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) Find 8^{-1} mod 17 using Fermat Little Theorem.

b) Explain Meet-in-the-middle attack in Data Encryption Standard (DES).

c) What is Shift Cipher? Explain with an example.

d) What is a group in modular arithmetic? Briefly discuss the properties of a group.

e) Discuss the role of Key Distribution Centre.

f) Discuss the Authentication Encryption (AE) process in cryptography with the help of block diagram.

g) What is second preimage resistance?

(7x4)

2.

a) Let p (prime number)=23, g (generator or primitive element)=5, a (Alice private key) =6 and b (Bob's private key) =15. Compute the session key between Alice and Bob using Diffie-Hellman key exchange protocol.

b) Can we solve $8x \equiv 7 \bmod 18$ using Chinese remainder theorem? If yes, find the possible solutions. If no, does any solution exist?

(12+6)

3.

a) Explain the key scheduling, encryption and decryption processes of Advanced Encryption Standard (AES) algorithm with the help of block diagram.

b) What are the roles of Digital Signature Schemes? Explain RSA digital signature scheme.

(12+6)

4.

a) What is Birthday Paradox? How many people are required in a room so that the probability of at least two of them sharing the same birthday should be greater than ½?

b) What are the applications of Pseudorandom Number Generators (PRNGs)? Is Blum-Blum-Shub (BBS) a binary PRNG Generator? If yes, explain with an example.

(9+9)

5.

a) What is a hash function? Discuss the digest size, block size, word size and number of rounds used in SHA-2 algorithm. Draw the Merkle-Damgard block diagram of SHA-2 also.

b) Draw the block diagram of Message Authentication Code (MAC) for the process of message authentication at source and destination sides. What security properties are required for making MAC stronger?

(12+6)

6.

a) List various cryptography primitives. Explain the roles of each primitive in cryptography.

b) Write short nodes on following modes of operations:

i) Electronic Codebook (ECB)
ii) Cipher Block Chaining (CBC)
iii) Cipher Feedback Mode (CFB)
iv) Output Feedback (OFB)
v) Counter Mode (CTR)

(6+12)

7.

a) Define multiple encryptions. Why multiple encryptions are required in DES. Discuss with example.

b) Is pseudorandom number generator (PRNG) required in stream cipher? Explain the need of PRNG using RC4 stream cipher.

c) What is perfect security? How can an encryption algorithm become perfectly secure?

(6+9+3)