CSS322 – Quiz 3

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

Question 1 [2 marks]

Consider a mono-alphabetic cipher, with a selected mapping from plaintext to ciphertext for all possible plaintext values shown below (the mapping is split into two to fit it on the page).

```
p: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a
C: V W O Q R C P m f e g H q Z S t h F z r w Y c y D o -

p: b c d e f g h i j k l m n o p q r s t u v w x y z _ -
C: l L u _ E K s B A v n G N i T b k X p M j I U a J x d
```

(a) With a computer that can make 10^{12} decrypt attempts per second, what is the worst case time for a brute force attack? [2 marks]

Question 2 [3 marks]

(a) ______________________ is a security service that assures the received data originated from the claimed sender.

(b) In a ______________________ attack, a malicious user sends an identical copy of a previous message they have intercepted.

(c) The information known only to sender and receiver in a cipher is called a______________________

Question 3 [2 marks]

Consider the ciphertext `fsxbosrrlteweixuco` output from a rows/columns transposition cipher using the key `236451`. What is the plaintext?

Plaintext: ______________________________

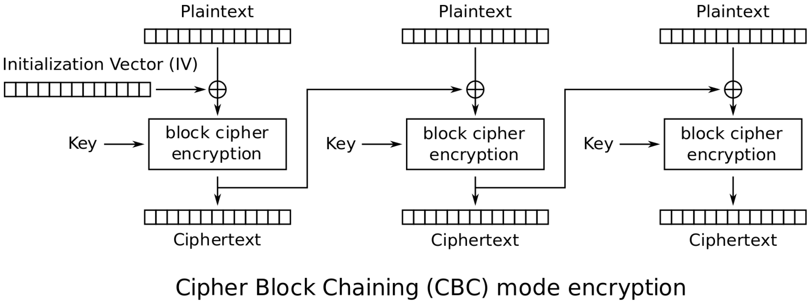

Figure 1: CBC encryption

Question 4 [2 marks]

Using block cipher *ABC* (the single version shown in the table), the plaintext 11010011 is encrypted using key 10 with CBC and IV 1110 (encryption with CBC is shown in

Figure 1). What is the ciphertext? [3 marks]

Question 5 [3 marks]

Consider a 4 bit block cipher, called *ABC*, that uses 2-bit keys. The ciphertext for all possible plaintexts and keys for cipher ABC are given below. To increase the strength of ABC against brute-force attack, I will apply the algorithm twice using a 4-bit key, K, which is two independent keys from ABC. The resulting cipher is *Double-ABC*. I have chosen a key and sent multiple ciphertexts to my friend. You are an attacker that has discovered two pairs of (plaintext, ciphertext): (0111,1101) and (1101,0100). Use a meet-in-the-middle attack to determine the most likely key I used. Show the steps.

Plaintext	00	01	10	11		Plaintext	00	01	10	11
0000	0001	0101	1000	0111		1000	1000	1011	0101	1000
0001	1101	0111	1101	0101		1001	1100	0000	0010	0110
0010	0000	0110	0111	1010		1010	1010	0010	0000	0100
0011	0101	1101	1111	0011		1011	1011	1100	1001	1001
0100	0111	1000	1100	1101		1100	0110	0011	1010	1100
0101	1001	1111	1011	0001		1101	1111	1110	0100	0000
0110	0011	1001	0001	1011		1110	0100	0100	0011	0010
0111	1110	0001	0110	1111		1111	0010	1010	1110	1110