CSS 322 – QUIZ 2

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________ out of 10

Question 1 [2 marks]

Explain an advantage of the Feistel structure for block ciphers.

Question 2 [4 marks]

True or false:

a) The decryption procedure for DES is the inverse of the encryption procedure. T F

b) A desirable property of an encryption algorithm is that small changes in plaintext values produces large changes in the output ciphertext. T F

c) The Initial Permutation in DES adds security to the overall algorithm by providing *confusion* of the bits. T F

d) Rijndael produces different ciphertext which is different in length to the input plaintext T F

Question 3 [4 marks]

The following information is shows part of the decryption procedure for Simplified AES (including the decryption S-Box, mix columns matrix and GF(2^4) multiplication table). Given the values of A and K2, determine the values of B, C, D and E.

K2: 0101 0101 1001 0000

A: 1101 0000 0000 1001

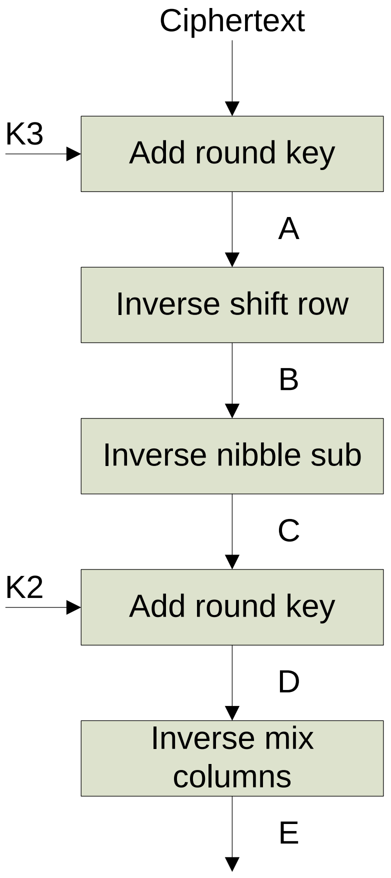
B: __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

C: __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

D: __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

E: __ __ __ __ X X X X X X X X __ __ __ __

(that is, you only need to calculate the first and fourth nibble for E)



$$\begin{bmatrix} 1010 & 0101 & 1001 & 1011 \\ 0001 & 0111 & 1000 & 1111 \\ 0110 & 0000 & 0010 & 0011 \\ 1100 & 0100 & 1101 & 1110 \end{bmatrix}$$

$$\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix}$$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A