Register Number: ……..

B.E/B.TECH., DEGREE EXAMINATIONS: MAY/JUNE 2013

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. Denial of transmission and reception is termed as
   a) disclosure b) repudiation
   c) masquerade d) traffic analysis
2. Play fair cipher is known as
   a) multiple cipher alphabets b) multiple letter encryption cipher
   c) ceasar cipher d) hill cipher
3. _____ is a technique used to provide steganography.
   a) auto key system b) one time pad
   c) character marking d) substitution
4. What is the value of ϕ(18)?
   a) 4 b) 6
   c) 2 d) 3
5. What is the use of Nounces?
   a) encryption b) to avoid replay attack
   c) decryption d) key exchange
6. Expand ESP _____ and the function of ESP _____
   a) Encapsulating security payload, authentication b) Encapsulating security payload , confidentiality
   c) encryption security protocol , authentication d) Encryption security protocol, confidentiality
7. _____ attaches itself to a program and propagates copies of itself to other programs
   a) Flooders b) logic bomb
   c) virus d) keyloggers

8. What is TGS?

a) Travel grant service
b) Ticket grant server
c) Tree grant service
d) Ticket great service

9. In which service the dual signature is used to provide security?

a) Email security
b) secure electronic transactions
c) IP security
d) Cryptography

10. What types of information might be derived from a traffic analysis attack?

a) Identities of partners
b) Message Pattern
c) Message Frequency
d) All the above

PART B (10 x 2 = 20 Marks)

11. Decrypt the following text using rail fence technique.
ioaoenonrtncogfmithly
12. Define the brute force attack.
13. Define diffusion and confusion.
14. What is avalanche effect?
15. Write the Fermat's and Euler's throrem.
16. What is Φ(35)?
17. Compare SHA-1 and MD5 algorithm
18. What are the contents of X.509 certificate format?
19. Draw the header format for an ISAKMP messages.
20. What is meant by polymorphic viruses?

PART C (5 x 14 = 70 Marks)

21. a) (i) Discuss any TWO substitution cipher encryption methods and list their merits and demerits. (10)

(ii) Explain about traffic confidentiality. (4)

(OR)

b) Give the detailed explanation about DES encryption algorithm along with single round function.

22. a) (i) Users A and B use the Diffie-Hellman key exchange technique, a common prime p=71 and a primitive root g =7 are used. If user A has private key XA=5, what is A's public key YA? If user B has private key XB =12, what is B's public key YB? What is the shared secret key? (10)

(ii) Write short notes of ECC. (4)

(OR)

b) Discuss in detail the different ways of distribution of public keys.

23. a) (i) Explain the processing of a message to generate authenticator using SHA-1.

(OR)

b) Explain about Digital Signature Standard algorithm and DSS signing and verifying.

24. a) (i) Describe the authentication dialogue used by Kerberos for obtaining services from other realm. (8)

(ii) Why does PGP maintain key rings with every user? Explain how the messages are generated and received by PGP using key rings. (6)

(OR)

b) Explain the overview and features of secure electronic transaction, how the dual signature is constructed and purchase request handling in detail.

25. a) Explain about password protection mechanisms and password selection strategies in detail with an example.

(OR)

b) (i) Describe the three common types of firewalls. (8)

(ii) Explain the nature of viruses and types of Viruses in detail. (6)

****