|  |  |
| --- | --- |
| Subject: Cryptography & System Security Lab | Course ID: CSL-602 |
| Semester: VI | Course: AI & DS |
| Laboratory: 302 | Name of teacher: Prof. Gitanjali Korgaonkar |
| Name of Student: Ayush Gupta | Roll No: VU2S2324001 |

**EXPERIMENT NO. 1**

**Aim:**

To perform and implement Hill cipher, Affine cipher and Keyless transposition cipher.

**Theory:**

1. **Hill Cipher:**

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

**Formula of Hill Cipher:**

* **Encryption:** Cipher Text = (Plain Text \* Key) Mod 26
* **Decryption:** Plain Text = (Cipher Text \* Key-1) Mod 26

1. **Affine Cipher:**

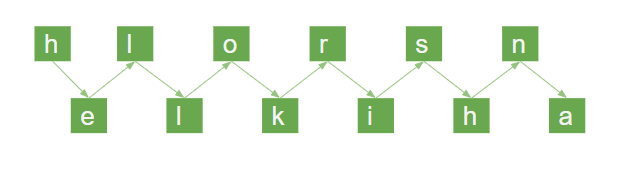
The Affine cipher is a type of monoalphabetic substitution cipher, where each letter in the alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and then converted back to a letter. The formula used ensures that each letter encrypts to exactly one other letter, and vice versa. This makes the cipher essentially a standard substitution cipher with a rule governing which letter maps to which. The entire process relies on working modulo *m*, where *m* represents the length of the alphabet being used. In the Affine cipher, the letters of an alphabet of size *m* are first mapped to the integers in the range 0 to *m-1*. The key for the Affine cipher consists of two numbers, which we'll refer to as *a* and *b*. The following discussion assumes the use of a 26-character alphabet (where *m = 26*). The value of *a* should be chosen to be relatively prime to *m* (i.e., *a* should have no factors in common with *m*).

**Formula of Affine Cipher:**

* **Encryption:** Cipher Text = (a \* Plain Text + b) Mod 26
* **Decryption:** Plain Text = a⁻¹ \* (Cipher Text - b) Mod 26

1. **Keyless Transposition Cipher:**

Keyless Transposition Ciphers are an essential part of cryptography that use the systematic shuffling of plain text characters or bits to secure data by altering their positions based on a defined algorithm. Unlike substitution ciphers, where different letters replace others, transposition ciphers merely shift the original letters, making the message appear completely scrambled. These strategies, although relatively primitive, laid the foundation for more sophisticated encoding techniques. Historical ciphers like the Rail Fence and Columnar Transposition are examples of such methods. Columnar transpositions are still explored and employed today, especially in complex systems involving hierarchical structures meant to enhance message secrecy through additional layers of obscurity. In this article, we will discuss the techniques used to encrypt messages through transposition ciphers. Specifically, we will focus on the Rail Fence Transposition Cipher, which is one of the simplest transposition techniques, also known as the zigzag cipher. This cipher gets its name from the zigzag pattern in which it encrypts the plain text. The steps to generate the cipher text using the Rail Fence Transposition cipher technique will be explained next.



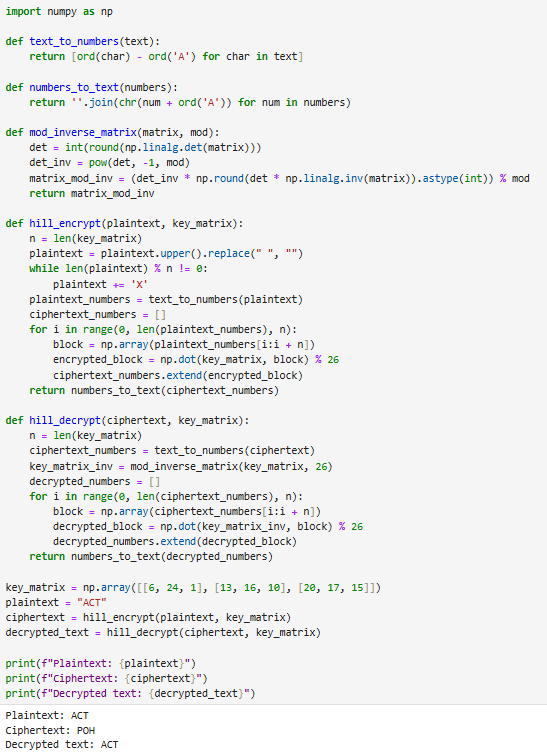
**Conclusion:**

Thus, we have studied & successfully implemented Hill cipher, Affine cipher and keyless Transposition cipher technique.

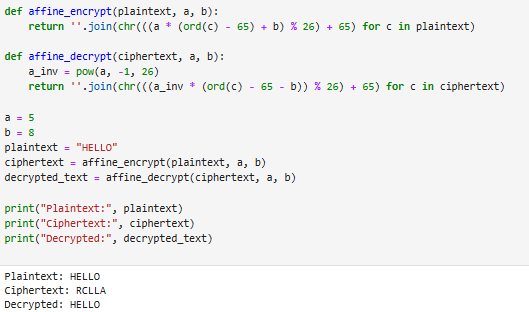


**Program and Output:**

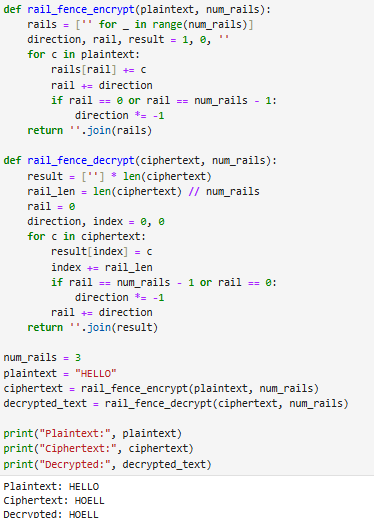
1. **Hill Cipher:**

****

1. **Affine Cipher:**

****

1. **Keyless Transposition Cipher:**

****