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.

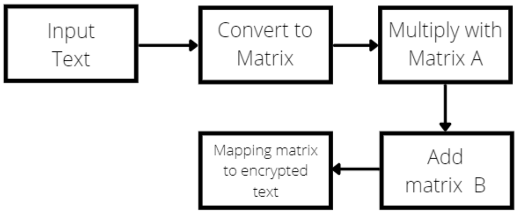
III. Motivation

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

- We studied different cipher algorithms and found out that Affine cipher is quite secure because it can have multiple keys.
- One advantage of Affine cipher is that the number of keys can be changed every time we want to encrypt new data.
- Affine cipher is a multistep process, therefore it increases the security of our data.
- We have explained the steps involved in encryption and decryption in the next few slides.

Encryption Algorithm:



Firstly, we convert plaintext to ciphertext and the steps are as follows:

1. Choose a nxn matrix A which is invertible and here n depends on the length of the message.
2. Change plaintext to mapped value as given in the below table.

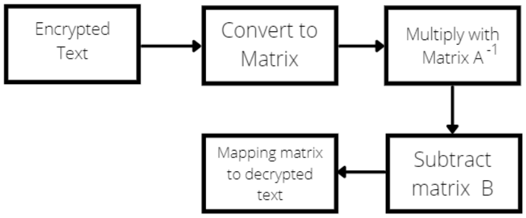
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

3. Apart from the above image, we will add 3 more characters (Space, ?, !).
4. After that, create a column (nx1) vector P having all the numerical values of plaintext.

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

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

Decryption Algorithm:



1. To decrypt the text, make a vector C and subtract k from that.
2. As shown below, take the inverse of all the key matrices which were multiplied.
3. Get each letter by converting the plaintext vector to its respective alphabet.

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

V. Contribution

Vatsal

➔ Documentation and report writing

➔ Research on decryption and related cipher functions

➔ Coding the encryption method

Digant

➔ Code for decryption method

➔ Research on affine cipher

➔ Documentation and report writing

Samarth

➔ Mathematical Formulation

➔ Research on encryption

➔ Coding the matrix multiplication and inversion method

➔ Documentation and report writin

VI. Custom Modifications

- To make the cipher program more viable for dynamic handling we made some modifications to the affine algorithm.
- The original affine cipher with only 26 characters was not enough to read spaces and encrypt them so we increased the keys to 29 and used sentences for encryption.
- We decided to use characters like space, ‘?’, and ‘.’ to increase the versatility of our code.
- We even programmed the cipher that will append the space to make the string length multiple of the size of the key matrix.

VII. Numerical Results

- Original string, P = “LONDON”
- Encryption algorithm: C = AP + B (mod 29)
- Here, A = $\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$ and B = $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$

For “LO”, P_1 = $\begin{pmatrix} 11 \\ 14 \end{pmatrix}$

$C_1 = \begin{pmatrix} 25 \\ 9 \end{pmatrix}$

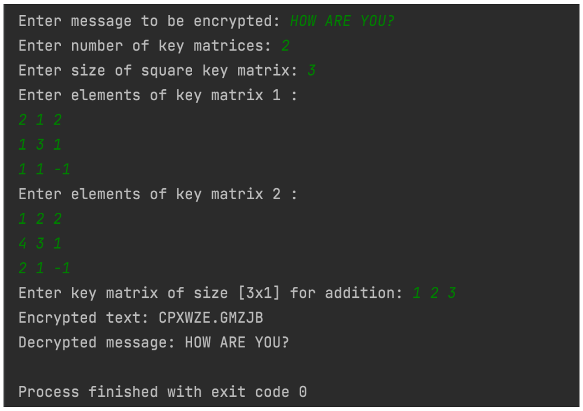
- Therefore, encrypted message = “ZJ?JFM”

- Encrypted String, C = “ZJ?JFM”
- Decryption Algorithm: P = $\mathbf{(A)^{-1}}$ **(C - B)** (mod 29)

(A and B are same as above example)

- $(A)^{-1} = \begin{pmatrix} 30 & 27 \\ 9 & 50 \end{pmatrix}$
- Therefore, Decrypted message = Original String = “LONDON”

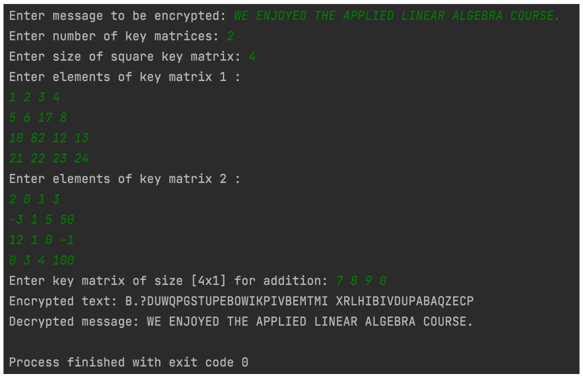
Result- 1:



```
Enter message to be encrypted: HOW ARE YOU?
Enter number of key matrices: 2
Enter size of square key matrix: 3
Enter elements of key matrix 1 :
2 1 2
1 3 1
1 1 -1
Enter elements of key matrix 2 :
1 2 2
4 3 1
2 1 -1
Enter key matrix of size [3x1] for addition: 1 2 3
Encrypted text: CPXWZE.GMZJB
Decrypted message: HOW ARE YOU?

Process finished with exit code 0
```

Resul- 2:



```
Enter message to be encrypted: WE ENJOYED THE APPLIED LINEAR ALGEBRA COURSE.
Enter number of key matrices: 2
Enter size of square key matrix: 4
Enter elements of key matrix 1 :
1 2 3 4
5 6 17 8
10 82 12 13
21 22 23 24
Enter elements of key matrix 2 :
2 0 1 3
-3 1 5 50
12 1 0 -1
0 3 4 100
Enter key matrix of size [4x1] for addition: 7 8 9 0
Encrypted text: B.?DUWQPGSTUPEBOWIKPIVBEMTMI XRLHIBIVDUPABAQZECP
Decrypted message: WE ENJOYED THE APPLIED LINEAR ALGEBRA COURSE.

Process finished with exit code 0
```

VIII. 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

[4]*Cryptography by means of linear algebra and number theory*. (n.d.). Retrieved October 20, 2021, from http://i-rep.emu.edu.tr:8080/xmlui/bitstream/handle/11129/1420/ElfadelAjaeb.pdf?sequence=1