

**Experiment No. 1**

**Title: Substitution Cipher**

**Batch:A3** **Roll No.:16010421073** **Experiment No.: 1**

**Aim:** To implement substitution ciphers – Affine and Vigenere cipher.



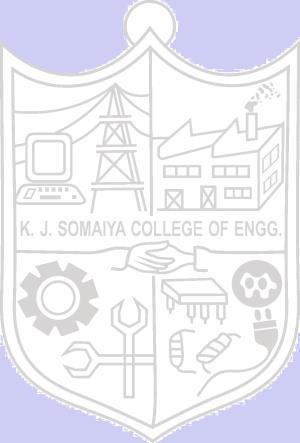
**Resources needed:** Windows/Linux.



**Theory**

**Pre Lab/ Prior Concepts:**

**Symmetric-key algorithms** are a class [of algorithms for cryptography that](http://en.wikipedia.org/wiki/Algorithm) use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Symmetric-key encryption can use either stream ciphers or block ciphers. Transposition Cipher is block cipher. Ancient cryptographic systems are classified as: Substitution and Permutation Ciphers.

**Simple Substitution Cipher**

A substitution cipher replaces one symbol with another. Letters of plaintext are replaced by other letters or by numbers or symbols. In a particularly simple implementation of a simple substitution cipher, the message is encrypted by substituting the letter of the alphabet n places ahead of the current letter. For example, with n = 3, the substitution which acts as the key

plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z

ciphertext: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

The convention is plaintext will be in lowercase and the cipher text will be in uppercase. In this example, the key could be stated more succinctly as “3” since the amount of the shift is the key. Using the key of 3, we can encrypt the plaintext message: “fourscoreandsevenyearsago” by looking up each letter in the plaintext row and substituting the corresponding letter in the ciphertext row or by simply replacing each letter by the letter that is three positions ahead of it in the alphabet. In this particular example, the resulting cipher text is IRXUVFRUHDAGVHYHABHDUVDIR

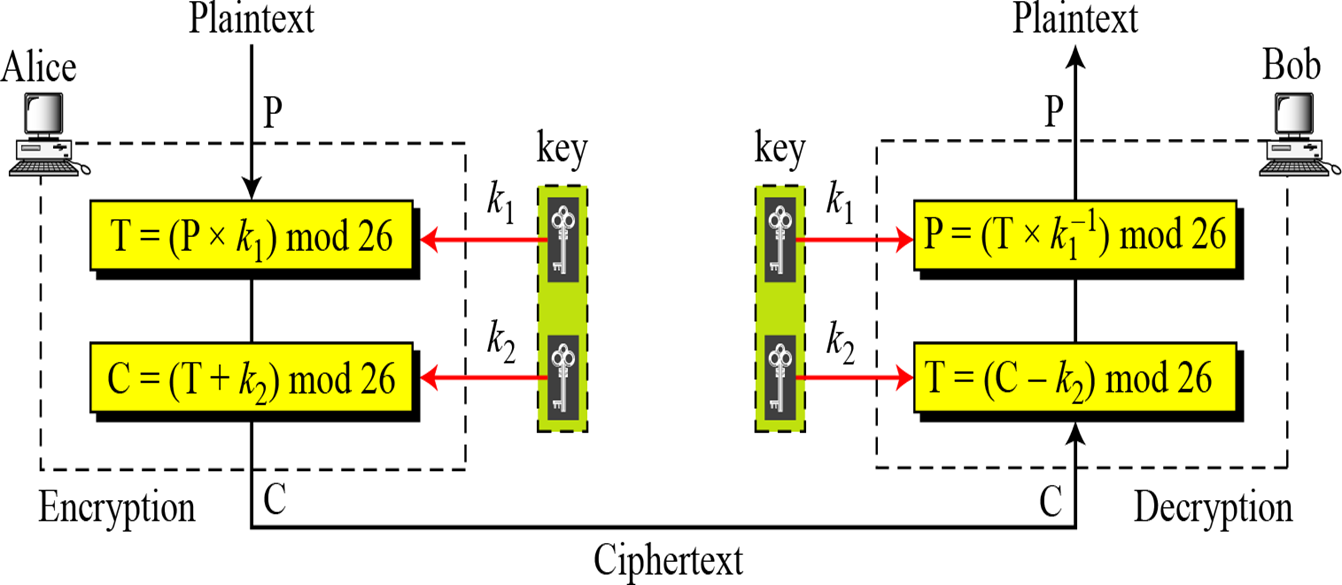
To decrypt, we simply look up the ciphertext letter in the ciphertext row and replace it with the corresponding letter in the plaintext row, or simply shift each ciphertext letter backward by three. The simple substitution with a shift of three is known as the Caesar’s cipher because it was reputedly used with success by Julius Caesar.

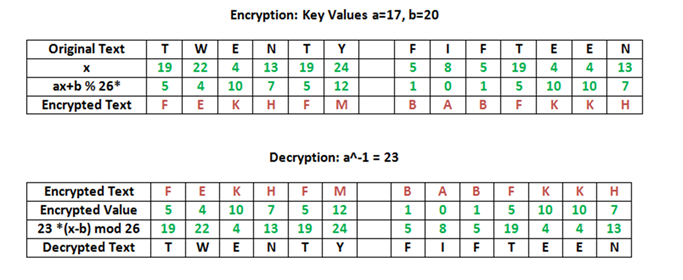
Substitution ciphers are classified as monoalphabetic and polyalphabetic substitution cipher. In monoalphabetic substitution cipher each occurrence of character is encrypted by same substitute character. In Polyalphabetic substitution cipher each occurrence of a character may have a different substitute due to variable Key.

**AFFINE CIPHER**

The Affine cipher is a type of monoalphabetic substitution cipher which uses a combination of Additive and Multiplicative Ciphers.  Each letter is enciphered with the function (ax + b) mod 26, where b is the magnitude of the shift. The encryption function for a single letter is C=(ax + b) mod m where 1≤a≤m, 1≤b≤m

where modulus m is the size of the alphabet and a and b are the keys of the cipher. The value a must be chosen such that a and m are coprime. The decryption function is P = a-1(c-b) mod m, where a−1 is the [modular multiplicative inverse](https://en.wikipedia.org/wiki/Modular_multiplicative_inverse) of a i.e., it satisfies the equation a a-1 = 1 mod m.



****

**Activity:**

Implement the following substitution ciphers:

1. Additive Cipher
2. Multiplicative Cipher

**Implementation:**

Implement a menu driven program. It should have an encryption function and a decryption function for each cipher. Function should take a message and a key as input from the user every time when the user calls the encryption/decryption function and display the expected output.



**Results:** (Program with output as per the format)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Questions:**

1. **Write down the flaws of Additive cipher and Multiplicative Cipher:**

**Ans:** **Additive Cipher (Caesar Cipher):-**

* **Lack of Key Space:**

The Additive Cipher has a very limited key space since it only uses a single parameter - the shift value. The key space is equal to the size of the alphabet being used, which makes it susceptible to brute-force attacks.

* **Weak Security:**

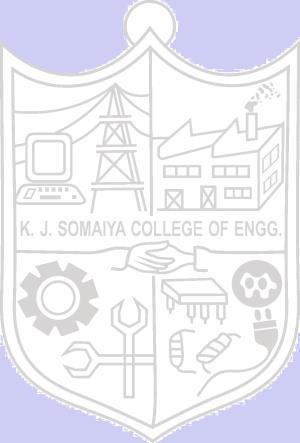
The Additive Cipher can be easily broken with modern computational power, making it unsuitable for secure communication. Brute-force attacks or simple statistical methods can quickly reveal the plaintext.

* **Lack of Encryption Strength:**

The Additive Cipher is a monoalphabetic substitution cipher, meaning that each letter in the plaintext is always substituted with the same corresponding letter in the ciphertext. This makes it relatively weak and easy to crack.

1. **Implement/Write down the code of Affine cipher and Vigenere Cipher:**





**Outcomes:**

**CO1 : Describe the basics of Information Security.**

**Conclusion:**

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**



**References: Books/ Journals/ Websites:**

1. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw Hill
2. William Stalling, “Cryptography and Network Security”, Prentice Hall