BE CO (Rev)
Sem VII
SS.

QP Code :15608

(3 Hours) **[Total Marks : 100]**

N.B. : (1) Question 1 is compulsory.
(2) Attempt any four out of remaining six questions.
(3) Assumptions made should be clearly stated.
(4) Assume suitable data whenever required but justify the same.

1 (a) What is Multilateral Security? **5**
(b) Compare Stream and Block encryption algorithms. **5**
(c) Distinuish between attack, vulnerability and access control. **5**
(d) What is Buffer overflow and incomplete mediation in Software Security? **5**

2 The following questions are based on scenario in which encrypted data are passed between Alice and Bob using RSA algorithm. Alice's public key is { 17, 23} and Bob's public key is { 5, 23} Assume that no one knows the private keys but the original owners. **20**
(a) Encrypt the message M=7 using Bob's public key.
(b) What should Alice have to do to decrypt the message from Q-2 a?
(c) What would Bob have to do to decrypt the message from Q-2 a?
(d) What is Alice's private key?
(e) What is Bob's private key?

3. (a) Explain how threat precursors are used for Reconnaissance of network. **10**
(b) Upon reception of a digital certificate, how one can decide whether to trust that or not. **10**

4. (a) Explain Physiological and Behavioral biometric techniques with example. **10**
(b) Write short note on Access control List (ACL) and Capabilities. **10**

5. (a) What is a firewall? Expalin different types of firewall. **10**
(b) Explain various types of port scan. **10**

6. (a) What is spoofing? Explain ARP spoofing. **5**
(b) What is SQL Injection? Give Example. **5**
(c) Compare packet sniffing and packet spoofing. Expalin the session hijacking attack. **10**

7. Write short note on (Any **Two**) **20**
(a) Compare AES and DES
(b) Explain different Security Mechanisms.
(c) Various ways for Memory and Address Protection
