CSS322 – Quiz 5

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

Question 1 [3 marks]

Using block cipher *ABC* (the single version shown in the table), the plaintext 00101010 is encrypted using key 01 with CBC and IV 0111 (encryption with CBC is shown in Figure 1 (left)). What is the ciphertext? [3 marks]

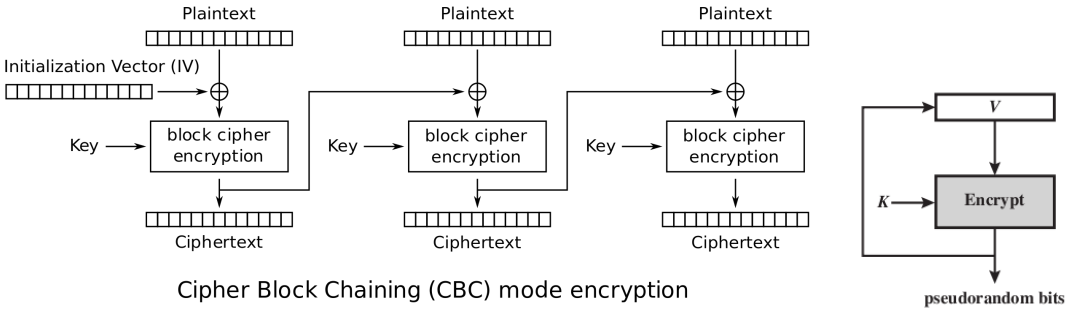

Figure 1: Left: CBC encryption; Right: Using block cipher for PRNG

Question 2 [3 marks]

A block cipher can be used as a PRNG. One way is to select a key and initial value (together they are the seed), encrypt using the block cipher, and the output ciphertext is then fed as the next input to the block cipher (as shown in Figure 1 (right)). The ciphertext is the pseudorandom bits.

(a) What is the maximum possible period, in bits, of a pseudorandom stream generated when using an ideal 12-bit block cipher? [1 mark]

(b) What is a disadvantage of using a real block cipher, like AES or Triple-DES, as a PRNG (as opposed to using a dedicated PRNG algorithm like Blum Blum Shub or LCG, or even a stream cipher like RC4)? [1 mark]

(c) You are given a sequence of 1 million bits. As one simple measure of "randomness" you would expect about half the bits to be 0's and half to be 1's. Explain another way you could measure the "randomness" of this sequence. [1 mark]

Question 3 [4 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): (0000,0101) and (1111,0011). 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