C8-R4: INFORMATION SECURITY

NOTE:

1. **Answer question 1 and any FOUR from questions 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time: 3 Hours **Total Marks: 100**

1.

a) For user workstations in a typical business environment, list potential locations for confidentiality attacks.

b) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? What is limited error propagation in CBC?

c) What requirement should a digital signature scheme satisfy?

d) What is a certificate chain? How is an X.509 certificate revoked?

e) Explain SSH transport layer protocol packet exchange.

f) What is birthday attack? How it is used in cryptography.

g) Describe authenticated encryption.

(7x4)

2.

a) The Play fair cipher was the first practical digraph substitution cipher. Encrypt the string “this is a secret message” using play fair cipher. The keyword is “awkadard”. Why cryptanalysis of play fair cipher is much more difficult than normal simple substitution cipher.

b) What are unconditionally secure and computationally secure encryption scheme?

c) List important design considerations for a stream cipher. What primitive operations are used in RC5?

(6+6+6)

3.

a) List out the strength and weaknesses of DES. What is weak key in DES? Give example of it.

b) What is pseudorandom number generator? Let $n = p \cdot q = 7 \cdot 19 = 133$ and $s = 100$ and explain the working of Blum Blum Shub Generator by generating first four random numbers.

c) Which parameter and design choices determine the actual algorithm of a Fiestel cipher?

(6+7+5)

4.

a) Write the detailed comparison of threats on Web.

b) Define Euclidean algorithm using an example.

c) What is Kerberos? What problem was Kerberos designed to address? In Kerberos, when Bob receives a Ticket from Alice, how does he know it is genuine?

(8+4+6)

5.

a) Identify the attacks in Context of Communication across the network and show how basic usage of MD for dealing with any one of attack.

b) What is Diffie-Hellman key exchange algorithm? How does man-in-the-middle attack break the security of it? How this attack can be prevented?

(9+9)

6.

a) Consider an ElGamal scheme with a common prime q= 71 and a primitive root α = 7.

i) If B has public key Y_B = 3 and A choose the random integer k = 2, what is the ciphertext of M = 30?

ii) If A now chooses a different value of k so that the encoding of M = 30 is C = (59, C_2), what is the integer C_2?

b) What are the minimum and maximum bits require for the padding in SHA-512. "SHA is collision resistant algorithm" Justify the statement.

c) What is the purpose of HTTPS? List and briefly define the parameters that define an SSL session connection.

(6+6+6)

7.

a) Explain the importance of prime numbers in the field of cryptography.

b) Prove the correctness of RSA algorithm using Euler's theorem.

c) What is the difference between statistical randomness and unpredictability?

(6+6+6)