CSS322 – Quiz 2

Name: _____ ID: _____ Marks: _____ (10)

Question 1 [2 marks]

The DES encryption operation, which has 16 rounds, can be written as:

$$ciphertext = IP^{-1}\left(f_{K_{16}}\left(SW\left(f_{K_{15}}\left(SW\left(\ldots\left(f_{K_2}\left(SW\left(f_{K_1}\left(IP\left(plaintext\right)\right)\right)\right)\right)\right)\right)\right)\right)$$

where IP is an initial permutation, f_{K_x} is a round function using key K_x and SW is a switch operation. Write an equation for the DES decryption operation.

Question 2 [3 marks]

(a) DES is no longer recommended for use today because:

i. Practical timing attacks are possible against it

ii. The avalance effect is not present

iii. The key length is too short

iv. The block size is too short

(b) A meet-in-the-middle attack on a Double-DES cipher:

i. Requires an average of approximately 2^{112} operations

ii. Involves storing approximately 2^{56} blocks in memory to work in practice

iii. Requires the attacker to know more than 2^{40} plaintext/ciphertext pairs to work in practice

iv. Does not involve applying a brute-force attack on (single) DES

(c) An ideal 4-bit block cipher would have:

i. 16 possible keys (or transformations)

ii. 16! possible keys (or transformations)

iii. 8 possible different plaintext blocks

iv. 16! possible different plaintext blocks

Question 3 [3 marks]

(a) The concept of _____ in block ciphers aims to reduce the statistical nature of input plaintext in the output ciphertext.

(b) A _____ cipher is well suited for real-time encryption, whereas a _____ cipher is better suited for encrypting files.

(c) The classical rails fence and rows/column ciphers are known as _____ ciphers.

Question 4 [2 marks]

If the initial permutation, IP, of S-DES was `[2 8 7 5 3 4 6 1]` then IP^{-1} would be: