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) The encryption key in a transposition cipher is (3, 1, 5, 2, 6, 4). Find the decryption key.

b) Find the inverse of following matrices in mod 26:

8	5	10
21	8	21
21	12	8

c) List and explain the crypto analysis attack.

d) Calculate 79^{23} mod 53 using fast exponential algorithm.

e) Using the Vigenère cipher, encrypt the word “We are students” using the key “leg”.

f) List and explain the parameters and design choices determine the actual algorithm of a Feistel cipher.

g) Describe authenticated encryption.

(7x4)

2.

a) Generate play fair cipher table with the key “Hello”. How many possible keys does the Play fair cipher have in general?

b) List the Requirements for a Cryptographic Hash Function.

(9+9)

3.

a) What is the difference between modular arithmetic and normal arithmetic? Briefly define the following:

i) Group
ii) Ring
iii) Field

b) Given p = 31, q = 23, e = 223 and m (plain text) = 439. Demonstrate the working of RSA algorithm (encryption and decryption) using given values. (To calculate exponential values use appropriate algorithm)

(9+9)

4.

a) What is digital signature? How digital signature differs from conventional signature? Explain how RSA and cryptography hash function can be used for digital signature.

b) List out the problem arises while distributing symmetric key and asymmetric key. Explain how X.509 has standardized the asymmetric key distribution.

(9+9)

5.

a) What is key distribution center? Explain why Kerberos requires authentication server and ticket granting server.

b) Explain the process of extracting information from key rings and message generation at sender site in PGP. What is key legitimacy in PGP?

(9+9)

6.

a) What is Cipher Feedback (CFB) mode? Explain the security issues and error propagation in CFB.

b) What is Merkel-Damgard (MD) scheme? Explain the Security characteristics associated with it.

(9+9)

7.

a) Write the steps for initialization in RC4. Differentiate between RC4 and CAST.

b) Define the Diffie-Hellman protocol and its purpose. Explain Man-in-the-Middle attack.

(9+9)