Practical No. 2

Vernam Cipher

**Q.1]** Write a Python code for encryption and decryption of Vernam cipher.

**Vernam Cipher:**The Vernam Cipher, often known as the One-Time Pad (OTP), is a type of substitution cipher where each character in the plaintext is encrypted by a modular addition with a corresponding character in a randomly generated key of the same length. It’s considered the only cipher that is theoretically unbreakable when the key is truly random, kept secret, and used only once.

**Formula:**

Ci​=(Pi​⊕Ki​) or (Pi​+Ki​)mod26 **Decryption:** Pi​=(Ci​⊕Ki​) or (Ci​−Ki​+26)mod26

Where:

* CiC\_iCi​ is the i-th character of the ciphertext.
* PiP\_iPi​ is the i-th character of the plaintext.
* KiK\_iKi​ is the i-th character of the key.
* ⊕\oplus⊕ denotes the XOR operation for binary data.

**Strengths:**

* **Unbreakable Security**: When the key is random, as long as the plaintext, kept secret, and used only once, the cipher is theoretically unbreakable.
* **Perfect Secrecy**: The ciphertext provides no information about the plaintext without the key. Each bit/letter of ciphertext is equally likely to represent any bit/letter of plaintext.

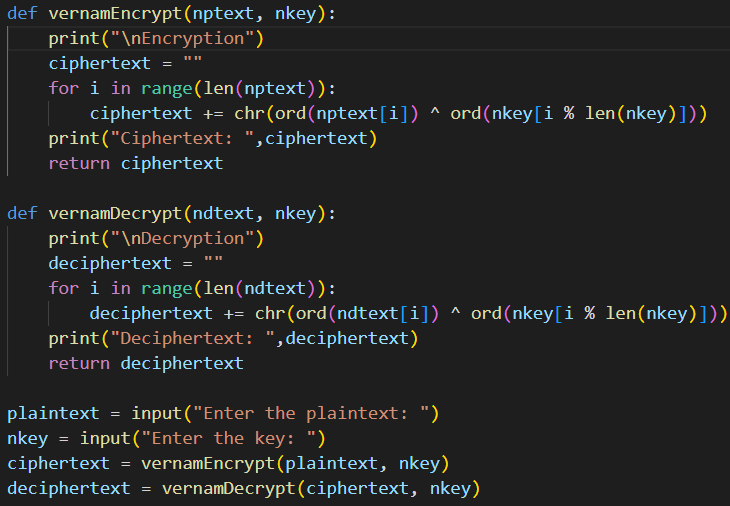
**Weakness:**

* **Key Management**: Requires a key that is as long as the message, which can be impractical for long messages.
* **Key Distribution**: Secure distribution and storage of such large keys can be challenging.
* **Single Use**: If a key is reused, it compromises security, making it susceptible to cryptanalysis.

**Attacks:**

* **Key Reuse Attack**: If the same key is used more than once, an attacker can use the XOR operation on two ciphertexts to reveal information about the plaintexts (e.g., a XOR attack).
* **Poor Key Generation**: If the key is not truly random or is generated with predictable patterns, the cipher’s security is compromised.
* **Known-Plaintext Attack**: If part of the plaintext is known or can be guessed, it reveals the corresponding part of the key.

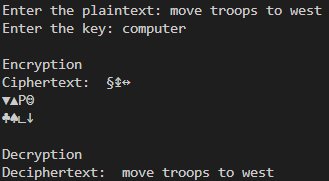
**Code:**



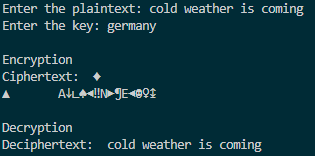
**Output:**

**Test Cases:**

**1]** Here the plaintext was “move troops to west” and the keyword was computer. This resulted in multiline ciphertext with only few characters visible. Mostly the ciphered text characters are different from each other.

****

**2]** Here, the plaintext was “cold weather is coming” and the keyword was “germany”. Here some repeated characters can be found in ciphered text.

****