Register Number.....

**M.E. DEGREE EXAMINATIONS: OCTOBER / NOVEMBER -2008**

Third semester

**COMMUNICATION SYSTEMS**

**P07CME10 Communication Network Security**

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

**PART –A (20 x 1 = 20 Marks)**

1.The protection of data from unauthorized disclosure is called as _____
A. Authentication B. Access control C. confidentiality D. Non repudiation

2. _____ is one that encrypts a digital data stream one bit or one byte at a time.
A .stream cipher B. block cipher C. Caesar cipher D. substitution cipher

3. The Playfair algorithm is based on the use of a _____ of letters constructed using a keyword
A . 5 x 5 matrix B. 5 4 matrix C. 4 4 matrix D. 4 5 matrix

4. An attempts to gain unauthorized access to computer systems is a_____ _attack.
A. Passive B. Active C. Masquerade D. replay

5. AES allows only a block length of_____ bits.
A. 128 B. 256 C. 192 D. 114

6. _____ analysis is the observation that the power consumed by a smart card at any particular time during the cryptographic operation .
A. Crypto B. security C. power D. traffic

7. Key stream generation involves the modulo operation and _____
A. byte swapping B. bit swapping C. octal swapping D. Quad swapping

8. A _____ is a value that is used only once, such as a timestamp, a counter, or a random number.
A. state B. nonce C. session key D. block lengths

9. An integer $p > 1$ is a _____ if and only if its only divisors are $\pm 1$ and $\pm p$.
A. positive integers B. prime number C. negative integers D. even number

10. The _____ can be used to encrypt information that can only be decrypted by the possessor of the private key.
A. session key B. master key C. distribution key D. public key

11. An authenticator that is a cryptographic function of both the data to be authenticated and a secret key is known as _____
A. message authentication code B. Hash value C. Hash function D. elliptic function

12. _____ is formed by encrypting a hash code of the message with the sender's private key
A. digital signature B. nonce C. arbiter D. authentication

13. _____ is an authentication service in a distributive environment
A. X.509 B. security C.Kerberos D. PKI

14. _____ is defined as the set of hardware, software needed to create, distribute and revoke digital certificates.

A. digital signature B. nonce C. PKI D. authentication

15. _____ is an open source software which provide authentication using digital signature.
A. PGP B. X.509 C. RFC 822 D. CAST128

16. An Internet standard to email security is known as _____
A.S/MIME B.IPsec C. X.509 D. PGP

17. _____ model is used to estabilish transition probabilities among various states.

A. standard deviation B. Markov C. operational D.multivariate

18. ----------anomaly detection involves the collection of data relating to the behavior of legitimate users over a period of time
A. statistical B. rule-Based C. distributed D.base rate

19. The decay systems that are designed to lurea potential attacker away from critical systems is known as _____
A. LAN monitor B. central manager C. host audit record D.honey pot

20. _____ attack is an attempt to prevent legitimate users of a service from using that service.
A. Denial of service B. spoofing C. black hole D.tunneling

**PART –B (5 x16 = 80 Marks)**

21.a) Explain : i) Caesar cipher (4)
ii) Monoalphabetic cipher (4)
iii) Playfair cipher (4)
iv) Rail fence cipher (4)

**(OR)**

21. b) i) Explain DES encryption and decryption in detail. (16)

22.a) Discuss the following:

i) Add round key (8)

ii) Difference between Rijndael and AES (8)

**(OR)**

22. b) Explain RC4 algorithm in detail. (16)

23.a) Explain Digital signature approaches and algorithm in detail (16)

**(OR)**

23. b) Explain : i) General operation of PGP (8)

ii) S/MIME algorithm and functions (8)

24.a) Discuss three types of X.509 authentication procedure in detail. (16)

**(OR)**

24.b) Explain IP security in detail (16)

25.a) Describe two approaches of intrusion detection. (16)

**(OR)**

25.b) Write note on : i) Honey pots (6)

ii) Password protection (10)

**********