CSS322 – Quiz 2

Name: _____

ID: _____ Mark: _____ (out of 10)

Question 1 [4 marks]

a) The one-time pad is considered to be “unconditionally secure”. Explain what that means (referring to the amount of processing power needed to break the cipher and the time needed). [1 mark]

b) Explain the important difference between how a one-time pad using Caesar cipher operates and the Vigenere cipher operates. [1 marks]

c) Explain two reasons why the one-time pad is not considered useful for most practical applications. [2 marks]

Question 2 [2 marks]

Assume I designed my own cipher to encrypt exam answers. The cipher uses a 40 bit key. I always create the answers 10 days before the exam and store them on my office computer, however on the same day that I created the exam answers a malicious student obtained access to my office computer and took a copy of the answers. The malicious student has free access to a computer that can decrypt the answers at a rate of 200×10^9 attempts per day (as the student wants to cheat on the exam, they don't know about any limitations in the encryption algorithm). Is this system used for encrypting exams computationally secure? Explain your answer, showing any calculations where necessary.

(Note that $2^{10} \approx 10^3$, $2^{20} \approx 10^6$, $2^{30} \approx 10^9$, and so on)

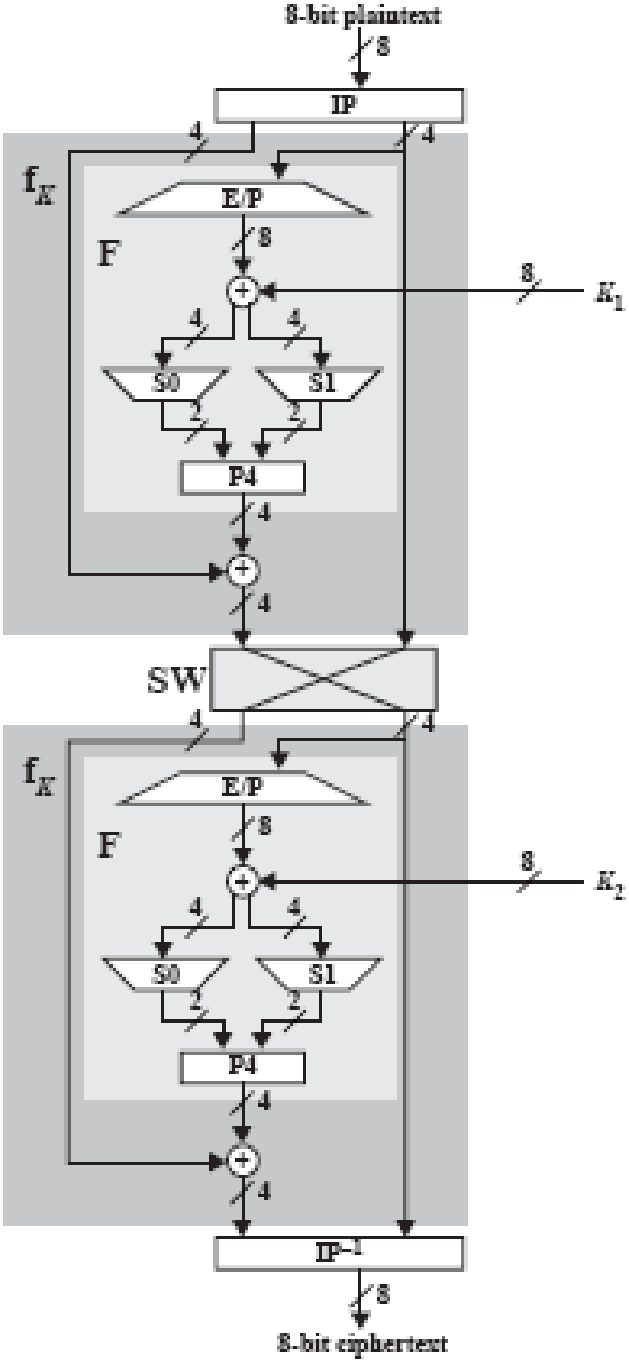
Question 3 [4 marks]

Consider S-DES encryption below. Assume the output of IP is 01101010 and K1 is 11100111. What is:

a) The output of E/P? ___ ___ ___ ___ ___ ___ ___ ___

b) The output of S0? ___ ___

c) The input to the 2nd round? ___ ___ ___ ___ ___ ___ ___ ___



IP: 2 6 3 1 4 8 5 7

IP^{-1}: 4 1 3 5 7 2 8 6

E/P: 4 1 2 3 2 3 4 1

P4: 2 4 3 1

S0:

01	00	11	10
11	10	01	00
00	10	01	11
11	01	11	10

S1:

00	01	10	11
10	00	01	11
11	00	01	00
10	01	00	11