CSS322 – Quiz 2 Answers

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]

Answer

Unconditionally secure means even with infinite processing power and infinite time to break the cipher, the attacker still cannot determine the original plaintext.

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

Answer

One-time pad must use a keyword as long as the input plaintext and truly random. The Vigenere may use a shorter (and non-random) keyword. The keyword is repeated until the length of plaintext is reached.

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

Answer

The keyword must as long as the input plaintext. Therefore to distribute the key uses a lot of resources, making communications inefficient.

The keyword must be random and change every time. It is difficult to produce truly random data over a long period of time (the data is often pseudo random, containing some structure).

Question 2 [2 marks]

Assume I designed my own cipher to encrypt exam answers. The cipher uses a 40/50 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)

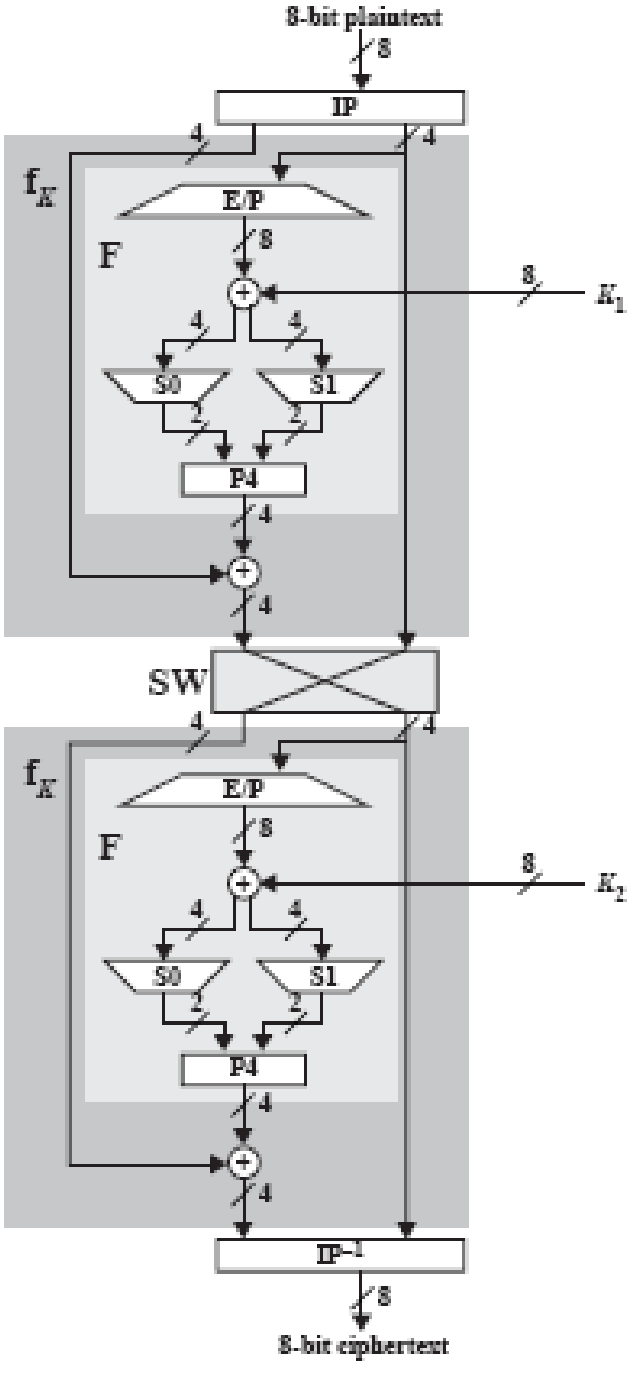
Answer

If the student applies a brute force attack, the maximum time to find an answer is:

40 bit key: $\approx 10^{12}$ combinations, at a rate of $2x10^{11}$ per day would take 5 days to find the answers. On average it would be even less. Therefore with this key size the system is not computationally secure because the malicious student could obtain valuable information will that information is still valid (i.e. before the exam).

50 bit key: $\approx 10^{18}$ combinations, at a rate of $2x10^{11}$ per day would take more than 5000 days to find the answers. On average less than half that (e.g. 2500 days) but still the malicious student cannot find the answers before the exam. Therefore it is considered computationally secure, because the time to find the answers is much greater than the valid lifetime of the information.

(Of course this may change if the conditions change, e.g. the student has access to a much faster computer or supercomputer).



Question 3 [4 marks]

Consider S-DES encryption below. Assume the output of IP is 01101010/01001110/11101001/01001011 and K1 is 11100111/00011100/01010101/10101101. What is:

a) The output of E/O?

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

Answer

Start: 01101010, K1: 11100111	Start: 01001110, K1: 00011100
Output of EP: 01010101	01111101
Output of S0: 11	10
Input to 2nd round: 10101101	11100111
Start: 11101001, K1: 01010101	Start: 01001011, K1: 10101101
Output of EP: 11000011	11010111
Output of S0: 11	00
Input to 2nd round: 10010001	10110100