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) How many permutations are used in a DES cipher algorithm and round key generation? Why does the DES function need expansion?

b) What is the Avalanche Effect? What is the relation between the Avalanche Effect and diffusion and confusion?

c) Describe Block Cipher Modes of Operation.

d) Explain specific authentication services defined in X.800.

e) List and explain types of Attacks on Encrypted Messages.

f) "The substitution cipher can model as a permutation if input and output can be decoded and encoded respectively." Justify the statement.

g) In AES 8th round key EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F is given. Find the first 4 bytes (first column) of the 9th round key. (Use Rcon=1B000000)

(7x4)

2.

a) Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

b) Explain the differential cryptanalysis and linear cryptanalysis.

c) Use a Hill cipher to encipher the message "SAKNOXAOJX". Use the following encryption key and find the decryption output (Z_{26}*).

$$K = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$$

(6+5+7)

3.

a) Consider ELGamal public key (e1 = 2 and e2 = 8) to send two messages P = 17 and P' = 37 using the same random integer r = 9. Intruder intercepts the cipher text and somehow he finds the value of P = 17. Show how he can use a known-plaintext attack to find the value of P'.

b) What are Message Detection Code (MDC) and Message Authentication Code (MAC)? Explain how Hash-based message authentication code is useful.

c) Use brute-force attack to decipher the following message. It is an affine cipher (additive cipher followed by multiplicative cipher) and the plaintext "ab" is enciphered to "GL".

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

(6+6+6)

4.

a) List and explain the contents of an X.509 certificate. Define certificate revocation process.

b) List the two criteria used to validate that a sequence of numbers is random. Given n=192649 (383 * 503) and the seed s = 101355 generate initial three random bits using Blum, Blum, Shub (BBS) generator.

c) Miller and Rabin Algorithm is typically used to test a large number for primality. Using Miller-Rabin Algorithm check number 581 is prime or not.

(6+8+4)

5.

a) What is Blind Signature? Explain the Blind Signature based on the RSA scheme.

b) Define Diffie-Hellman protocol and its purpose. In the Diffie-Hellman protocol, g = 7, p = 23, x = 3 and y = 5.

i) What is the value of the symmetric key?

ii) What is the value of R1 and R2??

c) Given N = 187, e = 13 of RSA find the plain text for cipher text 035 # 083 # 001.

(5+6+7)

6.

a) What is Fast Modular Exponentiation Algorithm? Calculate 13^{29} mod 23 using the algorithm.

b) Write the detailed comparison of MD5 and SHA1. Explain how initial constants (A-H) and round constants are generated in SHA 512? What is the padding for SHA-512 if the length of the message is 896?

c) What are the cryptographic Message Syntaxes in S/MIME? By taking suitable example explain Radix-64 conversion.

(6+6+6)

7.

a) Explain Transport Mode and Tunnel Mode in IPSec. List and describe the fields of Authentication Header protocol.

b) What is the process in the calculation of master secrete from pre-master secrete in SSL? Define Sessions and Connections.

c) What is PGP? Explain the format of private key ring table and public key ring table in PGP. List the inputs needed to extract information at the sender side in PGP.

(6+6+6)