20008

2008 PUNJAB TECHANICAL UNIVERSITY

B.TECH COMPUTER SCIENCE AND ENGINEERING

IT CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 3 HOUR
MARK: 1000

PART A-(10*2=20 marks)

1. When an encryption algorithm is said to be computationally secure?

2. If a bit error occurs in plain text block P1, how far does the error propagate in CBS mode of DES and 8-bit CFB mode of DES?

3. In RC5-CBC-Pad mode, the cipher will be longer than the plaintext at most the size of a single RC5 block. Why?

4. When an integer a, less than n is said to be the primitive root of n?

5. Define the one way property to be possessed by any hash function.

6. What is the block size of MD5 and how many bits are produced as the message digest?

7. What is the role of Ticket Granting Server in inter realm operations of Kerberos?

8. Why the leading two octets of message digest are stored in PGP message along with the encrypted message digest?

9. How the passwords are stored in password file in UNIX operating system?

10. What is the role of bastion host?

PART B-(5*16=80 marks)

11. (a) (i) What are the criteria used while designing the DES algorithm?

(ii) In AES, how the encryption key is expanded to produce keys for the 10 rounds.

(OR)

(b) (i)Explain the generation of subkey and S Box from the given 32 bits key by Blowfish.

(ii) Describe the block modes of operations of DES with their advantages.

12. (a) (i) write the detailed description of RSA algorithm.

(ii) How discrete logarithm is evaluated for a number? What is the role of discrete logarithms in the Diffie-Hellman key exchange in exchanging the secret key among two users?

(OR)

(b)(i) State the requirements for the design of an Elliptic Curve Crypto system. Using that, explain how secret keys are exchanged and messaged are encrypted.

(ii) Describe any two applications of public key cryptosystem.

13. (a) (i) What are Digital Signature Algorithms and show how signing and verification is done using DSS.

(ii) Explain how birthday attack is done.

(OR)

(b) Describe the MD5 message digest algorithm with necessary block diagram.

14. (a)(i) Describe the authentication dialogue used by Kerberos for obtaining required services.

(ii) Explain the format of the X.509 certificate.

(OR)

(b) Describe how PGP provides confidentiality and authentication service for e-mail applications.

15. (a)(i) Explain any two approaches for intrusion detection.

(ii) Suggest any three password selection strategies and identify their advantage and disadvantages if any.

(OR)

(b) (i) What kind of attacks is possible on packet filtering firewalls and suggest appropriate counter measures.

(ii) Describe the familiar types of firewall configurations.