C 3269

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2007.

Sixth Semester

Information Technology

IT 1352 — CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2004)

Time : Three hours   Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Distinguish passive attack from active attack with reference to X.800.

2. Decrypt the mono alphabetic ciphertext Boob Vojwfstjuz.

3. How does Diffie - Hellman key exchange achieve security.

4. Mention any one technique of attacking RSA.

5. Write down the purpose of hash function along with a simple hash function.

6. List any two properties a digital signature should essentially have?

7. In three way authentication, what is the special feature, other than self identification.

8. Draw the header format for an ISAKMP message.

9. Who is a masquerader and who is a clandestine user?

10. What is meant by a trusted system?

PART B — (5 × 16 = 80 marks)

11. (a) With a neat structure of the classical Feistel network, indicate the parameters and design features which are essential for the exact realisation of the network.

Or

(b) In DES, the first 24 bits of each sub key come from the same subset of 28 bits of the initial key and that the second 24 bits of each sub key come from a disjoint subset of 28 bits of the initial key. Prove the above using a suitable method.

12. (a) Bring out the various steps involved in Diffie-Hellman key exchange.

Or

(b) Using Elliptic curve encryption/decryption scheme, key exchange between users A and B is accomplished. The cryptosystem parameters are, Ellyptic group of points $E_{11}(1,6)$ and point G on the elliptic curve is G = (2,7). B's secret key is $n_B=7$. Now when.

(i) A wishes to encrypt the message $P_m=(10,9)$ and chooses the random value K=3. Determine the ciphertext C_m.

(ii) How will B recover P_m from C_m.

(iii) Find out B's public key P_B.

13. (a) (i) Compare the features of SHA - 1 and MD - 5 algorithm.

(ii) Discuss about the objectives of HMAC and its security features.

Or

(b) (i) With DSS, because the value of 'K' is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. When using RSA signatures this does not happen. What is the practical implication of this difference?

(ii) Give the details of digital signature algorithm.

14. (a) (i) How is the encryption key generated from password in kerberos?

(ii) Illustrate the confidentiality service provided by PGP.

Or

(b) (i) Summarize the S/MIME capability.

(ii) What services are provided by IP sec?

15. (a) List down the various measures that may be used for Intrusion Detection.

Or

(b) (i) When system administrator trusts the internal users, what type of Fire wall is to be used. What are its limitations and how is to over come these difficulties?

(ii) How will you enhance the ability of a system to defend against intruders and malicious programs?