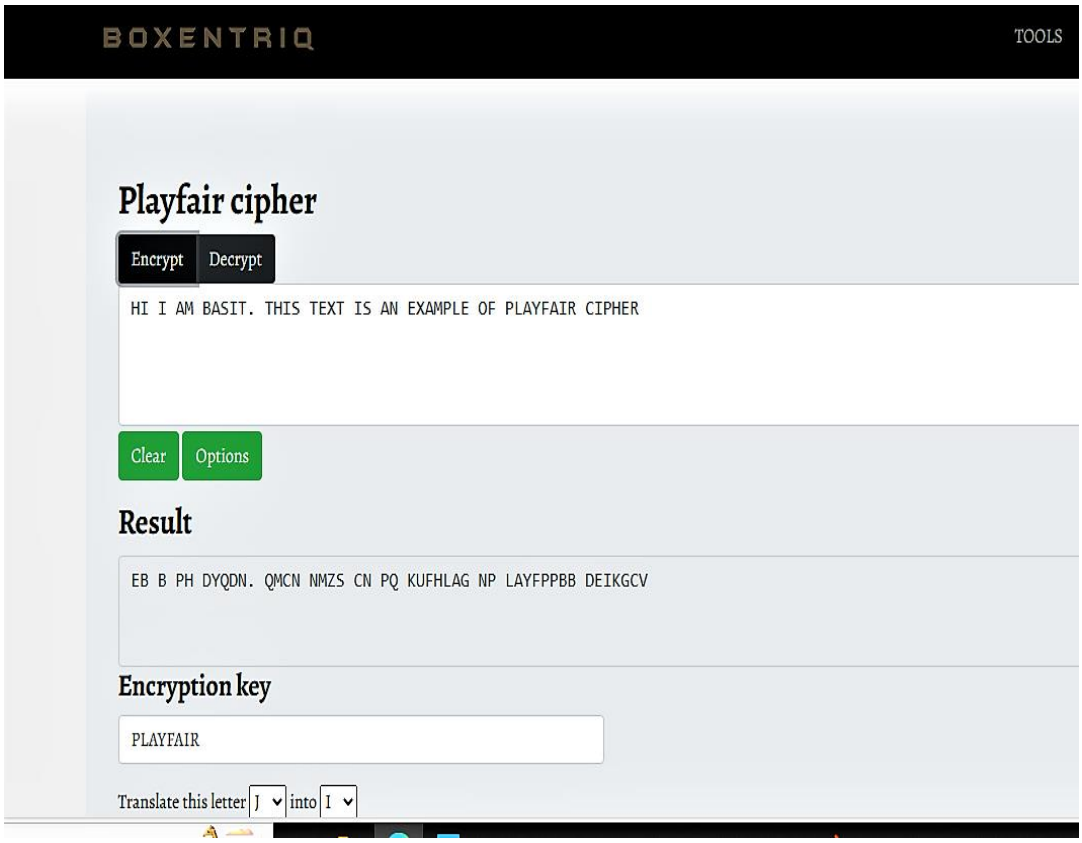


5. Playfair Cipher

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."
-
-

- 

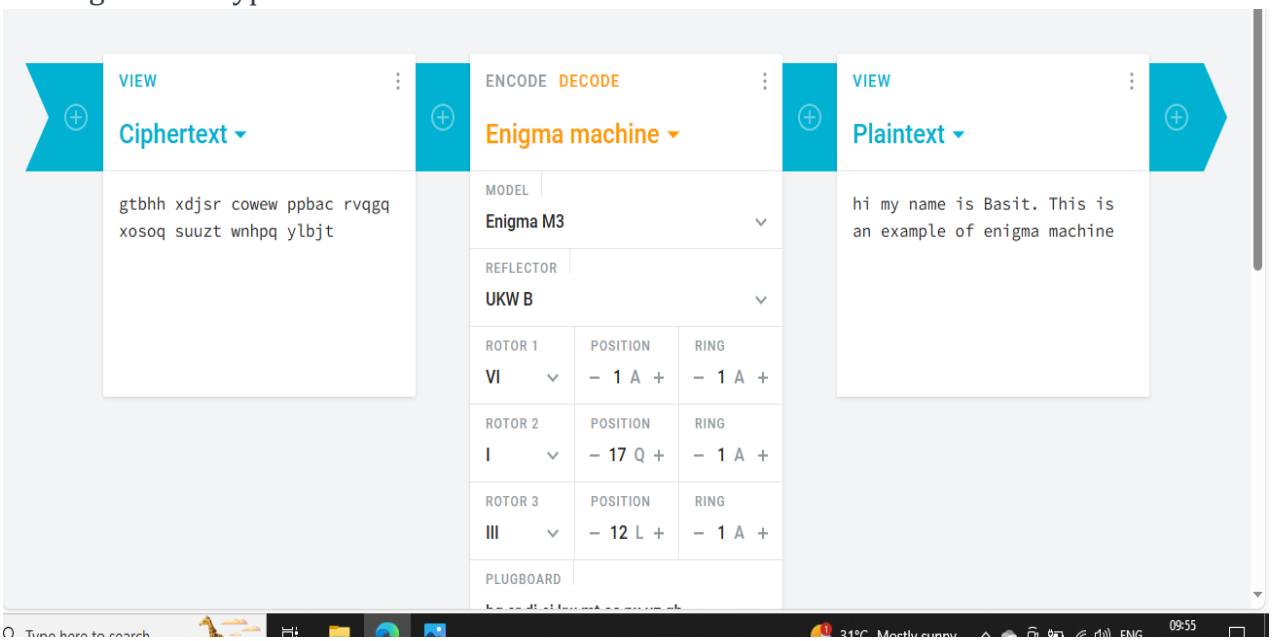
6. Enigma Machine

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.



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.