CSS 322 – QUIZ 2C

First name: _____   Last name: _____

ID: _____   Total Marks: _____

out of 10

Question 1 [2 marks]

A block cipher must be reversible. Give an example of a block cipher that operates on 2-bit blocks that is:

a) Reversible

b) Not reversible

Question 2 [3 marks]

Indicate whether each statement is True or False (circle the correct answer):

a) A desirable property of an encryption algorithm is that small changes in key values produces large changes in the output ciphertext   T / F

b) DES is no longer recommended for use because the Feistel structure does not provide adequate security.   T / F

c) Galois field arithmetic is used in the AES Mix Column operation.   T / F

d) AES can use a larger block size than DES.   T / F

e) Because of the weaknesses of DES, AES does not use *rounds*.   T / F

f) 16 subkeys are generated for DES encryption – we must generate another 16 different subkeys for the corresponding DES decryption operation.   T / F

Question 3 [1.5 marks]

S-DES can be represented by the following equation:

$$Ciphertext = IP^{-1}\left(f_k\left(SW\left(f_{k_1}\left(IP(planitext)\right)\right)\right)\right)$$

Where f_{ki} is the round function, IP is the initial permutation and SW is swapping the halves.

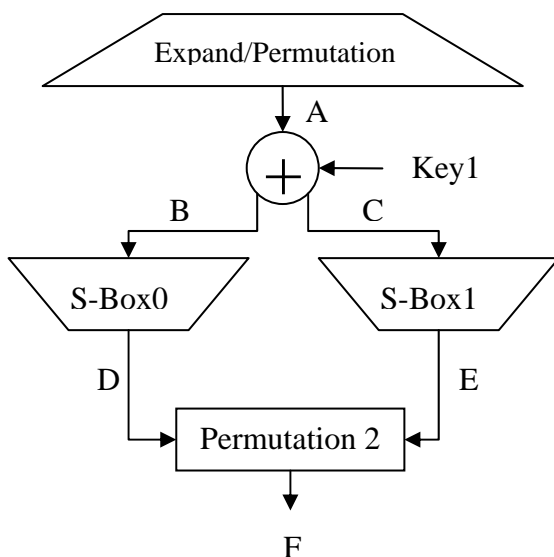Write a similar equation for the decryption in S-DES

Question 4 [3.5 marks]

Calculate the values for B, C, D, E and F in the diagram for S-DES encryption below, where A = 11001010 and Key 1 = 01011000. You may use the information below the diagram.

Answer (B): _____   Answer (C): _____

Answer (D): _____   Answer (E): _____

Answer (F): _____

Expand/Permutation with 8 bit input, output bit order is: 4 1 2 3 2 3 4 1

Permutation 2, output bit order is: 2 4 3 1

S-Box 0   S-Box 1

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \qquad S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$