Register Number.................

ME. DEGREE EXAMINATIONS: OCTOBER/NOVEMBER – 2008

Third Semester

COMPUTER SCIENCE & ENGINEERING

P07CSE09: Network Security

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

Answer ALL Questions: -

PART A (20 X 1 = 20 Marks)

1. Which among the following is a Transposition technique ?
A. One-Time Pad B. Rail Fence C. Vernam Cipher D. Playfair Cipher

2. The number of S-Boxes in DES is __________.
A. 8 B. 16 C. 32 D. 64

3. The length of the plaintext being encrypted in DES at a time is _______.
A. 128 bits B. 64 bits C. 32 bits D. 16 bits

4. Which of the following is not a Steganographic technique ?
A. Pin Puncture B. Invisible Ink C. Character Marking D. Certification

5. Euler's Totient Function Φ(P) for a prime number P is _________.
A. P B. P+1 C. P-1 D. P^2

6. Which among the following is a counter measure for Timing Attack ?
A. Blinding B. Bastion Host C. Notarization D. Signed Data

7. Which of the following public-key cryptosystems can not be used for Digital Signature ?
A. RSA B. ECC C. Diffie-Hellman D. DSS

8. Public-Key Certificates are used to implement ______________.
A. Confidentiality B. Message Integrity
C. Authorization D. Public Key Distribution

9. Hash Functions are used to implement ______________.
A. Confidentiality B. Message Integrity
C. Authorization D. Authentication

10. For any given block x, if it is computationally infeasible to find any pair (x,y) such that H(x)=H(y), then this property is called ______________.
A. One-way B. Weak collision Resistance
C. Strong Collision Resistance D. Computation Resistance

11. What is the Message Digest size of SHA-I ?
A. 160 B. 256 C. 384 D. 512

12. The number of rounds in MD5 is ________.
A. 16 B. 8 C. 4 D. 2

13. X.509 standard was defined by __________.
A. ITEF B. ISO C. ANSI D. ITU-T

14. Which of the following is a Technical deficiency of Kerberos Version 4 ?
A. Internet Protocol Dependence B. Double Encryption
C. Authentication Forwarding D. Ticket Lifetime

15. Which of the following Algorithm is not used in PGP ?
A. CAST B. IDEA C. RSA D. ECC

16. Change Cipher Spec Protocol is a part of __________.
A. SSH B. TLS C. SSL D. SET

17. Which among the following does not replicate ?
A. Trojan Horse B. Virus C. Worm D. Zombie

18. Which of the following does not need a host program ?
A. Trap door B. Worm C. Trojan Horse D. Virus

19. Which of the following Virus mutates with every infection ?
A. Parasitic Virus B. Stealth Virus
C. Boot Sector Virus D. Polymorphic Virus

20. Which among the following is called a Simple Security Property ?
A. Complete mediation B. Isolation
C. No read up D. No write down

PART B (5 X 16 = 80 Marks)

21. (a) (i) Encrypt the word "FIGHT" using Hill Cipher and verify. (10)

(ii) Briefly discuss about Transposition Techniques with an example. (6)

(OR)

(b) (i) Encrypt the word "FREEDOM" using Playfair Cipher and verify. (6)

(ii) Discuss the Data Encryption Standard in detail. (10)

22. (a) (i) Explain about Key management. (8)

(ii) Discuss about the RSA cryptographic algorithm. (8)

(OR)

(b) (i) Explain about Diffie-Hellman key exchange. (8)

(ii) Discuss about the ECC cryptographic algorithm. (8)

23. (a) (i) Briefly discuss about MD5. (8)

(ii) What you mean by Digital Signature? Explain. (8)

(OR)

(b) (i) Write a note on Message Authentication Codes. (8)

(ii) Discuss about the security of Hash functions. (8)

24. (a) (i) Explain about Kerberos. (8)

(ii) Discuss about the IP Security Architecture. (8)

(OR)

(b) (i) Explain about X.509 Authentication Service. (8)

(ii) Write a note on PGP. (8)

25. (a) (i) Discuss in detail about Malicious Programs. (10)

(ii) Write a note on Trusted Systems. (6)

(OR)

(b) (i) What you mean by a Firewall? Explain. (10)

(ii) Write notes on Digital Immune System and Behavior-Blocking Software. (6)

****