Register Number……

B.TECH. DEGREE EXAMINATIONS: APRIL / MAY 2010

Sixth Semester

INFORMATION TECHNOLOGY

U07IT603: Cryptography and Network Security

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

Answer ALL the Questions:-

PART A (10 x 1 = 10 Marks)

1. The X.800 standard focuses on security_____

(a) attack (b) mechanisms (c) services (d) All the above

2. Which modes of operation do not have feedback mechanism?

(a) CBC (b) CFB (c) ECB (d) OFB

3. A public key cryptosystem has _____

(a) Public key (b) Private key (c) Both (d) None of the above

4. _____ is used to identify key transaction uniquely

(a) Request (b) Time (c) identifier (d) Nonce

5. A Hash Function produces _____value.

(a) Hash Value (b) Message Digest (c) Random key (d) Both (a) and (b)

6.The process of verifying an identity claimed by a system entity.

(a) Authentication (b) Integrity (c) Confidentity (d) Access Control

7._____ is an authentication service designed for use in a distributed environment.

(a) PGP (b) S/MIME (c) Kerberos (d) None of the above

8._____ is an open encryption and security specification designed to protect credit card transactions on Internet.

(a) SSL (b) SET (c) TLS (d) None of the above

9.Which is not malicious programs?

(a) Anti virus (b) Virus (c) Worm (d) Logic Bomb

10._____ Serves as a secure platform for an application level gateway

(a) Bastion Host (b) Router (c) Information Server (d) Web server

PART B (10 x 2 = 20 Marks)

11. List out different categories of trusted systems information
12. Specify any four types of viruses
13. Define X.509
14. Draw the block diagram for SSL protocol stack.

15. Write HMAC Function expression.
16. Give any two examples for authentication function.
17. State Euler's theorem.
18. Diffie-Hellman key Exchange protocol is insecure. Justify your answer.
19. Cipher Text = "MWOCTCIWTW" and Key = 2.
    Find out Plain Text using Caesar techniques.
20. Differentiate Stream cipher form Block cipher.

PART C (5 x 14 = 70 Marks)

21. a) Describe block cipher modes of operation in detail.

(OR)

b) Describe basic elements of a symmetric encryption model.

22. a) Explain the Diffie-Hellman key exchange algorithm with an example.

(OR)

b) Explain the RSA algorithm with an example.

23. a) Briefly discuss about SHA-512 Round function operation.

(OR)

b) Briefly discuss DSS signing & verifying processes.

24. a) Draw the flowchart for the Transmission and Reception of PGP messages.

(OR)

b) Analyse IPSec document in detail.

25. a) Write a short notes about the following

(i) Firewall Types (7)

(ii) Firewall Configuration (7)

(OR)

b) Write a short notes about the following

(i) Access Control Structure (7)

(ii) Reference Monitor concept. (7)

****