MC215 Project
Cryptography using Linear Algebra

➲ **Group Members:-**

- ➔ **Manjal Shah (202003037)**
- ➔ **Mukund Ladani (202003039)**
- ➔ **Kashyap Halavadia (202003040)**
- ➔ **Nikhil Vaghasiya (202003042)**

❖ Introduction:-

- ➔ Cryptography is a technique of encoding our actual information with a proper "key" that is supposed to be known to both: the sender and receiver. The message is encoded using this key. Hence the original information is transformed into another form and then transferred to the receiver. Upon receiving that message, the receiver decrypts that message using the same key. Hence the communication is secured.
- ➔ Linear algebra serves as a useful tool in cryptography, permitting the manipulation of multiple variables simultaneously to create a unique and reversible output.

❖ Problem Statement:-

- ➔ **Suppose person A wants to send a text message S = "STUDY LINEAR ALGEBRA" to person B in a highly secured way such that no one other than person B should be able to read the message. What kind of technique can be used to efficiently encode and decode the message?**

❖ Solution:-

- ➔ Multiplication of the original integer matrix by some invertible matrix can be used as one of the powerful ways of encoding the message.

Step 1)

- ➔ Every message whether it be a text message or some other form can be represented in the form of an integer matrix. So first of all we need to convert the given plain-text message(S = "STUDYLINEARALGEBRA") into the corresponding integer

matrix by using the conversion table for converting each of the alphabets to the integers.

- ➔ We can use any scheme for converting alphabets to integers. Here we have used the position of alphabets for converting them into integers.
- ➔ The list of numbers corresponding to this particular string will be [19 20 21 4 25 12 9 14 5 1 18 1 12 7 5 2 18 1].

Step 2)

- ➔ To form the matrix, say it is a matrix B of dimension N x M matrix, each of the column vectors will be formed by taking N consecutive integers from the list of numbers. Here we are taking 3 consecutive integers from the list and putting them into columns of B. Here N=3 and M=$\lceil \frac{len(S)}{N} \rceil$.

B =

19	4	9	1	12	2
20	25	14	18	7	18
21	12	5	1	5	1

Step 3)

- ➔ Now we will choose an invertible matrix with integer entries such that its determinant is +1 or -1. We are choosing such a matrix because the inverse of such matrices will be easy to compute and also it will avoid fractional values in the inverse matrix and thereby will save a large amount of digital storage space. We will call this matrix as A
- ➔ Here we have chosen

A =

0	2	-1
1	-2	1
-1	-1	1

Step 4)

- ➔ Now we will pre-multiply A with B. The matrix which we will send will be AB. AB is the encoded matrix. So matrix AB will be transmitted in further stages of the communication line over the network.

$AB =$

19	38	23	35	9	35
0	-34	-14	-34	3	-33
-18	-17	-18	-18	-14	-19

Step 5)

- ➔ Now the receiver will receive this matrix and he will also need to decode it using $\mathbf{A^{-1}}$.
- ➔ So the receiver will need to compute this $\mathbf{A^{-1}}$.

$A^{-1} =$

1	1	0
2	1	1
3	2	2

Step 6)

- ➔ Both the communicating parties should have the alphabet to number conversion table and the key(i.e. matrix A).
- ➔ It will be very difficult for any third party to crack this encoded matrix. Additionally to keep the security high the key matrix i.e A can be changed after regular intervals of time.

Step 7)

- ➔ Now the receiver will receive this matrix and he will also need to decode it using $\mathbf{A^{-1}}$.
- ➔ So the receiver will need to compute this $\mathbf{A^{-1}}$. Also, we have to keep in mind this calculation expense.

Integer- Matrix Theorem:-

- ➢ If A is a N x N integer matrix and det(A) = ± 1 then A^{-1} exists and it is also an N x N integer matrix.

Q) Why is it useful?

1. The inverse of such matrices can be easily computed as it helps to avoid fractional values.
2. It takes less storage space to store integer matrices.

Application of determinant properties:-

- ➢ As mentioned earlier, for higher security we may change the key matrix A after regular intervals of time. Also, we need key matrices such that their determinant value is +1 or -1.
- ➢ We need a mechanism to generate such matrices, for that we can initially take an upper triangular matrix whose diagonal entries are +1 or -1. So that its determinant value will be +1 or -1.
- ➢ Now, for generating matrices whose determinant value is +1 or -1, we can perform elementary row operations on matrix A, to generate a number of such matrices. An example of this is shown here:

A =

+1	x	y
0	-1	z
0	0	1

1	x	y
1	-1+x	y+z
0	0	1

R1 -> R1 +R2

1	x	y
1	-1+x	y+z
1	x	y+1

R3-> R3 + R1

1	x	y
0	-2+x	y+2z
0	0	1

R2-> 2*R2 + R1

1	x	y
0	-2 +x	y +2z
1	x	2 +y

R3 -> 2*R3 +R1

Application of property: Determinant value does not change by doing elementary row transformations.

Extension:-

1) Increasing the number of keys, that entire group of keys can act as a master key. We can make the encryption more efficient by multiplying the plaintext matrix (i.e. B) with keys like $A_1 * A_2 * A_3 * \ldots * A_n$, Now to decode the final version of the encoded message the receiver should have $(A_1 * A_2 * A_3 * \ldots * A_n)^{-1} = (A_n^{-1} * A_{n-1}^{-1} * A_{n-2}^{-1} * \ldots * A_2^{-1} * A_1^{-1})$.

   The significance of using multiple keys can be understood by the following example. The encryption can be done by server1 when a message leaves from server1 and the plain text matrix gets multiplied

by A_1, Similarly, the encryption is done by server i when it leaves from server i, and the key matrix gets multiplied by A_i.

2) Various algorithms can be designed to decode the encoded matrix in case of loss of the key. This project can be extended to the analysis and design of such algorithms.

Roles and Contribution:-

Code:-

- ➡ Manjal Shah
- ➡ Nikhil Vaghasiya

Report:-

- ➡ Kashyap Halavadia
- ➡ Mukund Ladani

Presentation:-

- ➡ By the entire team.

We have done the project as a team, each one of us has tried to help the other whenever someone had some confusion or doubt.