KUMARAGURU
college of technology
character is life

Register Number:……..

**B.E/B.TECH DEGREE EXAMINATIONS: NOV/DEC 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. The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained. This type of attack is _____.
   a) Cryptanalysis b) Virus
   c) Brute-force attack d) Worm
2. The minimum key size for AES is _____ bits.
   a) 128 b) 64
   c) 256 d) 32
3. The first published public-key algorithm was
   a) Elliptic Curve Cryptography b) Diffie-Hellman Key Exchange
   c) MAC d) RSA
4. The RSA is
   a) Encryption algorithm b) Authentication algorithm
   c) Key exchange algorithm d) All the above
5. The maximum message size in SHA-1 is
   a) $2^{61} - 1$ bits b) $2^{63} - 1$ bits
   c) $2^{64} - 1$ bits d) $2^{62} - 1$ bits
6. An opponent can replay a time stamped message within the valid time window. This replay attack is named as _____.
   a) Simple replay b) Repetition that can be logged
   c) Repetition that can't be detected d) Backward replay without modification

7. Kerberos relies exclusively on

a) Symmetric encryption b) Private key encryption

c) Asymmetric key encryption d) Public key encryption

8. PGP provides a _____ service that is used for e-mail.

a) Confidentiality b) authentication

c) Confidentiality and authentication d) integrity

9. _____ are systems that divert an attacker from accessing critical systems.

a) Worm b) Trojan horse

c) Honeypots d) Password

10. SOCKS package is an example for

a) Packet filter b) Application-level gateway

c) Circuit-level gateway d) Bastion Host

**PART B (10 x 2 = 20 Marks)**

11. What is steganography?
12. List the types of information that might be derived from a traffic analysis attack.
13. What is Euler's theorem?
14. What is traffic padding? What is its purpose?
15. In what ways can a hash value be secured so as to provide message authentication?
16. What are the properties a digital signature should have?
17. What is a realm, in the context of Kerberos?
18. List any two limitations of SMTP.
19. Name the metrics that are useful for profile-based intrusion detection.
20. Differentiate a virus from a worm.

**PART C (5 x 14 = 70 Marks)**

21. a) (i) Illustrate Playfair Cipher with an example. (7)

(ii) Show that DES decryption is, in fact the inverse of DES encryption. (7)

**(OR)**

b) (i) How will you perform triple encryption using two keys? (4)

(ii) How does a known-plaintext attack act upon Triple DES? Illustrate with neat diagrams. (10)

22. a) (i) Give the RSA algorithm. (7)

(ii) Perform encryption and decryption using the RSA algorithm for the following: (7)
P=5, q=11, e=3, M=9

**(OR)**

b) Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root $\alpha$ =2.

(i) Show that 2 is a primitive root of 11.

(ii) If user A has public key $Y_A = 9$, what is A's private key $X_A$?

(iii) If user B has public key $Y_B = 3$, what is the shared secret key K?

23. a) (i) Investigate about the behaviour of Brute-force attack on Hash functions and MACs. (7)

(ii) Enumerate the authentication requirements. (7)

**(OR)**

b) (i) Illustrate how can a hash code be used to provide authentication with neat sketches. (10)

(ii) What do you mean by suppress-replay attack? Tell the way to counter it. (4)

24. a) (i) Draw the X.509 format of a public-key certificate. (4)

(ii) Write the significance of each element in the above certificate. (10)

**(OR)**

b) Illustrate the principle behind the transmission and reception of PGP messages with neat diagram.

25. a) (i) Express and expand the four techniques used to eliminate the guessable passwords. (7)

(ii) Illustrate the significance of compression used in virus. (7)

**(OR)**

b) (i) Enumerate the capabilities and limitations of a firewall. (7)

(ii) Explain the reference monitor concept of trusted systems with a neat sketch. (7)

**********