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 is a Shift Cipher? Explain how encryption and decryption can be done using shift cipher with an example.

b) Write and explain in brief on various characteristics of Advanced Symmetric Block Ciphers.

c) Write atleast FOUR distinct differences between DES and Triple-DES on various factors.

d) What is a Pseudo-random number generator? Explain in brief on various applications of it in cryptography.

e) What is Birthday Attack? Explain in brief with an example?

f) What is a key management in Cryptosystem? Write various challenges of key management.

g) What is Digital signature? Explain in brief with help of a diagram showing how a digital signature is applied and then verified.

(7x4)

2.

a) What is information security? Explain the role of Cryptography in ensuring security services like Confidentiality, Authentication, Integrity and Nonrepudiation with one example each.

b) Write and explain in brief on the key features of a Secure Electronic Transaction (SET) that are incorporated and also write names of cryptographic techniques/algorithms used in each feature.

(12+6)

3.

a) Explain ECB, CBC, CFB and OFB block cipher modes of operations with one example each along with their merits and limitations.

b) Write merits and limitations of DES and triple-DES.

c) Explain in brief on perfect security.

(12+3+3)

4.

a) Explain on Chinese Remainder theorem and its various application areas.

b) What is ANSI X9.17? Explain with an example, how key management can be done using ANSI X9.17.

(9+9)

5.

a) What are the four main properties of an ideal cryptographic hash function? Explain how hash functions used in Digital Signatures and Message Authentication Codes (MACs) as part of information security applications.

b) 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.

c) Compare SHA-1 with MD5.

(9+6+3)

6.

a) Explain in detail the Diffie-Hellman Key Exchange Algorithm with an example.

b) Explain on the important aspects (needed to work and security) of conventional and public-key encryption.

c) Compare RSA, DES and AES algorithms on various key factors such as key-length, block-size, scalability, security and inherent vulnerabilities.

(9+4+5)

7. Write short notes on:

a) Multiple Encryptions

b) Fermat's theorem in Public-key cryptography with an example

c) Finite Field Arithmetic

(6+6+6)