

Introduction to Cryptography

Cryptography: is the study of the techniques of writing and decoding messages in code.

Cipher: A procedure that will render a message unintelligible to the recipient. Used to also recreate the original message.

Plaintext: The message or information that is being encrypted.

Ciphertext: The message or information that is created after the cipher has been used.

Encrypting a Message

1. Each character of the plaintext is given a numerical value.
2. These values are then separated into vectors, S.T. the number of rows of each vector is equivalent to the number of rows of the cipher matrix.
Values are placed into each vector one at a time, going down a row for each value. Once a vector is filled the next vector is created. If the last vector does not get filled by the plaintext then the remaining entries will hold the value for a space.
3. The vectors are then augmented to form a matrix that contains the plaintext.
4. The plaintext matrix is then multiplied with the cipher matrix to create the ciphertext matrix.

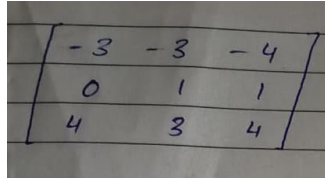
Decrypting a Message

1. To decrypt a ciphertext matrix the original cipher matrix must be used. The cipher matrix must be inverted in order to decrypt the ciphertext.
2. This inverted cipher matrix is then multiplied with the ciphertext matrix.
The product produces the original plaintext matrix.
3. The plaintext can be found again by taking this product and splitting it back up into its separate vectors, and then converting the numbers back into their letter forms.

Message Encryption

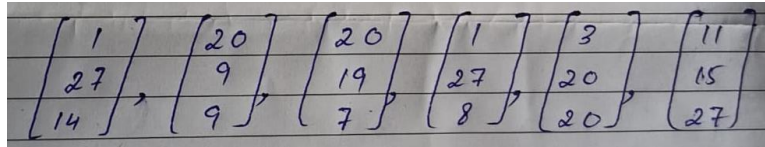
- Let Cipher Matrix

A =



-3	-3	-4
0	1	1
4	3	4

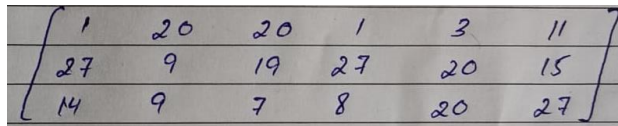
- For this example, we 'll use;
ATTACK IS TONIGHT
- Now replace each letter with its numerical equivalent given above in the chart
1, 20, 20, 1, 3, 11, 27, 9, 19, 27, 20, 15, 14, 9, 7, 8, 20
- Now separate the plaintext into 3x1 vector until the whole plaintext is used



$\begin{bmatrix} 1 \\ 27 \\ 14 \end{bmatrix}$	$\begin{bmatrix} 20 \\ 9 \\ 9 \end{bmatrix}$	$\begin{bmatrix} 20 \\ 19 \\ 7 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 27 \\ 8 \end{bmatrix}$	$\begin{bmatrix} 3 \\ 20 \\ 20 \end{bmatrix}$	$\begin{bmatrix} 11 \\ 15 \\ 27 \end{bmatrix}$
---	--	---	--	---	--

- Augment these Vector into a plaintext matrix

B =

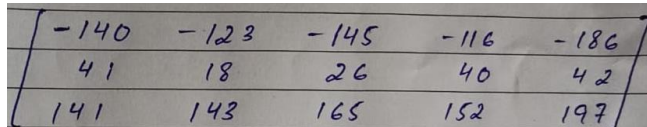


1	20	20	1	3	11
27	9	19	27	20	15
14	9	7	8	20	27

- Multiply the plaintext matrix with the cipher matrix to form the encrypted matrix

AxB

- The new form matrix contains the ciphertext



-140	-123	-145	-116	-186
41	18	26	40	42
141	143	165	152	197

Message Decryption

- To decrypt the matrix back into plaintext matrix, multiply it by the inverse of cipher

$$\left[\begin{array}{ccc|ccc} -3 & -3 & -4 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 4 & 3 & 4 & 0 & 0 & 1 \end{array} \right]$$

$$\begin{aligned} R_1 \times (-1/3) & \left[\begin{array}{ccc|ccc} 1 & 1 & 4/3 & -1/3 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 4 & 3 & 4 & 0 & 0 & 1 \end{array} \right] \\ R_2 + (-1)R_1 & \left[\begin{array}{ccc|ccc} 1 & 1 & 4/3 & -1/3 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & -1 & -4/3 & 4/3 & 0 & 1 \end{array} \right] \\ R_1 + (-1)R_2 & \left[\begin{array}{ccc|ccc} 1 & 0 & 1/3 & -1/3 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1/3 & 4/3 & 1 & 1 \end{array} \right] \\ R_2 + (1)R_2 & \left[\begin{array}{ccc|ccc} 1 & 0 & 1/3 & -1/3 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1/3 & 4/3 & 1 & 1 \end{array} \right] \\ R_3 \times (-3) & \left[\begin{array}{ccc|ccc} 1 & 0 & 1/3 & -1/3 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -4 & -3 & -3 \end{array} \right] \\ R_1 + (-1/3)R_3 & \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/3 & 0 & 1 \\ 0 & 1 & 0 & 4 & 4 & 3 \\ 0 & 0 & 1 & -4 & -3 & -3 \end{array} \right] \\ R_2 + (-1)R_3 & \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/3 & 0 & 1 \\ 0 & 1 & 0 & 4 & 4 & 3 \\ 0 & 0 & 1 & -4 & -3 & -3 \end{array} \right] \end{aligned}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & 3 \end{bmatrix} \times \begin{bmatrix} 146 & -123 & 145 & -116 & -186 \\ 41 & 18 & 26 & 46 & 42 \\ 141 & 143 & 165 & 152 & 197 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 20 & 20 & 1 & 3 & 11 \\ 27 & 9 & 19 & 27 & 20 & 15 \\ 14 & 9 & 7 & 8 & 20 & 27 \end{bmatrix}$$

0		9	I	18	R
1	A	10	J	19	S
2	B	11	K	20	T
3	C	12	L	21	U
4	D	13	M	22	V
5	E	14	N	23	W
6	F	15	O	24	X
7	G	16	P	25	Y
8	H	17	Q	26	Z

Now if we look at the decrypted message and compare it with given chart

Note*:

In our case 0 is equals to space

1 = a,

20 = t,

20 = t,

1 = a,

3 = c,

11 = k,

27 = space (0),

9 = l,

19 = s,

27 = space (0),

20 = t,

15 = o,

14 = n,

9 = l,

7 = g,

8 = h,

20 = t,

27 = space (0)

Decrypted Message = "ATTACK IS TONIGHT"

Encryption/Decryption Algorithm:

```
# import the numpy module
import numpy
# import the module
from numpy import random

Crypto = {"0": 27, "a": 1, "b": 2, "c": 3, "d": 4, "e": 5, "f": 6, "g": 7, "h": 8,
, "i": 9, "j": 10, "k": 11, "l": 12, "m": 13,
    "n": 14, "o": 15, "p": 16, "q": 17, "r": 18, "s": 19, "t": 20, "u": 21, "v":
22, "w": 23, "x": 24, "y": 25, "z": 26}

Cryptolist = list(Crypto)

message = "Attack is tonight"

message = message.replace(" ", "0")

message = message.lower()

j = 0
EmptyList = []

character = ""
for i in message:
    character = message[j]
    j = j + 1
    y = 0
    item = ""
    for x in Crypto:
        if(character == x):
            EmptyList.append(Crypto[x])
            y = y + 1

filledList = EmptyList

NewListLength = len(EmptyList)
Zeroslist = []
while(True):
    if(NewListLength%3 != 0):
        Zeroslist.append(27)
        NewListLength = NewListLength + 1
    else:
        break
```

```

NewList = EmptyList + Zeroslist

listArray = numpy.array(NewList)

listArray1 = listArray.reshape(3, int(len(NewList)/3))

cipherarray = numpy.array([[-3, -3, -4],[0, 1, 1], [4, 3, 4]])
cipherarrayInverse = numpy.linalg.inv(cipherarray)

encryptedmessage = numpy.dot(cipherarray, listArray1)
print(f"Encryted Message:\n{encryptedmessage}")

decryptedmessage = numpy.dot(cipherarrayInverse, encryptedmessage)

print(f"\nDecryted Message:\n{decryptedmessage}")

decryptedmessage = listArray.tolist()

key_list = list(Crypto.keys())
val_list = list(Crypto.values())
b = 0
position = 0
EmptyList1 = []
for a in decryptedmessage:
    b = b + 1
    k = 0
    for c in Crypto:
        if(a == Crypto[c]):
            value = val_list.index(Crypto[c])
            EmptyList1.append(key_list[value])
            k = k + 1

print("\nDecryted Message in plaintext:")
for plaintext in EmptyList1:
    if(plaintext == '0'):
        print(" ", end="")
    else:
        print(plaintext, end="")

```

Output:

```
File Edit Selection View Go Run Terminal Help    Cryptography.py - WebAPI Projects - Visual Studio Code

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

HOME@DESKTOP-R5SJM5B MINGW64 ~/Downloads/Programming/WebAPI Projects
$ python Cryptography.py
Encrypted Message:
[[-140 -123 -145 -116 -149 -186]
 [ 41  18  26  35  40  42]
 [ 141 143 165 117 152 197]]

Decrypted Message:
[[ 1. 20. 20.  1.  3. 11.]
 [27.  9. 19. 27. 20. 15.]
 [14.  9.  7.  8. 20. 27.]]

Decrypted Message in plaintext:
attack is tonight
HOME@DESKTOP-R5SJM5B MINGW64 ~/Downloads/Programming/WebAPI Projects
$
```