Register Number: ……..

B.E.DEGREE EXAMINATIONS: NOV/DEC 2010

Seventh Semester

COMPUTER SCIENCE AND ENGINEERING

U07IT603: Cryptography and Network Security

Time: Three hours **Maximum Marks: 100**

Answer ALL Questions:-

PART A (10 x 1 = 10 Marks)

1. ---------- cipher process the input element continuously

   a) Blocks cipher b) Stream cipher c) Ceaser cipher d) Mono alphabetic cipher

2. In --------- attacks the attackers tries every possible key on a piece of cipher

   a) Traffic analysis b) Brute Force attack c) Masquerade d) DOS

3. What is the size of the single word in the AES algorithm

   a) 2 bytes b) 6 bytes c) 4 bytes d) 8 bytes

4. Which of the following statement is correct?

   a) Shift row is simple permutation

   b) Shift row it shifts the row circularly left or right

   c) Shift roe uses an s- box top perform a byte by byte substitution of the block

   d) both a&b

5. Select the name of the property in which for any given block x it is computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$

   a) fixed length output b) One way Property

   c) Week collision resistance d) Strong collision resistance.

6. How many number of steps will be used in SHA 512

   a) 80 b) 64 c) 20 d) 16

7. Which protocol is said to be store and forward email protocol

   a) SMTP b) FTP c) HTTP d) TCP

8. Select the name of the algorithm that is used by DSS

   a) MD5 b) SHA c) RIPEMD d) FIFO

9. Denial of transmission of message by source is said to be _____

   a) Sequence modification b) Destination repudiation

   c) Timing Modification d) Source repudiation

10. Hash Code is also referred to _____

    a) Authenticator b) Message digest c) Hash function d) Traffic analysis

PART B (10 x 2 = 20 Marks)

11. What is the difference between OFB and CFB?
12. Explain the Avalanche effect.
13. State any two requirements for public key cryptography.
14. State Fermat's theorem.
15. Compare SHA-1 and MD5.
16. What is mutual authentication?
17. Draw the block diagram of SSL Record protocol.
18. What is signature component in PGP message?
19. What are the types of viruses?

20 What is Zombie?

PART C (5 x 14 = 70 Marks)

21. a) Explain various modes of block cipher in detail.

(OR)

b) Explain how secret keys are exchanged and messages are encrypted in Elliptic Cryptosystem.

22. a) How security is achieved by using Hash function and MACs?

(OR)

b) (i) What are the three procedure used in X.509 authentication? (7)

(ii) Write short notes on PGP. (7)

23. a) Explain in detail about SSL Record protocol operation.

(OR)

b) Explain about password selection strategies.

24. a) What are the four general techniques that firewall use to control access. Explain any one.

(OR)

b) Explain rule-based intrusion in detail.

25. a) Describe RSA algorithm and Explain.

(OR)

b) Explain about the security of RSA in detail.

****