Register No: ……………………..

**B.TECH DEGREE EXAMINATIONS: APRIL/MAY 2011**

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 principle of ____________ ensures that the sender of a message cannot later claim that the message was never sent

   a) Access control b) Authentication c) Availability d) Non-repudiation

2. The process of writing the text as diagonals and reading it as sequence of rows is called as

   a) Rail Fence Technique b) Caesar Cipher

   c) Mono-Alphabetic Cipher d) Homophonic Substitution Cipher

3. To decrypt a message encrypted using RSA, we need the __________.

   a) Sender’s private key b) Sender’s public key

   c) Receiver’s private key d) Receiver’s public key

4. _____________ are very crucial for the success of asymmetric cryptography.

   a) Groups b) Prime numbers c) Negative numbers d) Integers

5. When two different message digests have the same value, it is called as ______.

   a) Attack b) Collision c) Hash d) Digital envelope

6. ___________ is a message digest algorithm

   a) DES b) AES c) MD5 d) RSA

7. SSL layer is located between _________and ________.

   a) Transport layer, network layer b) Application layer, transport layer

   c) Data link layer, physical layer d) Network layer, data link layer

8. The main purpose of SET is related to _____.

   a) Secure communication between browser b) Digital signatures and server

   c) Message digests d) Secure credit card payments on the Internet

9. In ____________, direct connection between the internal hosts and the packet filter are avoided.

   a) Screened host firewall, Dual-homed bastion

   b) Screened host firewall, single-homed bastion

c) Screened host firewall, None-homed bastion

d) Screened host firewall, Triple-homed bastion

10. One of the most important tools in intrusion detection is the usage of _____.

a) MIB b) Audit records c) Session details d) passwords

**PART B (10 x 2 = 20 Marks)**

11. Differentiate diffusion and confusion.
12. What are the two problems with the one-time pad?
13. Define Fermat’s Theorem.
14. Find gcd(86,56)using Euclid,s algorithm.
15. Define weak collision property of a hash function.
16. Mention any two differences between SHA-1 and MD5.
17. State the applications of IPSec.
18. List three approaches to secure user authentication in a distributed environment.
19. What are the three classes of intruders?
20. List down the four phases of Viruses.

**PART C (5 x 14 = 70 Marks)**

21. a) (i) Encrypt the plain text “Friday” using Hill cipher algorithm and the key is

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$ (7)

(ii) In AES, how the encryption key is expanded to produce keys for the 10 rounds. (7)

**(OR)**

b) (i) With a neat diagram explain the operation of DES. (8)

(ii) Explain any two modes of operation of DES. (6)

22. a) (i) Users A and B use Diffie Hellman technique, a common prime p=71 and a primitive root g=7 are used. If user A has private key $X_A$=5, what is A’s public key $Y_A$? If user B has private key $X_B$=12, what is B’s public key $Y_B$? What is the shared secret key? (7)

(ii) How are arithmetic operations on integers carried out from their residues modulo a set of pair wise relatively prime moduli? Give the procedure to reconstruct the integers from the residues. (7)

**(OR)**

b) In ECC, the cryptosystem parameters are $E_{11}(1,6)$ and point G on the elliptic curve is G = (2,7). B's secret key is $n_B = 7$.

(i) Find out B's public key $P_B$. A wishes to encrypt the message $P_m$ = (10, 9) and chooses the random value K=3.Determine the cipher text $C_m$. (10)

(ii) How will B recover Pm from $C_m$? (4)

23. a) (i) With DSS, because the value of 'K' is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. But, when using RSA signatures this does not happen? What is the practical implication of this difference? (4)

(ii) With necessary diagrams explain the signing and verification of DSS. (10)

**(OR)**

b) (i) Explain the operation of RIPEMD. (7)

(ii) Explain the processing of a message block of 512bits using MD5. (7)

24. a) (i) Explain handshake protocol actions of SSL. (10)

(ii) Explain the tunnel mode and transport mode of IPSec. (4)

**(OR)**

b) Discuss in detail about Secure Electronic Transaction.

25. a) (i) When system administrators trust the internal users, What type of firewall is used? What are its limitations and how is to overcome these difficulties? (6)

(ii) How will you enhance the ability of a system to defend against intruders and malicious programs? (8)

**(OR)**

b) (i) Discuss in detail about firewall design principles. (7)

(ii) List and brief, the different generations of antivirus software? (7)

**********