Q. P. Code: 37512

Time: 3hrs **Total Marks: 100**

Note: 1. Question No. 1 is compulsory
2. Attempt any four out of remaining six questions
3. Illustrate answers with sketches wherever required.

Q1. a. What is cryptography? Compare Symmetric Key Cryptography and Asymmetric Key Cryptography. **[10]**

b. Explain in detail PGP. **[10]**

Q2. a Explain Diffie Hellman key exchange protocol with a suitable example. How can this mechanism be foiled by an attacker? **[10]**

b. Explain different algorithm modes. **[10]**

Q3. a. Define network security? What are the services and mechanisms provided by network security? **[10]**

b. Give Comparison of MD5 and SHA-1. **[10]**

Q4. a. What is Ticket Lifetime? Distinguish between Renewable Tickets and Postdated Tickets. **[10]**

b. Explain mutual authentication and reflection attack with the help of diagram. Suggest two methods to fix it. **[10]**

Q5. a. Explain SSL Architecture. **[10]**

b. What are the various types of Malware? Explain in detail **[10]**

Q6. a. Explain working of Kerberos. How is Kerberos V5 different from V4? **[10]**

b. Explain the security mechanism used on the electronic transactions **[10]**

Q7. Write short notes on **any four** **[20]**

a. Certificate Revocation.
b. Digital Signature
c. IPSec
d. Biometrics
e. El-Gamal signatures

****