

# CSS322 – Quiz 2

Name: \_\_\_\_\_ ID: \_\_\_\_\_ Marks: \_\_\_\_\_ (10)

## Question 1 [2 marks]

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

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

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:
- The key space is too small
  - The S-Boxes are considered insecure
  - The avalanche effect is not present
  - There are not enough rounds
- (b) An ideal  $n$ -bit block cipher would have:
- $2n$  possible different plaintext blocks
  - $2^n!$  possible different plaintext blocks
  - $2^n$  possible keys (or transformations)
  - $2^n!$  possible keys (or transformations)
- (c) A meet-in-the-middle attack on a Double-DES cipher:
- Requires an average of approximately  $2^{112}$  operations
  - Involves storing approximately  $2^{56}$  blocks in memory to work in practice
  - Requires the attacker to know more than  $2^{40}$  plaintext/ciphertext pairs to work in practice
  - Does not involve applying a brute-force attack on (single) DES

**Question 3** [3 marks]

- (a) The Feistel structure for block ciphers achieves security by using multiple rounds, where in each round it alternates between \_\_\_\_\_ and \_\_\_\_\_.
- (b) Two commonly used block ciphers today are 3DES and \_\_\_\_\_.
- (c) Techniques that hide messages in fake messages in order to avoid others knowing secret communications are taking place are referred to as \_\_\_\_\_.

**Question 4** [2 marks]

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