**Cryptography & Network Security**

**TE IT**

**Experiment No 1 (Part B)**

**Implementation of Vernam Cipher (One-Time-Pad)**

**Aim**: To write a Python program to perform encryption using conventional cryptography technique – Vernam Cipher.

**Learning Objectives**:

* To understand the transposition technique.
* To describe the Vernam cipher algorithm and encrypt the plain text.
* To decrypt the cipher text using Vernam cipher algorithm.

**Theory**:

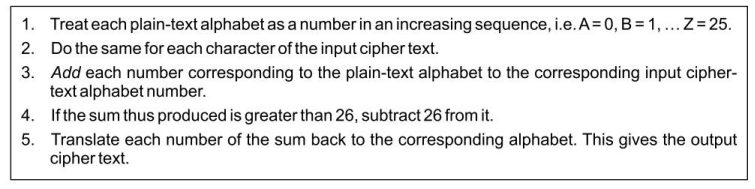
**Transposition Techniques:**

Substitution techniques focus on substituting a plain-text alphabet with a cipher-text alphabet. Transposition techniques differ from substitution techniques in the way that they do not simply replace one alphabet with another, but they also perform some permutation over the plain text.

**Algorithm of Vernam Cipher (One-Time Pad)**:

The Vernam cipher, whose specific subset is called one-time pad, is implemented using a random set of non-repeating characters as the input cipher text. The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other message (hence the name one-time).

The length of the input cipher text is equal to the length of the original plain text. The algorithm used in the Vernam cipher is described in Fig. 1



***Fig. 1 Algorithm for Vernam cipher***

It should be clear that since the one-time pad is discarded after a single use, this technique is highly secure and suitable for small plain-text messages, but is clearly impractical for large messages.

**Results:**

Encrypt and Decrypt your full name using Vernam Cipher using. Assume a suitable one-time pad for encryption and decryption.

**Conclusion:**

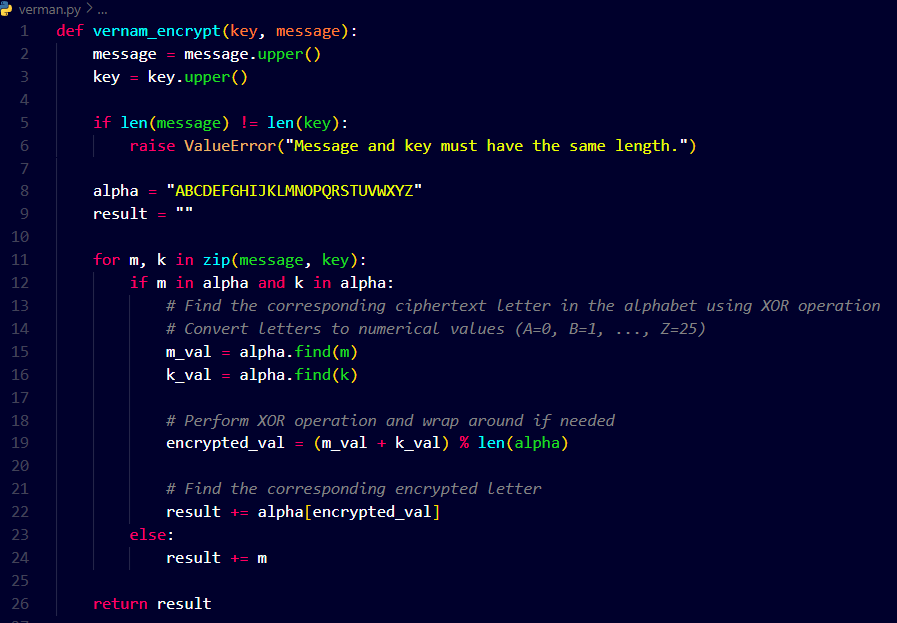
In conclusion, the Vernam cipher, also known as the one-time pad, offers perfect secrecy when used correctly. It encrypts messages by combining a random key of the same length as the plaintext, resulting in statistically random ciphertext. However, the practical limitations of generating, managing, and securely distributing long keys make it suitable only for short, critical communications where absolute secrecy is essential. For general-purpose encryption of longer messages, other cryptographic algorithms are more practical and widely used.

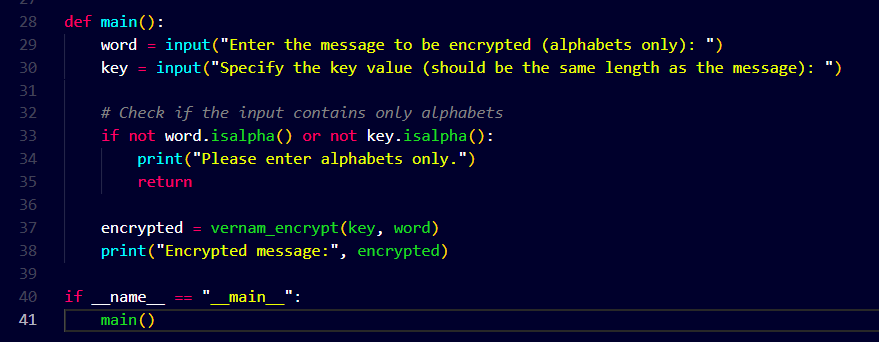
**Answer the following questions.**

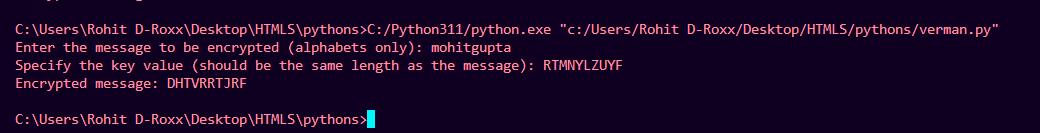
Why is Vernam Cipher suitable only for short messages?

The Vernam cipher requires a key as long as the plaintext, making it impractical for longer messages. Key generation and distribution complexities also limit its use for everyday communication. It's mainly suitable for short, critical communications when perfect secrecy is crucial.

**Outputs:**







**Practical Learning Outcomes:**

|  |  |
| --- | --- |
| After performing the practical, the learner is able to: | Marked |
| 1. To understand the transposition technique. 2. To describe the Vernam cipher algorithm and encrypt the plain text. 3. To decrypt the cipher text using the Vernam cipher algorithm. |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Outcome** | **PLO 1** | **PLO 2** | **PLO 3** | **Performance** | **Attendance** | **Total Score** | **IT DEPARTMENT- TCET** |
| **Weight** | **20** | **20** | **20** | **20** | **20** | **100** | Date of  Performance: \_\_\_\_\_\_\_  Date of Correction: \_\_\_\_\_\_\_\_\_\_\_  Roll No: \_\_\_\_\_\_\_\_\_  Marks: \_\_\_\_\_\_/100  Signature of Faculty: |
| **Score** |  |  |  |  |  |  |