

# CSS322 – Quiz 2

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

## Question 1 [5 marks]

Consider a 4 bit block cipher, called *ABC*, that uses 2-bit keys. The ciphertext for a selection of plaintext and keys for cipher *ABC* are given below.

Plaintext	00	01	10	11
0000	0001	0101	1000	0111
0001	1101	0111	1101	0101
0101	0000	0110	0111	1010
0111	0101	1101	1111	0011
1000	0111	1000	1100	1101
1001	1001	1111	1011	0001
1101	0011	1001	0001	1011
1111	1110	0001	0110	1111

To increase the strength of *ABC* against brute-force attack, you apply the algorithm twice using a 4-bit key,  $K$ , which is two independent keys from *ABC*. The resulting cipher is *Double-ABC*.

- (a) If I choose the key 1100, what is the original plaintext for the ciphertext 0000? [2 marks]
- (b) I have chosen a new key and sent multiple ciphertexts to my friend. You are an attacker that has discovered a pair of (plaintext, ciphertext): (0111, 0001). Use a meet-in-the-middle attack to determine the most likely key I used. Show and explain the steps. [3 marks]

**Question 2** [4 marks]

- (a) You select two prime numbers to use in RSA key generation to be: 17, 13. Calculate and fill in the values for the two keys generated if  $e$  is the smallest valid value chosen which is greater than 8. [3 marks]

PU = ( \_\_\_\_\_ , \_\_\_\_\_ ) and PR = ( \_\_\_\_\_ , \_\_\_\_\_ )

- (b) Write an equation that represents the decryption of the ciphertext 24 that was confidentially sent using the keys in part (a). You may use the actual values (e.g. 3), or simply variables (e.g.  $e$ ) in your equation. You don't have to calculate the answer, just write the equation. [1 mark]

**Question 3** [1 marks]

Which of the following cannot be used as a PRNG?

- (a) ANSI X9.17
- (b) Blum Blum Shub
- (c) 3DES
- (d) RC4
- (e) LCG
- (f) None of the above