KUMARAGURU
college of technology
character is life

Register Number: ………………..

B.E / B.TECH DEGREE EXAMINATIONS: MAY 2015

(Regulation 2009)

Sixth Semester

ITY110: CRYPTOGRAPHY AND NETWORK SECURITY

(Common to CSE & IT)

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. In Cryptography, What is a Cipher?

   a) Algorithm for performing encryption and decryption b) Encrypted message

   c) Key d) Both (a) and (b)

2. DES algorithm uses a key of size

   a) 64 bits b) 128 bits

   c) 56 bits d) 48 bits

3. Which one of the following algorithm is not used in asymmetric-key cryptography?

   a) RSA algorithm b) Diffie Hellman algorithm

   c) Electronic Code Book algorithm d) Elliptic Curve algorithm

4. Cryptanalysis in RSA algorithm is used to

   a) To increase the speed b) To find some insecurity in the algorithm and scheme

   c) To encrypt the data d) To select the key

5. Cryptographic hash function takes an arbitrary block of data and returns

   a) Fixed Size Bit String b) Variable Size Bit String

   c) Both (a) and (b) d) 160 bit hash code

6. HMAC is

   a) Combination of Hash and MAC b) Hash code

   c) MAC code d) Message Digest

7. Which one of the following is a cryptographic protocol used to secure HTTP Connection?

a) Stream Control Transmission Protocol (SCTP)	b) Transport Layer Security (TLS)
c) Explicit Congestion Notification (ECN)	d) Resource Reservation Protocol (RRP)

8. Voice privacy in GSM cellular telephone protocol is provided by

a) A5/2 cipher	b) b5/4 cipher
c) b5/6 cipher	d) b5/8 cipher

9. A Firewall is installed at the point where the secure internal network and the untrusted external network meet which is also known as

a) Meeting point	b) Firewall point
c) Choke point	d) Security point

10. The _____________ is used to provide Integrity Check, Authentication and Encryption to IP Datagram

a) SSL	b) ESP
c) TLS	d) PSL

PART B (10 x 2 = 20 Marks)

11. What are the two basic functions used in encryption algorithms?
12. How many keys are required for two people to communicate via a cipher?
13. Show that 3 is a primitive root of 7.
14. Find the GCD of 2740 and 1760 using Euclidean algorithm.
15. Compare Message Authentication Code (MAC) and Hash Function.
16. Define one way property, weak collision resistance and strong collision resistance of Hash Function.
17. Summarize the services provided by S-MIME.
18. Compare and contrast Kerberos version 4 and Kerberos version 5.
19. Outline the common techniques used to protect a password file.
20. Classify the different viruses and their corresponding Anti Virus Software.

PART C (5 x 14 = 70 Marks)

21. a) (i) Draw the general structure of DES and explain the encryption, decryption process. (10)

(ii) Infer the strengths and weakness of the DES Algorithm. (4)

(OR)

b) Discuss the block cipher modes of operation in detail with relevant diagrams.

22. a) Explain how encryption and decryption are done in RSA cryptosystems with example.

(OR)

b) (i) Users A and B apply the Diffie Hellman key exchange technique with a common prime q=11 and a primitive root α = 7. If user A has private key $X_A = 3$ and user B has private key $X_B = 6$, Find both A and B's Public key Y_A and Y_B respectively. (8)

(ii) Deduct the shared secret key by applying the Diffie Hellman key exchange algorithm. (6)

23. a) Describe SHA – 1 logic to produce message digest with a neat sketch.

(OR)

b) (i) What is a Digital Signature? Acquaint the concept of Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA) (10)

(ii) Analyze the security of Hash Functions and MAC's. (4)

24. a) Elaborate how does PGP provide confidentiality and Authentication for E-mail and file storage applications? Draw the block diagram and explain its components.

(OR)

b) (i) Bring out the importance of security associations in IP. (6)

(ii) Mention the SSL specific protocol – Handshake action in detail. (8)

25. a) (i) Inspect the positive and negative effects of a firewall. (4)

(ii) Generalize the design principles of different types of firewall. (10)

(OR)

b) Elaborate the different types of host based intrusion detection systems. List any two IDS software available.

****