**Logo, company name

Description automatically generated**

**Text Encryption**

By:

Ahmed Ashraf Mohamed 202000563

Ali Fouad Marzban 202002450

Mohamed Yaser Aboshama 202001242

Mostafa Samer Dorrah 202000125

Yousif Adel Khalil 202000238

# **Table of Contents**

**Cover Page**………………………………………………………………………….……1

**Table of Contents**……………………………………………………………………..….2

**Abstract**………………………………………………………………………………..…4

**Introduction**…………………………………………………………………………..….5

**Literature Review**………………………………………………………………….……6

**3.1 History of Text Encryption**………………………………………………6

**3.2 Types of Text Encryption**………………………………………………...7

**3.2.1 Advanced Encryption Standard (AES)**………………………………….8

**3.2.2 Data Encryption Standard (DES)**………………………………………..8

**3.2.3 Rivest-Shamir-Adleman (RSA)**……………………………………….….8

**Mathematical Formulation of Text Encryption**………………………………………..9

**4.1 The Matrix……………………………………………………………...**9

**4.2 Matrix multiplication………………………………………………....**10

**4.3 Inverse matrix………………………………………..………………..**11

**4.4 Identity matrix………………………………………………….....…..**11

**4.5 Modulo 26…………………………………………………..………….**12

**Methodology**…………………………………………………………………………….13

**Results & Analysis**……………………………………………………………………...16

**Conclusion**……………………………………………………………………………....18

**Appendix**………………………………………………………………………………...19

**References**…………………………………………………………………………….…24

# **Abstract**

# Since the beginning of the communication, there exists a need to share information secretly. The need for secrecy and its various applications gave rise to cryptography. Text encryption technique is one of effective means of information security. Based on analyzing the parallels between text watermarking and text encryption, a text encryption algorithm based on natural language processing is proposed. Three linguistic transformations in natural language processing are introduced [5]. Finally, the requirements and the process of the text encryption algorithm are provided. So, in this paper we discuss the history of text encryption, and we discuss the types of text encryption such as AES, DES, and RSA. The AES, DES, and RSA are the three most popular encryption methods. And discuss the Mathematical Formulation of Text Encryption (Matrix, Matrix multiplication, Inverse matrix, Identity matrix, Modulo).

# **Introduction**

Information security plays a significant part in the development of communication system, where more randomization in the mysterious keys expands the security just as the intricacy of the cryptography calculations. In the new year’s network security has turned into a significant concern. Cryptography assumes an essential part in the data security framework against different assaults. Cryptography is a technique for encoding or decoding data to cover its genuine significance with other innovation and send data subtly. In software engineering, it alludes to using a calculation that is hard to unravel, change messages, and assurance information security (Mathur & Bansode, 2019) [1]. In cryptography, plaintext is decoded data, instead of data scrambled for capacity or transmission. Plaintext generally implies decoded data forthcoming contribution to cryptographic calculations, ordinarily encryption calculations. Plaintext generally alludes to information that is communicated or put away decoded while ciphertext is the aftereffect of encryption performed on plaintext utilizing a calculation, called a code. Ciphertext is otherwise called scrambled or encoded data since it contains a type of the first plaintext that is muddled by a human or PC without the legitimate code to unscramble it. Encryption is a type of information security where data is changed over to ciphertext. Just approved individuals who have the key can interpret the code and access the first plaintext data while decryption, the reverse of encryption, is the most common way of transforming ciphertext into clear plaintext. Ciphertext isn't to be mistaken for code text on the grounds that the last option is an aftereffect of a Code, not a code.

Qr code

Description automatically generated

# **Literature Review**

Throughout this literature review, this section attempts to clarify the history of text encryption, development of the progression of text encryption, and types of text encryption.

## **3.1 History of Text Encryption**

Cryptography, or the use of codes and cyphers to keep secrets safe, has been practiced since ancient times. Until past decades, it has been the story of what could be called classic cryptography — that is, of techniques of encryption that use pen and paper, or perhaps basic mechanical aids. The innovation of highly complicated mechanical and electromechanical devices, including the Enigma rotor machine, offered more sophisticated and efficient methods of encryption in the early twentieth century, and the successive beginning of electronics and computing has granted elaborate plans of even increasing complexity, the significant proportion of which are unsuited to pen and paper.

Cryptography has developed in lockstep with cryptanalysis, or the "breaking" of codes and ciphertext. The rapid detection and application of frequency distribution to the decoding of encryption software has changed the world on several occasions. As a result, the Zimmermann Telegram prompted the United States' entry into World War I, and the Allies' decryption of Nazi Germany's cyphers delayed World War II by as much as two years, according to several estimates.

Secure cryptography was mainly the province of governments until the 1960s. The introduction of public encryption standard (DES) and the creation of public-key cryptography now have pushed it into the public domain.

## **3.2 Types of Text Encryption**

AES, DES, and RSA are the three most popular encryption methods. Although there are numerous various methods of encryption, we will focus on three among the most used. The majority are mostly modifications of earlier models, and many are no more authorized or suggested. Daily, technology progresses, that even the most up-to-date devices will eventually be superseded by later models.

## **3.2.1 Advanced Encryption Standard (AES)**

Advanced Encryption Standard (AES), among the strongest cryptographic methods, is used for sensitive communications by governments, security organizations, and everyday businesses. The AES method computes "symmetric" key encryption.[4] To decrypt the information, someone on the receiving end will require a key.

## **3.2.2 Data Encryption Standard (DES)**

DES encryption, which has been acknowledged as a standard of encryption in the 1970s, is no longer considered to be secure on its own. It only encrypts 56 bits of information at a time, and it has been quickly discovered to be vulnerable to hacking. It has, however, served as a basis for more secure encryption solutions in the future.[4]

## **3.2.3 Rivest-Shamir-Adleman (RSA)**

"Rivest-Shamir-Adleman," or RSA, is another popularly used encryption method. It is often used to encrypt information sent through the internet and depends on a public key to do so. To decrypt the communications, everyone on the receiving end will have their own private key.[4] It's been shown to be a safe technique to exchange data among people who don't know one another yet wish to connect without endangering their sensitive and confidential information.

# **Mathematical Formulation of Text Encryption**

In this section we will explain in details the important linear algebra methods that is used in the text encryption techniques that uses linear algebra.

* 1. **The Matrix**

Matrix is a linear combination of vectors that form a rectangular shape using the numbers in the vectors and it is added between rectangular brackets.[1]

A picture containing text, shoji, clock

Description automatically generated

Each Matrix is made of a specific dimension that is often referred to as M by N. M is the number of rows and N is the number of columns in the matrix.[1]

M Rows

N columns A picture containing text, shoji, clock

Description automatically generated

In computer and programming Matrix is used in a lot in things like image processing, image representation, graph representation, and even text encryption.[1]

* 1. **Matrix Multiplication**

When multiplying 2 matrices there are an important rule that must be fulfilled first which is that the number of columns in the first matrix must equal the number of rows in the second Matrix and these dimensions are called the inner dimensions. For example, if we have 2 matrices the first with dimension 3x1 and the second with dimensions 2x1 the multiplication between them cannot be done because the inner dimensions are not equal but if the second matrix was with dimensions 3x1 then the multiplication is possible because they both have inner dimensions 3. To know the dimensions of the output of multiplying 2 matrices we will take the outer dimensions for example, if we have 2x3 and 3x4 matrices the output’s dimensions will be 2x4.[1]

When multiplying 2 matrices for example they both have dimensions 2x2 so the output will be 2x2 also so to find the number in the output row 1 column 1 we will multiply row 1 in the first matrix with column 1 in the second matrix. Then to find the number in the output row 1 column 2 we multiply row 1 in matrix 1 with column 2 in matrix 2. Then to find the number in the output row 2 column 1 we take row 2 in matrix 1 and multiply it with column 1 in matrix 2. Then to find the last number which is in the output row 2 column 2 we multiply row 2 in matrix 1 with column 2 in matrix 2.[1]

A picture containing text, watch, clock, gauge

Description automatically generated = A picture containing text, clock

Description automatically generated = A close-up of some writing

Description automatically generated with low confidence

* 1. **Inverse matrix**

The inverse of a matrix is the opposite to it for example if we have a matrix called A the inverse will be .[1] So, to get the inverse of a matrix with dimensions 2x2 we can get the inverse by following this equation:

A close-up of a calculator

Description automatically generated with low confidence

For example, if we have a 2x2 matrix with numbers 7,17,2, and 5.

A picture containing text, clock, watch, gauge

Description automatically generated

Its inverse will be:

A picture containing diagram

Description automatically generated

A picture containing text, clock, watch, gauge

Description automatically generated

So now the inverse of 7,17,2, and 5 is 5, -17, -2,7

* 1. **Identity matrix**

The Identity of a matrix is that when a matrix is multiplied by its inverse, they should be matrix with the same dimensions, with diagonals all are 1 and the other numbers are 0. If the matrix doesn’t have an identity, then this matrix doesn’t have any inverse.[1]

For example, if we used the last example which is the 2x2 matrix with numbers 7,17,2 and 5 to check if the inverse we did is right or wrong we will multiply it with its inverse.

A picture containing text, clock, watch, gauge

Description automatically generated = Text

Description automatically generated

=  so that means that the inverse of the matrix is correct.

* 1. Modulo 26

Modulo 26 is a technique used to scale the number lager than 25 so that they can be represented by letters.

![A picture containing text, wall, clock, white

Description automatically generated]()

The way is work is that it divides the number bigger than 25 with 26 and the remainder will be the number that represent the letter in the photo above.

For example, if we have the number 222 and we want to know which letter it represents we will divide 222 with 26 and then we will get a remainder of 14 this means that 222 represent letter O.[2]

# **Methodology**

**Encryption process**

Firstly, we assigned each letter in the alphabets to a number. So, this simple scheme A=0, B = 1, …, Z = 25 was used as shown in **fig. (2).**

Calendar

Description automatically generated

**Figure. (2)**

Matrix multiplication will be used to change the message matrix, so that nobody could decipher the result without the key. To encrypt the message with a key there are 5 steps should be passed.

* Create a square matrix of 2x2 which is called key matrix (Encoding matrix), but this matrix must be invertible matrix.
* Convert the message to Matrix of 2 rows by converting each letter to its corresponding number.
* Multiply the encoding matrix by the message matrix then a new matrix will be generated.
* Reduce modulo 26.
* Convert the new matrix to characters to get the encrypted message.

Let’s illustrate by encoding “YOUSEF” with the key “HLOL” as shown in the following.

Convert the key text (“HLOL”) to a matrix of 2x2 called K and Convert the message (“YOUSEF”) to a matrix of 2 rows called M.

K= M=

Multiplicate the two matrix and reduce modulo 26 for the resulted matrix which called C (cipher text).

C = KM = = (Mod 26)

C = (Mod 26) =

Finally, when converting the C matrix to text. it will give the encoded message which is “ASCEUX” in our example.

**Decryption process**

Matrix Identity property will be used to decrypt the encoded message and return the real message. As we said in the previous that the cipher matrix is C=KM so to get the message matrix. the inverse matrix will be used. so, you should apply left multiplication by the inverse matrix of the key matrix for this equation C=KM. After applying the multiplication, the equation will be = then =. the conclusion, in order to get the message matrix, you should multiply the inverse of key matrix by the cipher matrix. As shown in the following.

get the inverse of the key matrix:

K= , Determinant=((7x11) - (11x14)) mod (26) = 1

mod (26)

then after we have got the inverse key matrix () we should multiply it with the cipher matrix:

M = = mod (26)

M =

Finally, we got the message matrix, so to get the message, the numbers of the matrix should be converted to characters.

so, if we converted the numbers to characters, the result will be “Yousef” the same word that we have encrypted.

# **Results & Analysis**

Graphical user interface, application

Description automatically generated

* As shown in the image when the user typed his message (yousef) in the message place and enter a key of 4 letters (hlol) (these key characters when converted to numbers must produce a key matrix that is invertible) and press on Encrypt button, the message will be encrypted and appear on the screen (The Encrypted Message: ACCCUV). if the user typed his encrypted message (ACCCUV) in the Encrypted message place and enter the key that he used in the encryption process (hlol) and press on Decrypt button, the encrypted message will be decrypted and appear on the screen (The Decrypted Message: Yousef).

Graphical user interface, application

Description automatically generated

* As shown in the above image when the user enters a key. these key characters when converted to numbers produced a key matrix that is uninvertible. then the program will display a message saying “uninvertible key, Enter another key”.

Graphical user interface, application

Description automatically generated

* if the user enters a key (more than 4 letters). the program will take the first 4 letters and will neglect the others.

# **Conclusion**

Now we have reviewed most all things about text encryption by the history of Text encryption that the Cryptography, or the use of codes and ciphers to keep secrets safe, has been practiced since ancient times. And reviewed the types of it that include Advanced Encryption Standard (AES): is used for sensitive communications by governments, security organizations, and everyday businesses, Data Encryption Standard (DES): It only encrypts 56 bits of information at a time, and it has been quickly discovered to be vulnerable to hacking, Rivest-Shamir-Adleman (RSA): It is used to encrypt information sent through the internet and depends on a public key to do so; their types are the most common encryption methods. Also discussed is the Mathematical Formulation of Text Encryption and explained in detail the important linear algebra methods that are used in the text encryption techniques that use linear algebra such as (Matrix, Matrix multiplication, Inverse matrix, Identity matrix, Modulo). And showed the Encryption process method that uses matrix multiplication to change the message matrix, Decryption process method that using the matrix Identity property to decrypt the encoded message and return the real message.

# **Appendix**

#Hill Cipher Program

import numpy as np

from tkinter import \*

# we used tkinter to create the GUI

# we used numpy to ease the use of the arrays

# this function is to encrypt the message with the key(matrix)

def encrypt():

msg=x1.get()

cipher=y1.get()

global msg\_length

msg\_length=len(msg)

msg = msg.replace(" ", "")

C = make\_key(cipher)

len\_check = len(msg) % 2 == 0

if not len\_check:

msg += "0"

P = matrix\_string(msg)

msg\_len = int(len(msg) / 2)

encrypted\_msg = ""

for i in range(msg\_len):

# product of matrix

row\_0 = P[0][i] \* C[0][0] + P[1][i] \* C[0][1]

integer = int(row\_0 % 26 + 65)

encrypted\_msg += chr(integer)

row\_1 = P[0][i] \* C[1][0] + P[1][i] \* C[1][1]

integer = int(row\_1 % 26 + 65)

encrypted\_msg += chr(integer)

Label(text=encrypted\_msg ,font=80,fg='black').place(x=312,y=170)

return

# this function is to decrypt the message with the key(matrix)

def decrypt():

encrypted\_msg=x2.get()

cipher=y2.get()

C = make\_key(cipher)

determinant = C[0][0] \* C[1][1] - C[0][1] \* C[1][0]

determinant = determinant % 26

multiplicative\_inverse = multiplicative(determinant)

C\_inverse = C

C\_inverse[0][0], C\_inverse[1][1] = C\_inverse[1, 1], C\_inverse[0, 0]

C[0][1] \*= -1

C[1][0] \*= -1

for row in range(2):

for column in range(2):

C\_inverse[row][column] \*= multiplicative\_inverse

C\_inverse[row][column] = C\_inverse[row][column] % 26

P = matrix\_string(encrypted\_msg)

msg\_len = int(len(encrypted\_msg) / 2)

decrypted\_msg = ""

for i in range(msg\_len):

column\_0 = P[0][i] \* C\_inverse[0][0] + P[1][i] \* C\_inverse[0][1]

integer = int(column\_0 % 26 + 65)

decrypted\_msg += chr(integer)

column\_1 = P[0][i] \* C\_inverse[1][0] + P[1][i] \* C\_inverse[1][1]

integer = int(column\_1 % 26 + 65)

decrypted\_msg += chr(integer)

if msg\_length%2!=0:

decrypted\_msg = decrypted\_msg[:-1]

Label(text=decrypted\_msg ,font=80,fg='black').place(x=312,y=400)

return

# this function is used to check the multiplicative inverse of the key matrix

def multiplicative(determinant):

multiplicative\_inverse = -1

for i in range(26):

inverse = determinant \* i

if inverse % 26 == 1:

multiplicative\_inverse = i

break

return multiplicative\_inverse

# this function is used to make the key matrix

def make\_key(cipher):

determinant = 0

C = None

while True:

C = matrix\_string(cipher)

determinant = C[0][0] \* C[1][1] - C[0][1] \* C[1][0]

determinant = determinant % 26

inverse\_element = multiplicative(determinant)

if inverse\_element == -1:

messagebox.showwarning("Error","uninvertible key , Enter another key")

quit()

else:

break

return C

# this function is used to create matrix of integers from string

def matrix\_string(string):

integers = []

for char in string:

char = char.upper()

integer = ord(char) - 65

integers.append(integer)

length = len(integers)

M = np.zeros((2, int(length / 2)))

iterator = 0

for column in range(int(length / 2)):

for row in range(2):

M[row][column] = integers[iterator]

iterator += 1

return M

# the part below is mainly for the GUI (labels, buttons & etc.)

window=Tk()

window.geometry('550x500+300+150')

window.title('Hill Cipher')

e=Button(text='Encrypt',command=encrypt,bd=10,font=90,height=1,width=16,fg='white',bg='green').place(x=200,y=90)

d=Button(text='Decrypt',command=decrypt,bd=10,font=90,height=1,width=16,fg='black',bg='red').place(x=200,y=310)

messagetxt=Label(text='Message',font=80,fg='black').place(x=150,y=13)

keytxt=Label(text='key (4 letters)',font=80,fg='black').place(x=120,y=55)

encrypted\_messagetxt=Label(text='The Encrypted Message: ' ,font=80,fg='black').place(x=80,y=170)

messagetxt2=Label(text='Encrypted Message' ,font=20,fg='black').place(x=75,y=232)

messagetxt2=Label(text='The Decrypted Message: ' ,font=20,fg='black').place(x=75,y=400)

keytxt2=Label(text='key (4 letters)',font=80,fg='black').place(x=120,y=273)

x1=StringVar()

y1=StringVar()

message1=Entry(textvariable=x1, width=30).place(x=270,y=20)

key1=Entry(textvariable=y1, width=30).place(x=270,y=60)

x2=StringVar()

y2=StringVar()

message2=Entry(textvariable=x2, width=30).place(x=270,y=240)

key2=Entry(textvariable=y2, width=30).place(x=270,y=280)

window.mainloop()

# **References**

1. *Hill cipher project introduction vectors and matrices*. Retrieved from

<https://massey.limfinity.com/207/hillcipher.pdf>

2. Khan Academy. *What is modular arithmetic?* Retrieved from

<https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic>

*3. Chapter 16: Cryptography*. World Scientific. Retrieved from

<https://www.worldscientific.com/doi/abs/10.1142/9789811238819_0016>

4. 2019, August 21.Knerl, L. . *What are the different types of encryption?: HP® Tech takes*. What Are the Different Types of Encryption? | HP® Tech Takes. Retrieved from

<https://www.hp.com/us-en/shop/tech-takes/what-are-different-types-of-encryption>

*5. S2SLE: An encryption methodology for securing data using.* Retrieved from

<https://www.researchgate.net/publication/280302289_S2SLE_An_Encryption_Methodology_for_Securing_Data_using_Linear_Algebraic_Equations>

6. 2021, July 21. *Hill cipher*. GeeksforGeeks. Retrieved from

<https://www.geeksforgeeks.org/hill-cipher/>