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) What are the basic objectives of Information Security ?
(b) What is the difference between block and stream ciphers ?
(c) Define groups, fields and rings.
(d) Explain the advantages of Asymmetric Cryptography.
(e) What is MAC ? How does it differ from standard encryption ?
(f) How pseudorandom number generation is done using hash functions ?
(g) What is Counter operation mode ?

(7×4)

2. (a) Explain Fermat's theorem.
(b) Factor number 7373 using Fermat's factorization.
(c) How does man-in the-middle attack affect Deffie Hellman algorithm ?

(6+6+6)

3. (a) Discuss the various attacks, and their effects in RSA technique.
(b) What is the collision of a Hash value ? Describe the properties of a Hash and Hash function.

(10+8)

4. (a) Describe the logic of SHA algorithm.
(b) Prove that every finite field has a prime characteristic.

(10+8)

5. (a) Explain the EIGamal cryptosystem.
(b) What is entity based authentication ? Discuss its various types.

(8+10)

6. (a) Explain Naïve's algorithm. Find the primality test for the number 47 using Nave's algorithm.
(b) How does RC4 stream cipher works ?

(8+10)

7. (a) Differentiate between Encryption and Digital Signature. Explain about Digital Signature standards.
(b) What are the different types of attacks, a password can suffer ?

(8+10)