Muhammad Izham Bin Norhamadi
B032020039
BITZ

Tutorial 4 128-bit AES

Do the initial and first round of AES Encryption on the string plaintext M using the symmetric key K below. Take the plaintext M as the first 16 character of your name instead. You are also given K written in hexadecimals.

```
String Plaintext  M = "Muhammad Izham B"
String Cipher Key K = "FTMKUTeM31OGOS57"

Input Plaintext M =
      4d 75 68 61 6d 6d 61 64 20 49 7a 68 61 6d 20 42

Cipher Key      K =

      46  54  4D  4B  55  54  65  4D  33  31  4F  47  4F  53  35  37
```

1. XOR input plaintext with Key K_0

Initial State Round 0 ⊕ Initial Key 0 = Input State Round 1

4D	6D	20	61
75	6D	49	6D
68	61	7A	20
61	64	68	42

⊕

46	55	33	4F
54	54	31	53
4D	65	4F	35
4B	4D	47	37

=

0B	38	13	2E
21	39	78	3E
25	04	35	15
2A	29	2F	75

Round	Start of Round	After SubBytes	After ShiftRows	After Mix Columns		Round Key Value	
0 input	4D 6D 20 61 75 6D 49 6D 68 61 7A 20 61 64 68 42				⊕	46 55 33 4F 54 54 31 53 4D 65 4F 35 4B 4D 47 37	=
1 input	0B 38 13 2E 21 39 78 3E 25 04 35 15 2A 29 2F 75				⊕	AA FF CC 83 C2 96 A7 F4 D7 B2 FD C8 CF 82 C5 F2	=

Muhammad Izham Bin Norhamadi
B032020039
BITZ

2. **SubBytes**() Transformation

S1=

0B	38	13	2E
21	39	78	3E
25	04	35	15
2A	29	2F	75

A=

2B	07	7D	31
FD	12	BC	B2
3F	F2	96	59
E5	A5	15	9D

Round	Start of Round	After SubBytes	After ShiftRows	After Mix Columns		Round Key Value	
1 input	0B 38 13 2E 21 39 78 3E 25 04 35 15 2A 29 2F 75	2B 07 7D 31 FD 12 BC B2 3F F2 96 59 E5 A5 15 9D			⊕	AA FF CC 83 C2 96 A7 F4 D7 B2 FD C8 CF 82 C5 F2	=

3. **ShiftRows**() Transformation

A=

2B	07	7D	31
FD	12	BC	B2
3F	F2	96	59
E5	A5	15	9D

B=

2B	07	7D	31
12	BC	B2	FD
96	59	3F	F2
9D	E5	A5	15

Round	Start of Round	After SubBytes	After ShiftRows	After Mix Columns		Round Key Value	
1 input	0B 38 13 2E 21 39 78 3E 25 04 35 15 2A 29 2F 75	2B 07 7D 31 FD 12 BC B2 3F F2 96 59 E5 A5 15 9D	2B 07 7D 31 12 BC B2 FD 96 59 3F F2 9D E5 A5 15		⊕	AA FF CC 83 C2 96 A7 F4 D7 B2 FD C8 CF 82 C5 F2	=

Muhammad Izham Bin Norhamadi
B032020039
BITZ

4. **MixColumns**() Transformation

$$C = \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 2B & 07 & 7D & 31 \\ 12 & BC & B2 & FD \\ 96 & 59 & 3F & F2 \\ 9D & E5 & A5 & 15 \end{bmatrix}$$

C =

6B	6D	AC	AD
33	6A	E7	C8
B2	3D	45	0C
D8	3D	5B	76

C_{00} =

```
01·2B = 00101011
02·2B = 01010110 = 56

01·12 = 00010010
02·12 = 00100100
03·12 = 00110110 = 36

01·96 = 10010110

01·9D = 10011101

01010110 = 56
00110110 = 36
10010110 = 96
10011101 = 9D
01101011 = 6B
```

C_{01} =

```
01·07 = 00000111
02·07 = 00001110 = 0E

01·BC = 10111100
02·BC =101111000
02·BC +100011011
02·BC = 01100011
01·BC = 10111100
03·BC = 11011111 = DF
```

Muhammad Izham Bin Norhamadi
B032020039
BITZ

01·59 = 01011001

01·E5 = 11100101

00001110
11011111
01011001
11100101
01101101 = 6D

C_{02} =
01·7D = 01111101
02·7D = 11111010 = FA

01·B2 = 10110010
02·B2 =101100100
02·B2 +100011011
02·B2 = 01111111
01·B2 = 10111100
03·B2 = 11000011 = C3
CC

01·3F = 00111111

01·A5 = 10100101

11111010
11000011
00111111
10100101
10100011 = A3
AC

C_{03} =
01·31 = 00110001
02·31 = 01100010 = FA

01·FD = 11111101
02·FD =111111010
02·FD +100011011
02·FD = 11100101
01·FD = 11111101
03·FD = 00011000 = 18

Muhammad Izham Bin Norhamadi
B032020039
BITZ

01·F2 = 11110010

01·15 = 00100101

01100010
00011000
11110010
00100101
10101101 = AD

C_{10} =
01·2B = 00101011

01·12 = 00010010
02·12 = 00100100 = 24

01·96 = 10010110
02·96 =100101100
02·96 +100011011
02·96 = 10100001
01·96 = 10010110
03·96 = 00110111 = 37

A1

01·9D = 10011101

00101011
00100100
00110111
10011101
10100101 = A5

33

C_{11} =
01·07 = 00000111

01·BC = 10111100
02·BC =101111000
02·BC +100011011
02·BC = 01100011 = 63

Muhammad Izham Bin Norhamadi
B032020039
BITZ

01·59 = 01011001
02·59 = 10110010
01·59 = 01011001
03·59 = 11101011 = EB

01·E5 = 11100101

00000111
01100011
11101011
11100101
01101010 = 6A

C_{12} =
01·7D = 01111101

01·B2 = 10110010
02·B2 =101100100
02·B2 +100011011
02·B2 = 11001101 = CD
7E

01·3F = 00111111
02·3F = 01111110
01·3F = 00111111
03·3F = 01000001 = 41

01·A5 = 10100101

01111101
11001101
01000001
10100101
01010100 = 54
E7

C_{13} =
01·31 = 00110001

01·FD = 11111101
02·FD =111111010
02·FD +100011011
02·FD = 11100001 = E1

01·F2 = 11110010
02·F2 =111100100
02·F2 +100011011

Muhammad Izham Bin Norhamadi
B032020039
BITZ

02·F2 = 11111111
01·F2 = 11110010
03·F2 = 00001101 = 0D

01·15 = 00010101

= C8

C_{20} =
01·2B

01·12

02·96 = 00110111 = 37

03·9D = 10111100 = BC

= B2

C_{21} =
01·07

01·BC

02·59 = B2

03·E5 = 34

= 3D

C_{22} =
01·7D

01·B2

02·3F = 7E

03·A5 = F4

= 45

C_{23} =
01·31

01·FD

Muhammad Izham Bin Norhamadi
B032020039
BITZ

02·F2 = FF

03·15 = 3F

= 0C

C_{30} =
03·2B = 7D

01·12

01·96

02·9D = 21

= D8

C_{31} =
03·07 = 9

01·BC

01·59

02·E5 = D1

= 3D

C_{32} =
03·7D = 87

01·B2

01·3F

02·A5 = 51

= 5B

C_{33} =
03·31 = 53

01·FD

01·F2

Muhammad Izham Bin Norhamadi
B032020039
BITZ

02·15 = 2A

= 76

Round	Start of Round				After SubBytes				After ShiftRows				After Mix Columns					Round Key Value				
1 input	0B	38	13	2E	2B	07	7D	31	2B	07	7D	31	6B	6D	AC	AD		AA	FF	CC	83	
	21	39	78	3E	FD	12	BC	B2	12	BC	B2	FD	33	6A	E7	C8	⊕	C2	96	A7	F4	
	25	04	35	15	3F	F2	96	59	96	59	3F	F2	B2	3D	45	0C		D7	B2	FD	C8	=
	2A	29	2F	75	E5	A5	15	9D	9D	E5	A5	15	D8	3D	5B	76		CF	82	C5	F2	

5. XOR key_1

Initial State Round 2

	6B	6D	AC	AD		AA	FF	CC	83		C1	92	6F	2E
C =	33	6A	E7	C8		C2	96	A7	F4		F1	FC	F3	3C
	B2	3D	45	0C	⊕	D7	B2	FD	C8	=	65	8F	B8	C4
	D8	3D	5B	76		CF	82	C5	F2		17	BF	9E	84

6. Inverse Mix Column operation

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

6B	6D	AC	AD
A5	6A	E7	C8
B2	3D	45	0C
D8	3D	5B	76

2B	07	7D	31
12	BC	B2	FD
96	59	3F	F2
9D	E5	A5	15

E_{00} =
0E·6B + 0B·33 + 0D·B2 + 09·D8
14 + D6 + AB + 42 = 2B

E_{10} =
09·6B + 0E·33 + 0B·B2 + 0D·D8
1E + 29 + 2A + 0F = 12

E_{20} =
0D·6B + 09·33 + 0E·B2 + 0B·D8

Muhammad Izham Bin Norhamadi
B032020039
BITZ

A9 + B0 + 66 + E9 = 96

E_{30} =
0B·6B + 0D·33 + 09·B2 + 0E·D8
C8 + 7C + 55 + 7C = 9D

E_{01} =
0E·6D + 0B·6A + 0D·3D + 09·3D
30 + C3 + 3A + CE = 07

E_{11} =
09·6D + 0E·6A + 0B·3D + 0D·3D
28 + 1A + B4 + 3A = BC

E_{21} =
0D·6D + 09·6A + 0E·3D + 0B·3D
87 + 17 + 7D + B4 = 59

E_{31} =
0B·6D + 0D·6A + 09·3D + 0E·3D
F2 + A4 + CE + 7D = E5

E_{02} =
0E·AC + 0B·E7 + 0D·45 + 09·5B
D2 + 4B + 54 + B5 = 78