CSS 322 – QUIZ 3

First name: _____ Last name: _____

ID: _____ Total Marks: _____

out of 10

Question 1 [3 marks]

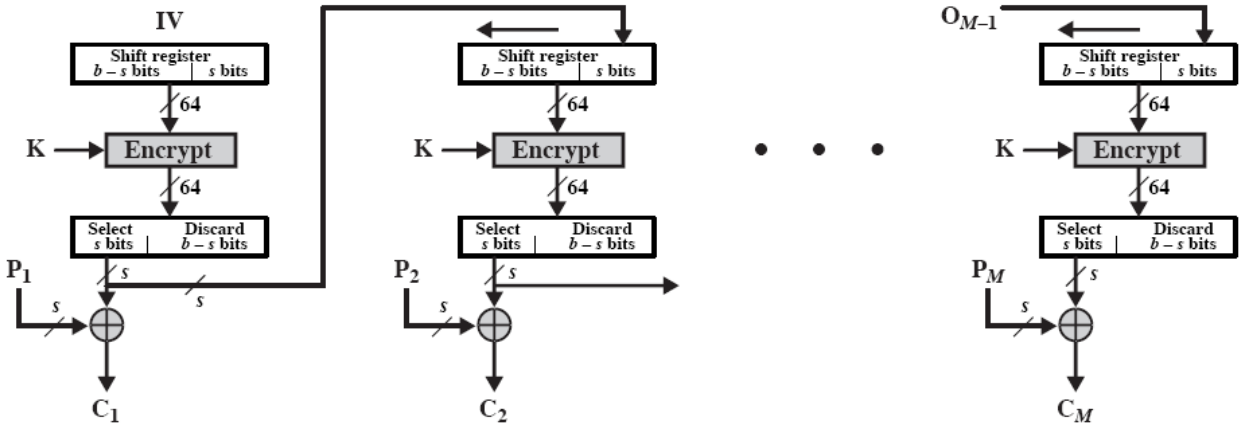
Assume you have designed a 4-bit block cipher that produces the following Ciphertext when used with a key *K*:

P	**C**	**P**	**C**	**P**	**C**	**P**	**C**
0000	0101	0100	0010	1000	1110	1100	1000
0001	1001	0101	0111	1001	1011	1101	0100
0010	1101	0110	0000	1010	1100	1110	0011
0011	1111	0111	1010	1011	0001	1111	0110

If you use your cipher in the Counter mode of operation (with initial value of 0), what is the plaintext for the ciphertext C = 011001001010 and key *K*.

Question 2 [3 marks]

The following diagram shows the encryption phase of the Output Feedback Mode of operation for 64-bit block ciphers.



Assume you are using a modified Output Feedback Mode that operates on 4-bit block ciphers and it is used with the encryption algorithm designed in Question 2. The plaintext blocks are 2-bits. What is the ciphertext for the plaintext P = 01101011 encrypted using key *K*? The Initialisation Vector is 0000.

Question 3 [4 marks]

Assume you designed your own encryption algorithm, *A*, which uses 4-bit blocks and 2-bit keys. The ciphertext for a *selection* of plaintext and keys for the algorithm, *A*, are given below.

	Key			
Plaintext	**00**	**01**	**10**	**11**
0001	1101	0111	1101	0110
0101	0000	0110	0111	1010
0111	0101	1101	1111	0011
1000	0111	1000	1100	1101

To increase the strength of your algorithm, *A*, against brute-force attack, you apply the algorithm twice using a 4-bit key, *K*. The first two bits of *K* are used as a key into *A* to encrypt the plaintext to produce output *X*, and the second two bits of *K* are used as a key into *A* to encrypt *X* to produce the ciphertext. You call this new algorithm *Double-A*.

An attacker has discovered a pair of (plaintext, ciphertext) for *Double-A*:

(0101, 1101)

a) Use the meet-in-the-middle attack to determine the most likely key *K* used to produce this ciphertext.

b) A limitation of the meet-in-the-middle attack is the amount of memory needed. Explain why, and give the approximate amount of memory needed to perform the attack on Double-DES (which uses two 56-bit keys)?