****

**CryptoLock**

A Custom Encryption/Decryption Scheme

**NAME: NASHRA GHAFFAR**

**ROLL NUMBER: CT-20032**

**COURSE CODE: CT-486**

**INSTRUCTOR: Dr. MUBASHIR KHAN**

**Q) Design your own encryption/decryption scheme. Implement its code in python, explain and perform some test cases with random plaintexts.**

**Overview:**

The CryptoLock is a custom encryption and decryption scheme. This scheme employs a dual-layered approach: first, converting each character to its ASCII code and applying modular addition with a secret key and fixed modulus, and second, implementing a Caesar cipher with a specified shift. The encryption process enhances security by introducing complexity and variability. The subsequent decryption reverses these operations, requiring knowledge of the key and modulus for a successful reversal. Strengths include the inherent difficulty in reversing modular addition, while weaknesses center on the reliance on key secrecy.

**Design:**

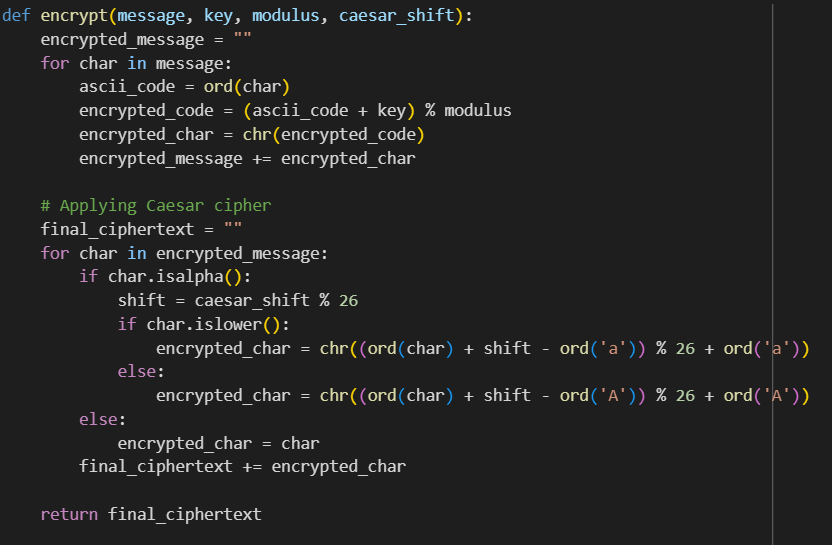
**Encryption:**

- Convert each character of the message to its ASCII code.

- Apply modular addition using a secret key and fixed modulus.

- Convert the encrypted code values back to ASCII characters.

- Apply a Caesar cipher using a specified shift.

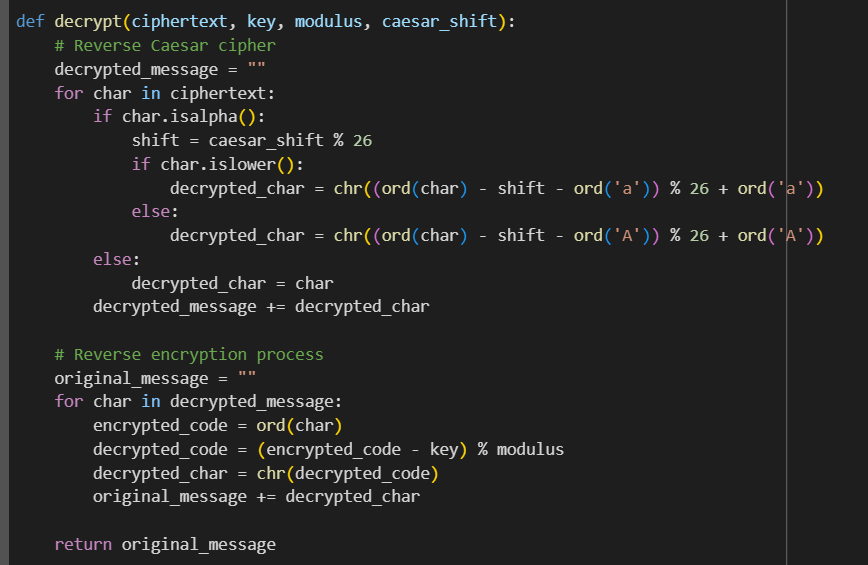


**Decryption:**

- Reverse the Caesar cipher applied during encryption.

- Reverse the modular addition using the same key and modulus.

- Convert the decrypted code values back to ASCII characters.



**Explanation:**

**Encryption:**

- Each character's ASCII code is shifted by a secret key modulo a fixed modulus.

- This prevents easy reversal without knowledge of the key and modulus.

- A Caesar cipher adds an extra layer of substitution for security.

**Decryption:**

- Reverse the Caesar cipher to obtain the encrypted message.

- Reverse the modular addition process using the key and modulus.

**Python Script:**

https://colab.research.google.com/drive/1Eei6DDehXBHf1Q9famUaX7hIuBLHOS2u?usp=sharing

**Analysis:**

**Strengths:**

- Modular addition provides a mathematical operation that is difficult to reverse without the key.

- The additional Caesar cipher adds complexity and variability.

**Weaknesses:**

- Security heavily depends on the secrecy of the key.

- Caesar cipher has known vulnerabilities if the shift is small.

**Testing with Samples of Plaintext:**

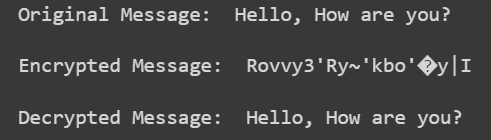
Let's test the script with a sample:

**secret\_key = 7**

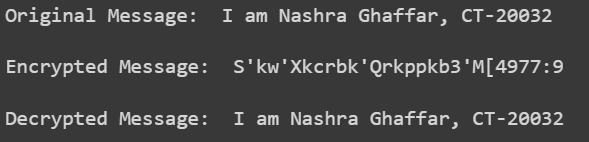
**modulus\_value = 128**

**caesar\_shift\_value = 3**

**CASE 1 (String):**

****

**Case 2 (Alphanumeric):**

****