

Message(ASCII):- codesmilecodesmi Message(Hexa):- 63 6f 64 65 73 6d 69 6c 65 63 6f 64 65 73 6d 69 Key(Hexa):- f6 cc 34 cd c5 55 c5 41 82 54 26 02 03 ad 3e cd Cipher(Hexa):- dd 08 e5 ae a1 1a 78 0c 59 f9 68 cc 33 fb 8e ff					
Initialization:- Fill key and plain text matrix	Input bits 63 73 65 65 6f 6d 63 73 64 69 6f 6d 65 6c 64 69	Key bits f6 c5 82 03 cc 55 54 ad 34 c5 26 3e cd 41 02 cd			
Key expansion:- W[0:43]	w[0] = f6 cc 34 cd w[1] = c5 55 c5 41 w[2] = 82 54 26 02 w[3] = 03 ad 3e cd	RotWord()= ad 3e cd 03 SubWord()= 95 b2 bd 7b ^ Rcon()= 94 b2 bd 7b w[4] = 62 7e 89 b6 w[5] = a7 2b 4c f7 w[6] = 25 7f 6a f5 w[7] = 26 d2 54 38	RotWord()= d2 54 38 26 SubWord()= b5 20 07 f7 ^ Rcon()= b7 20 07 f7 w[8] = d5 5e 8e 41 w[9] = 72 75 c2 b6 w[10] = 57 0a a8 43 w[11] = 71 d8 fc 7b		
	RotWord()= d8 fc 7b 71 SubWord()= 61 b0 21 a3 ^ Rcon()= 65 b0 21 a3 w[12] = b0 ee af e2 w[13] = c2 9b 6d 54 w[14] = 95 91 c5 17 w[15] = e4 49 39 6c	RotWord()= 49 39 6c e4 SubWord()= 3b 12 50 69 ^ Rcon()= 33 12 50 69 w[16] = 83 fc ff 8b w[17] = 41 67 92 df w[18] = d4 f6 57 c8 w[19] = 30 bf 6e a4	RotWord()= bf 6e a4 30 SubWord()= 08 9f 49 04 ^ Rcon()= 18 9f 49 04 w[20] = 9b 63 b6 8f w[21] = da 04 24 50 w[22] = 0e f2 73 98 w[23] = 3e 4d 1d 3c		
	RotWord()= 4d 1d 3c 3e SubWord()= e3 a4 eb b2 ^ Rcon()= c3 a4 eb b2 w[24] = 58 c7 5d 3d w[25] = 82 c3 79 6d w[26] = 8c 31 0a f5 w[27] = b2 7c 17 c9	RotWord()= 7c 17 c9 b2 SubWord()= 10 f0 dd 37 ^ Rcon()= 50 f0 dd 37 w[28] = 08 37 80 0a w[29] = 8a f4 f9 67 w[30] = 06 c5 f3 92 w[31] = b4 b9 e4 5b	RotWord()= b9 e4 5b b4 SubWord()= 56 69 39 8d ^ Rcon()= d6 69 39 8d w[32] = de 5e b9 87 w[33] = 54 aa 40 e0 w[34] = 52 6f b3 72 w[35] = e6 d6 57 29		
	RotWord()= d6 57 29 e6 SubWord()= f6 5b a5 8e ^ Rcon()= ed 5b a5 8e w[36] = 33 05 1c 09 w[37] = 67 af 5c e9 w[38] = 35 c0 ef 9b w[39] = d3 16 b8 b2	RotWord()= 16 b8 b2 d3 SubWord()= 47 6c 37 66 ^ Rcon()= 71 6c 37 66 w[40] = 42 69 2b 6f w[41] = 25 c6 77 86 w[42] = 10 06 98 1d w[43] = c3 10 20 af			
Initial state (Key Addition Layer)	<u>Round Key</u> f6 c5 82 03 cc 55 54 ad 34 c5 26 3e cd 41 02 cd	<u>Plain</u> 63 73 65 65 6f 6d 63 73 64 69 6f 6d 65 6c 64 69	<u>Result</u> 95 b6 e7 66 a3 38 37 de 50 ac 49 53 a8 2d 66 a4		
Round 1	<u>Round Key</u> 62 a7 25 26 7e 2b 7f d2 89 4c 6a 54 b6 f7 f5 38	<u>AfterByteSub</u> 2a 4e 94 33 0a 07 9a 1d 53 91 3b ed c2 d8 33 49	<u>After Shift</u> 2a 4e 94 33 07 9a 1d 0a 3b ed 53 91 49 c2 d8 33	<u>AfterMixColumns</u> 2f 06 9f da 20 8f 83 bc 80 48 5c 55 d0 3a 42 a8	<u>KeyAddition</u> 4d a1 ba fc 5e a4 fc 6e 09 04 36 01 66 cd b7 90

Round 2	<u>Round Key</u> d5 72 57 71 5e 75 0a d8 8e c2 a8 fc 41 b6 43 7b	<u>AfterByteSub</u> e3 32 f4 b0 58 49 b0 9f 01 f2 05 7c 33 bd a9 60	<u>AfterShiftRows</u> e3 32 f4 b0 49 b0 9f 58 05 7c 01 f2 60 33 bd a9	<u>AfterMixColumns</u> 63 e0 f5 c8 1e fe 6f a4 00 2f b5 f7 b2 fc f8 28	<u>KeyAddition</u> b6 92 a2 b9 40 8b 65 7c 8e ed 1d 0b f3 4a bb 53
Round 3	<u>Round Key</u> b0 c2 95 e4 ee 9b 91 49 af 6d c5 39 e2 54 17 6c	<u>AfterByteSub</u> 4e 4f 3a 56 09 3d 4d 10 19 55 a4 2b 0d d6 ea ed	<u>AfterShiftRows</u> 4e 4f 3a 56 3d 4d 10 09 a4 2b 19 55 ed 0d d6 ea	<u>AfterMixColumns</u> 92 6f 8b 08 2e a5 e7 51 0c 43 79 d0 8a ad f0 69	<u>KeyAddition</u> 22 ad 1e ec c0 3e 76 18 a3 2e bc e9 68 f9 e7 05
Round 4	<u>Round Key</u> 83 41 d4 30 fc 67 f6 bf ff 92 57 6e 8b df c8 a4	<u>AfterByteSub</u> 93 95 72 ce ba b2 38 ad 0a 31 65 1e 45 99 94 6b	<u>AfterShiftRows</u> 93 95 72 ce b2 38 ad ba 65 1e 0a 31 6b 45 99 94	<u>AfterMixColumns</u> fe 22 9b f7 28 82 b4 66 56 5e 7b b1 af 08 18 f1	<u>KeyAddition</u> 7d 63 4f c7 d4 e5 42 d9 a9 cc 2c df 24 d7 d0 55
Round 5	<u>Round Key</u> 9b da 0e 3e 63 04 f2 4d b6 24 73 1d 8f 50 98 3c	<u>AfterByteSub</u> ff fb 84 c6 48 d9 2c 35 d3 4b 71 9e 36 0e 70 fc	<u>AfterShiftRows</u> ff fb 84 c6 d9 2c 35 48 71 9e d3 4b fc 36 0e 70	<u>AfterMixColumns</u> 18 31 91 74 39 2c 8e fb db aa 1e 88 51 c8 6d b2	<u>KeyAddition</u> 83 eb 9f 4a 5a 28 7c b6 6d 8e 6d 95 de 98 f5 8e
Round 6	<u>Round Key</u> 58 82 8c b2 c7 c3 31 7c 5d 79 0a 17 3d 6d f5 c9	<u>AfterByteSub</u> ec e9 db d6 be 34 10 4e 3c 19 3c 2a 1d 46 e6 19	<u>AfterShiftRows</u> ec e9 db d6 34 10 4e be 3c 2a 3c 19 19 1d 46 e6	<u>AfterMixColumns</u> ba ce 05 91 d9 aa 45 7c 8b 8a 27 6b 15 20 88 11	<u>KeyAddition</u> e2 4c 89 23 1e 69 74 00 d6 f3 2d 7c 28 4d 7d d8
Round 7	<u>Round Key</u> 08 8a 06 b4 37 f4 c5 b9 80 f9 f3 e4 0a 67 92 5b	<u>AfterByteSub</u> 98 29 a7 26 72 f9 92 63 f6 0d d8 10 34 e3 ff 61	<u>AfterShiftRows</u> 98 29 a7 26 f9 92 63 72 d8 10 f6 0d 61 34 e3 ff	<u>AfterMixColumns</u> 82 db e5 28 63 12 83 2a 69 c7 0d 54 50 91 ba f0	<u>KeyAddition</u> 8a 51 e3 9c 54 e6 46 93 e9 3e fe b0 5a f6 28 ab
Round 8	<u>Round Key</u> de 54 52 e6 5e aa 6f d6 b9 40 b3 57 87 e0 72 29	<u>AfterByteSub</u> 7e d1 11 de 20 8e 5a dc 1e b2 bb e7 be 42 34 62	<u>AfterShiftRows</u> 7e d1 11 de 8e 5a dc 20 bb e7 1e b2 62 be 42 34	<u>AfterMixColumns</u> ac 0e 01 41 cd e9 d2 67 3b 87 37 dd 73 b2 75 83	<u>KeyAddition</u> 72 5a 53 a7 93 43 bd b1 82 c7 84 8a f4 52 07 aa
Round 9	<u>Round key</u> 33 67 35 d3 05 af c0 16 1c 5c ef b8 09 e9 9b b2	<u>AfterByteSub</u> 40 be ed 5c dc 1a 7a c8 13 c6 5f 7e bf 00 c5 ac	<u>AfterShiftRows</u> 40 be ed 5c 1a 7a c8 dc 5f 7e 13 c6 ac bf 00 c5	<u>AfterMixColumns</u> 5d 28 91 c4 39 77 53 6b 0b e2 03 43 c6 b8 f7 6f	<u>KeyAddition</u> 6e 4f a4 17 3c d8 93 7d 17 be ec fb Cf 51 6c dd
Round 10	<u>Round key</u> 42 25 10 c3 69 c6 06 10 2b 77 98 20 6f 86 1d af	<u>AfterByteSub</u> 9f 84 49 f0 eb 61 dc ff f0 ae ce 0f 8a d1 50 c1	<u>AfterShiftRows</u> 9f 84 49 f0 61 dc ff eb ce 0f f0 ae c1 8a d1 50	No Inverse mix columns in this round	<u>KeyAddition</u> dd a1 59 33 08 1a f9 fb e5 78 68 8e ae 0c cc ff

Other test cases: -

One Block Example:-

Plaintext(ASCII):- abcdefghabcdefgh

Plaintext(Hexa):- 61 62 63 64 65 66 67 68 61 62 63 64 65 66 67 68

Key(Hexa):- 61 62 63 64 65 66 67 68 61 62 63 64 65 66 67 68

Key(ASCII):- abcdefghabcdefgh

Cipher(Hexa):- ff 4e b3 ad 54 a5 e1 4a ec b2 10 8b 0e 0a 65 80

.....

3 Blocks Example

Plaintext (ASCII):- Information technology department

Plaintext (After handling):- Information technology department*****

Plaintext(Hexa):-

49 6e 66 6f 72 6d 61 74 69 6f 6e 20 74 65 63 68

6e 6f 6c 6f 67 79 20 64 65 70 61 72 74 6d 65 6e

74 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a

Key(Hexa):- 61 62 63 64 65 66 67 68 61 62 63 64 65 66 67 68

Key(ASCII):- abcdefghabcdefgh

Cipher(Hexa):-

f4 2a 5a a9 d5 80 c9 47 ae 95 54 eb 79 e7 d0 3c

fe 9b ed 53 cd 0a 5a 37 2e 6d 77 9a 19 aa 5c 90

83 44 b6 26 84 41 5f 51 b2 4d 6d 43 d5 7f ce 54

.....

Plaintext less than one block: -

Plaintext (ASCII):- Friday

Plaintext After Handling :- Friday*****

Plaintext(Hexa):- 46 72 69 64 61 79 2a 2a 2a 2a 2a 2a 2a 2a 2a

Key(Hexa):- 61 62 63 64 65 66 67 68 61 62 63 64 65 66 67 68

Key(ASCII):- abcdefghabcdefgh

Cipher(Hexa):-

8b 94 d7 19 91 14 b8 6e 14 75 1e 7d b8 a9 2e 9f

.....

Key less than one block: -

Plaintext(Hexa):- Friday*****

Key(Hexa):- 61 62 63 64 65 66 67 68

Key(ASCII):- abcdefgh

Displaying error message and request another key from user.