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) Define Cryptanalysis, Cryptanalyst, Cryptology and Cryptosystem?
b) Differentiate between an unconditionally secure cipher and a computationally secure cipher?
c) List and briefly define categories of Cyber security services.
d) Explain any substitution techniques for cryptography.
e) List and briefly define categories of Cyber security mechanisms.
f) Why is SSL important?
g) Mention some of the properties of Digital Signatures?

(7x4)

2.

a) Discuss RSA algorithm in detail.
b) Explain the Diffie-Hellmen Key exchange algorithm.
c) What is man in the middle attack and meet in the middle attack on double encryption?

(7+7+4)

3.

a) What is the significance of hash functions w.r.t cryptography?
b) What is Message Authentication Code (MAC)? Explain in brief.

(9+9)

4.

a) Explain SNMP Protocol in detail.
b) What are web security threats? Give countermeasures of web security threats. What is difference between HTTP and HTTPS protocol?

(9+9)

5.

a) Explain PGP for e-mail security.
b) Describe S/MIME.

(9+9)

6.

a) What is IPSec Protocol? Explain in detail with operation mode and its application. Draw frame format of IPSec also.
b) What is firewall? Explain different types of firewall.

(9+9)

7. Differentiate between **any three** of the following:

a) Direct Digital Signatures and Arbitrated Digital Signatures
b) Diffusion and Confusion
c) Block Cipher and Stream Cipher
d) Hash and Message Authentication Code (MAC)

(6+6+6)