C8-R4: INFORMATION SECURITY

«QP_SRLNO»

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) Differentiate between Symmetric and Asymmetric encryption.

b) Differentiate cryptanalysis, cryptography and cryptology.

c) What are weak keys in Data Encryption Standard (DES)? Give examples of weak keys.

d) What are the drawbacks of Output Feedback mode (OFB)? Why Cipher Feedback Mode (CFB) and Cipher Block Chaining are better than OFB?

e) Differentiate between Authentication and Authorization with example.

f) Let u = 19500 and v = 11143. Use the Euclidean Algorithm to compute w = gcd(u, v). Carry out the computation so that you are able to find R and S such that w = Ru + Sv.

g) Compute Euler's Totient function, φ(1716).

(7x4)

2.

a) Alice uses the RSA Cryptosystem to receive messages from Bob. She chooses – p=13, q=23 and her public exponent e=35, Alice published the product n=pq=299 and e=35. Check whether e=35 is a valid exponent for the RSA algorithm ? Compute d , the private exponent of Alice. Bob wants to send to Alice the (encrypted) plaintext P=15. What does he send to Alice? Verify she can decrypt this message.

b) What are different versions of Fermat Little Theorem? Discuss various applications of Fermat Little Theorem with examples.

(9+9)

3.

a) Explain the key scheduling, encryption and decryption processes of Data Encryption Standard (DES) algorithm with the help of block diagram. What are the consequences of weak and semi weak keys in DES algorithm?

b) Explain the Diffie-Hellman key exchange algorithm.

(12+6)

4.

a) Solve $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$ using Chinese Remainder Theorem. Find first 3 possible solutions of x.

b) Write pseudo-code and draw block diagram of ANSI X9.17 Pseudorandom Number Generator (PRNG). Name some attacks that are possible in ANSI X9.17 PRNG.

(9+9)

5.

a) Explain, how Preimage resistance, Second preimage resistance and Collision resistance properties are used to measure the strength of any hash function. Draw a block diagram for explaining the working of hash function in any cryptosystem.

b) Define MAC. What are the security requirements of MAC?

c) Differentiate between deterministic and probabilistic primarily testing algorithms. List some algorithm in each category also.

(6+6+6)

6.

a) What is the purpose of Digital Signature Schemes? Name algorithms used in any digital signature schemes. Draw block diagram and discuss the properties of digital signature schemes.

b) What is Fast Exponentiation? Which cryptography algorithm requires fast exponentiation? Write steps of one fast exponentiation algorithm.

(9+9)

7. Explain the following:

a) Advanced Encryption Standard (AES)

b) Cryptography Primitives

c) Modular Arithmetic in Group, Ring and Field.

(6+6+6)