KUMARAGURU
college of technology
character is life

Register Number: …….

B.E DEGREE EXAMINATIONS: APRIL/MAY 2016

(Regulation 2013)

Sixth Semester

COMPUTER SCIENCE AND ENGINEERING

U13CST602 : Cryptography and Network Security

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Denial of service comes under the category of
   a) Passive attack b) Active attack
   c) Traffic analysis d) Security Service
2. ……. exploits the characteristics of the algorithm to attempt to deduce a specific plaintext.
3. In asymmetric key cryptography ……..keys are required per communication party.
   a) 3 b) 4
   c) 2 d) 5
4. The discrete logarithm of b for the base a, mod p is expressed as ……..
5. The hash value of a message is encrypted with a user's private key to create
   a) Digital signature b) Message Authentication code
   c) Message digest d) Hash value
6. Message Authentication code is also known as …….
7. Requirements of the Kerberos does not require
   a) Scalable b) Transparent
   c) Efficient d) Reliable
8. Tunnel mode provides protection for ……
9. A Basic Service Set (BSS) is said to be Independent BSS when
   a) All stations are disconnected b) All stations are stationery
   c) All stations are mobile d) None of the above
10. Wireless Transport Layer Security (WTLS) provides authentication by the use of …….

PART B (10 x 2 = 20 Marks)

(Answer not more than 40 words)

11. How Masquerading is performed by an attacker?
12. Compare and contrast Cryptanalysis and Brute force attack.

13. State Fermat's Theorem.
14. Define Abelian group with an example.
15. Write down any four requirements of Message Authentication.
16. Draw the schematic diagram of Digital Signature Standard (DSS) approach.
17. Sketch the general structure of private-key ring.
18. Compare Statistical anomaly detection and Rule-based detection.
19. Differentiate between Secure connection and secure session.
20. How APs advertise its security policy in a wireless network during discovery phase?

PART C (5 x 14 = 70 Marks)
(Answer not more than 400 words)

Q.No. 21 is Compulsory

21. Explain handshake protocol action of Secure Socket Layer.

22. (a) (i) Draw and describe symmetric cipher model. (6)

(ii) Encrypt and decrypt "CRYPTOGRAPHY" using Hill Cipher with key $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$. (8)

(OR)

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

23. (a) (i) Compare the working principle of True Random Number Generator (TRNG) and Pseudo Random Number Generator (PRNG). (6)

(ii) Construct a Diffie Hellman scheme with a common prime 11 and a primitive root is 2. (8)

i) Show that 2 is a primitive root of 11.
ii) If user A has public key is 9 then what is A's private key.
iii) If user B has public key is 3 then what is B's private key.
iv) What is the shared secret key?

(OR)

(b) (i) Write down RSA algorithm for encryption and decryption. Explain with simple example. (7)

(ii) Find A, (7)

A=3mod7
A=3 mod 13
A=0 mod 12 by CRT method

24. (a) Calculate and verify the signature using the DSS algorithm. Let q=101, p=881, h=3, the private key is 61 and random number is also 61. Assume that H(m)=5000.

(OR)

(b) (i) What is meant by Message Digest? Give example ways of using hash function for message authentication. (6)

(ii) Describe in detail SHA-512 (8)

25. (a) (i) What is Kerberos? Explain how it provides authentication service (10)

(ii) Briefly write down the architecture of IPSEC (4)

(OR)

(b) Discuss Secure Electronic Transaction.

****