# Ciphering/Deciphering data using Affine Cipher Algorithm

**Group-7_Fanatics**

Vatsal Patel - AU2040043
Digant Patel - AU2040086
Samarth Chauhan - AU2040097

***Abstract*- Cryptography is a means of using codes to protect information and communications so that only those who are supposed to read and process it; may do so. Knowledge of ciphers is said to have been acquired by the Ancient Greeks and used for military purposes. Affine cipher uses alpha-numeric conversions and principles of matrix inversion to encrypt and decrypt data.**

## I. Introduction

"Crypt-" means 'hidden' and "graphy" means 'writing'. It is a term used to refer to the assemblage of operations such as encryption, decryption and hashing. Cryptography is mainly used to maintain secrecy in communication and easily convey encrypted messages. Affine cipher uses singular-alphabetic substitution where every alphabet is assigned a numeric key and basic mathematics is used to encrypt the text messages. Right now there exists a total of 286 affine ciphers; since there are multiple variations possible, it can be considered one of the best if not the best cipher known to humans till date.

## II. Background

Hiding of secret messages has been going on for thousands of years, but research in this field just started in the digital world. The first known evidence of cryptography being used was around 100 BC when Julius Caesar used encoding to convey secret messages to his army [2]. The Caesar cipher was found easily breakable when Brute Force was put into use while decryption. Hence there was a need for a less penetrable cipher and Affine cipher was just the right choice.

## III. Motivation

Encryption is a very fascinating field of computer science. Hearing about data leaks is very disappointing and we want to examine and learn more about the various aspects of encryption. We are also going to create an encryption method of our own by taking inspiration from the Affine Cipher algorithm.

## IV. Literature Survey

In the Affine cipher, we convert each letter of the input data (text) to its numeric equivalent. These numeric values are formed into a matrix. It is then multiplied with another matrix (A) of our own and another matrix (B) is added to it to encrypt the data. To decrypt the data, we subtract B and then multiply the result obtained from above with the inverse matrix of A. This process of encryption and decryption can be made more complex by increasing the number of multiplications.

Encryption:

$$C \equiv (AB.....M)P + K \pmod{N}.$$

$$\begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} ..... \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix} + \begin{pmatrix} k_{11} \\ \vdots \\ k_{n1} \end{pmatrix} (\text{mod } N)$$

Decryption:

$$P \equiv (AB....M)^{-1}(C - K) \pmod{N}.$$

## V. References


- [1] Richards, K. (2020, April 6). What is cryptography? - definition from whatis.com. SearchSecurity. Retrieved September 27, 2021, from What is Cryptography? Definition from SearchSecurity.
- [2] Sidhpurwala, H. (2019, March 19). A brief history of cryptography. Red Hat Customer Portal. Retrieved September 27, 2021, from A Brief History of Cryptography.
- [3] GeeksforGeeks. (2021, August 4). *Implementation of Affine Cipher*. Implementation of Affine Cipher