32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34

2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

19 3d e3 b3 a0 f4 e2 2b 9a c6 8d 2a e9 f8 48 08

a0 fa fe 17 88 54 2c b1 23 a3 39 39 2a 6c 76 05

a4 9c 7f f2 68 9f 35 2b 6b 5b ea 43 02 6a 50 49

f2 c2 95 f2 7a 96 b9 43 59 35 80 7a 73 59 f6 7f

aa 8f 5f 03 61 dd e3 ef 82 d2 4a d2 68 32 46 9a

3d 80 47 7d 47 16 fe 3e 1e 23 7e 44 6d 7a 88 3b

48 6c 4e ee 67 1d 9d 0d 4d e3 b1 38 d6 5f f8 e7

ef 44 a5 41 a8 52 5b 7f b6 71 25 3b db 0b ad 00

e0 92 7f e8 c8 63 63 c0 d9 b1 35 50 85 b8 be 01

d4 d1 c6 f8 7c 83 9d 87 ca f2 b8 bc 11 f9 15 bc

f1 00 6f 55 c1 92 4c ef 7c c8 8b 32 5d b5 d5 0c

6d 88 a3 7a 11 0b 3e f ddb f9 86 41 ca 00 93 fd

26 0e 2e 17 3d 41 b7 7d e8 64 72 a9 fd d2 8b 25

4e f4 f9 0e 5f 5f c9 f3 84 a6 rf b2 4e a6 dc 4f 4f

fa 41 42 b1 19 49 dc 1f a3 e0 19 65 7a 8c 04 0c

ea 83 5c f0 04 45 33 2d 65 5d 98 ad 85 96 b0 c5

eb 40 f2 1e 59 2e 38 84 8b a1 13 e7 1b c3 42 d2

39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32

|  |  |
| --- | --- |
| Crambones Team | |
|  | |
| Abdullah Mohamed Abd El Ghany | Section 10 |
| Hazem Youssef El-Sebaay | Section 6 |
| Rodaina Hesham Sokkar | Section 8 |
| Hassan Adham Hassan | Section 7 |
| Dina Yahia Hussien | Section 8 |

Substitute Bytes

Shifting Rows

Mix Columns

Generate Round Key

Add Round Key

Counter = Counter+1

Input Plaintext

Input Key

Add Round Key

Counter = 1

Substitute Bytes

Shifting Rows

Generate 10th Round Key

Add Round Key

Output Ciphertext

Counter<=9

Yes

No

**AES Encryption Flowchart**

Inverse Shift Rows

Inverse Substitute Bytes

Get Round Key

Add Round Key

Inverse Mix Columns

Counter = Counter+1

Input Ciphertext

Get 10th Round Key

Add Round Key

Counter = 1

Counter<=9

Inverse Shift Rows

Inverse Substitute Bytes

Get Round Key

Add Round Key

Output Plaintext

**AES Decryption Flowchart**

No

Yes

AES-Networking

Encrypting

Decrypting

Shift

Rows

Encrypt

Mix

Columns

Encrypt

Copy

Key

ToAll

Keys

mixColumns

Decrypt1

Add Round

Key

Add

Round

Key

Substitute

Bytes

Encrypt

Substitute

Bytes

Decrypt

Shift

Rows

Decrypt

GenerateAll

Keys

mixColumns

Decrypt2

Key

Generation

**Procedures Hierarchy**