

CSS 322 – QUIZ 2 ANSWERS

First name: _____ Last name: _____

ID: _____

Total Marks: _____

out of 10

- Write your name and ID in the space provided at the top of the sheet.
- Answer the questions on this sheet(s) only, using the space given.

Question 1 [2 marks]

Confusion is a fundamental concept in block ciphers: *confusion* aims to make the relationship between the ciphertext and key as complex as possible, usually using a complex substitution algorithm. In DES, select the component that provides the most *confusion* (only select one):

1. Initial Permutation
2. Expand and Permutation operation
3. Swapping the left and right halves

4. S-Boxes

5. Permutation of S-box outputs
6. Exclusive OR operations

Question 2 [2.5 marks]

Indicate whether each statement is True or False (circle the correct answer):

- a) A desirable property of an encryption algorithm is that small changes in key values produces small changes in the output ciphertext T / F
- b) 16 subkeys are generated for DES encryption – we must generate another 16 different subkeys for the corresponding DES decryption operation. T / F
- c) DES is no longer recommended for use because the Feistel structure does not provide adequate security. T / F
- d) A stream cipher would be better than a block cipher if encrypting an Internet-based telephone conversation. T / F
- e) AES can use a larger block size than DES. T / F

Question 3 [2.5 marks]

Connect the operations on the left with the correct description on the right for Simplified AES:

- | | |
|-----------------------------|---|
| a. Nibble substitution | 1. uses an exclusive OR on a round key. |
| b. The Shift Row operation | 2. uses an exclusive OR with a 8-bit constant (10000000) |
| c. The Add Key operation | 3. swaps the 2 nd and 4 th nibbles in the state matrix. |
| d. The Mix column operation | 4. uses S-Boxes. |
| e. Key generation | 5. uses Galois Field GF(2 ⁴) arithmetic. |

Answers:

- Nibble substitution: 4. uses S-Boxes
- The Shift Row operation: 3. swaps the 2nd and 4th nibbles in the state matrix.
- The Add Key operation: 1. uses an exclusive OR on a round key.
- The Mix column operation: 5. uses Galois Field $GF(2^4)$ arithmetic.
- Key generation: 2. uses an exclusive OR with a 8-bit constant (10000000) OR 4. uses S-Boxes.

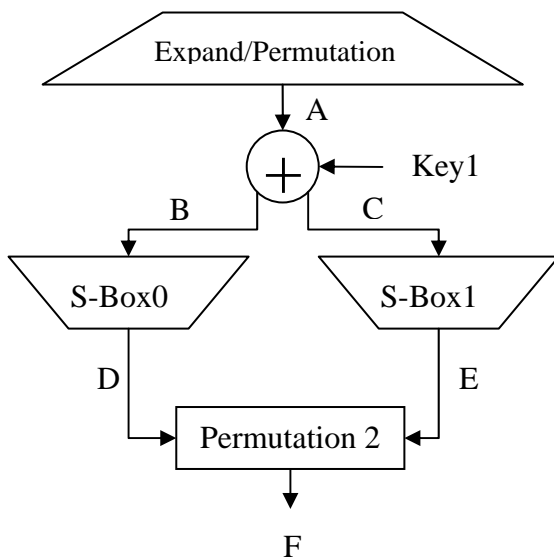
Question 4 [3 marks]

Calculate the values for B, C, D, E and F in the diagram for S-DES encryption below, where $A = 10011101$ and Key 1 = 01010000. You may use the information below the diagram.

Answer (B): 1100 Answer (C): 1101

Answer (D): 01 Answer (E): 00

Answer (F): 1000



Expand/Permutation with 8 bit input, output bit order is: 4 1 2 3 2 3 4 1

Permutation 2, output bit order is: 2 4 3 1

S-Box 0

S-Box 1

$$S_0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$