Register Number: ……………………..

B.E / B.TECH DEGREE EXAMINATIONS: APRIL/MAY 2014

(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. Which of the following is a passive attack?
   a) Traffic Analysis b) Masquerade
   c) Replay d) Denial of Service
2. Use the Caesar cipher with key=4 to decrypt the message "QIIX QI".
   a) NEAR TO b) MEET TO
   c) MEET ME d) MAIL ME
3. For the prime number p, What is the value of Φ(p)?
   a) P+1 b) p-1
   c) p d) p^2
4. What is the value of 11^4 mod 187?
   a) 57 b) 59
   c) 55 d) 53
5. An opponent can replay a time stamped message within the valid time window is called __________.
   a) Simple Replay b) Repetition that can be logged
   c) Birthday attack d) Backward replay
6. Insertion of messages into the network from a fraudulent source id called is ______________.
   a) Traffic analysis b) Masquerade
   c) Disclosure d) Source repudiation
7. Which of the following is the open source software for e-mail security?
   a) Kerberos b) X.509
   c) MIME d) d. PGP
8. Which of the following is the framework for authentication service?
   a) X.509 b) X.506
   c) SET d) SSL

9. The two techniques that are used to protect the password file are_____________ .
   a) One way function ,Access control b) Authenticataion,Access control
   c) One way function ,DoS d) Authentication,DoS
10. Which of the following virus is explicitly designed to hide itself from detection by antivirus software?
    a) Stealth virus b) Polymorphic virus
    c) Boot Sector virus d) Parasitic virus

PART B (10 x 2 = 20 Marks)

11. What is the difference between link encryption and end-to-end encryption?
12. Using the Vigenere cipher, encrypt the word "explanation" using the key leg.
13. State the difference between conventional encryption and public-key encryption.
14. On the elliptic curve over real numbers $Y^2=x^3-36x$,let P=(-3.5,9.5) and Q=(-2.5,8.5).Find P+Q.
15. What characteristics are needed for a secured hash function?
16. What is the difference between strong and weak collision resistance?
17. How does IPSec offer the authentication and confidentiality service?
18. List two disputes that can arise in the context of message authentication.
19. What is a honeypot?
20. List three design goals for a firewall.

PART C (5 x 14 = 70 Marks)

21. a) (i) Summarize the salient features of various classical Encryption techniques. (8)

    (ii) Make use of Hill cipher to encipher the message "We live in an insecure world". Use the (6)

    $$k=\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix}$$

    Show your calculations and the result.

    (OR)

    b) (i) Discuss the working of DES algorithm. Also mention the strengths and weaknesses of DES algorithm. (8)

    (ii) Construct a Playfair matrix with the key occurrence. Using that matrix encrypt the message "Must see you over Cadogan West." (6)

22. a) (i) Explain briefly the RSA algorithm. Perform encryption and decryption using RSA algorithm for the following : (8)

    P=11,q=13,e=11, M=7

    (ii) How do Elliptic curves take part in Encryption and Decryption process? (6)

(OR)

b) (i) Explain briefly the Diffie-Hellman key exchange. Suppose users A and B use this key exchange technique with a common prime $q=71$ and a primitive root $\alpha=7$, compute the following: (10)

i) If user A has private key $X_A=5$, What is A’s public key *YA?*

ii) If user B has private key $X_B=12$, What is B’s public key *YB* ?

iii) What is the shared secret key?

(ii) Build an efficient procedure for picking a prime number. (4)

23. a) (i) Discuss how SHA-512 generates message digest with a neat sketch. (8)

(ii) List the properties of a Hash function. (6)

(OR)

b) (i) Explain the signing and verification process of DSS with a neat diagram. (8)

(ii) List the design objectives for HMAC. Illustrate the overall operation of HMAC. (6)

24. a) How does PGP provide confidentiality and authentication service for e-mail and storage applications? Draw the block diagram and explain its components. (14)

(OR)

b) (i) Discuss in detail the working of Kerberos protocol. (10)

(ii) How is an X.509 certificate revoked? (4)

25. a) (i) What is a Virus? What are its types? Explain. (8)

(ii) What is a firewall and what are its limitations? Why do corporate houses impleme more than one firewall for security? (6)

(OR)

b) (i) Explain the various types of Intrusion Detection Systems. (8)

(ii) Summarize the various password selection strategies. (6)

****