University of Chittagong

Department of Computer Science and Engineering

7th Semester B.Sc. (Engg.) Examination-2020

Course Code: CSE-717 **Course Title: Information Security**

Total marks: 52.5 Marks Time: 4.00 hours

[Answer any ***three*** questions from each of the ***Group-A*** and ***Group-B***. A separate answer script must be used for Group-A and Group-B. Figures in the right-hand margin indicate full marks.]

Group-A

1. a) Using the following Playfair matrix: 4.75

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message: "*Must see you over CU playground. Coming now.*"

b) Using the Vigenère cipher, encrypt the word "*explanation*" using the key *cse*. 4

2. a) Solve the following congruences using the Chinese remainder theorem. 4.75

$$X \equiv 1 \bmod 3$$
$$X \equiv 1 \bmod 4$$
$$X \equiv 1 \bmod 5$$
$$X \equiv 1 \bmod 7$$

b) (i) Calculating $3^{11} \bmod 17 = X$ is easy, but calculating discrete logarithm $11 = 3^x \bmod 17$ is very difficult. Explain the above statement. In this aspect, what do you understand by the cyclic group? 2+2

(ii) Find out the distinct remainders for b^x mod 7.

3. a) Using the extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1769. 4.75

b) (i) Using Fermat's theorem, find 3^{202} mod 11. 2+2

(ii) Use Euler's theorem to find a number a between 0 and 9 such that a is congruent to 7^{1000} modulo 10.

4. a) (i) The following questions are related to data encryption standards: 2+2.75
If initial permutation (IP) is there, why do we need IP^{-1}? What is the S_1-box representation of 37? [The value given at row 3 and col 2 at S_1 table is 08]

(ii) Draw the details of the F-function in DES.

b) (i) For DES, explain the following equation. 2+2

At the end of the decryption process

$$IP^{-1}(R^d_{16}\ ,\ L^d_{16}) = IP^{-1}(L_0\ , R_0) = IP^{-1}(IP(x)) = x$$

Where x is the plain text that was the input to the DES encryption.

(ii) How the concept of the finite field are used in cryptography?

Group-B

5. a) (i) Draw a block diagram of 3-DES. Write down a simple equation to represent DES encryption for 3-DES. 2.75+2

(ii) What do understand by the avalanche effect? Write down two families of attacks in DES.

b) Draw the classical Feistel cipher structure for the symmetric block encryption algorithm. 3

c) What are the differences between a block cipher and a stream cipher? 1

6. a) Perform encryption and decryption using the RSA algorithm, for $p = 3$, $q = 11$, $e = 7$, and $M = 2$. (The value of n and cipher-text must be explicitly shown.) 4.75

b) (i) In an RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? 2+2

(ii) In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

7. a) Draw the generic model of the digital signature process. 4.75

b) Find out the 8-bit word related to $x^5 + x^2 + x$. 2

c) How would you test a number $n = 29$ is a prime or not using the Miller-Rabin algorithm? Show the steps clearly. 2

8. a) Determine the benefits of IPSec. What are the differences between transport mode and tunnel mode? 2.25

b) What are the general services defined by RFC4301 for IPSec? 2.25

c) Discuss the application areas of IPSec. Compare session state and connection state. 2.25

d) Explain the architecture of IPSec. 2