Printed Pages – 3 CS – 023/IT – 701

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 1013 Roll No. | | | | | | | | | | |

B.Tech.

SEVENTH SEMESTER EXAMINATION, 2006 - 07

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note : *(i) Attempt ALL questions.*

(ii) All questions carry equal marks.

(iii) Be precise in your answer.

1. Attempt ***any four*** parts of the following : **(5x4=20)**

(a) Detailing different categories of security attacks of a computer system, clearly distinguish between security attack, security mechanism and security service.

(b) Compare and contrast substitution techniques with Transposition techniques under classical encryption.

(c) Explain the principle of differential cryptanalysis.

(d) Discuss the strength of DES algorithm.

(e) "The strength of any cryptographic system rests with the key distribution technique" comment.

(f) What is a random number ? How do we generate cryptographically secure pseudorandom numbers. Explain one scheme only.

03245

2. Attempt *any four* parts of the following : **(5x4=20)**

(a) Explaining Fermat's theorem find 3^{201} mod 11.

(b) Find all primitive roots of number 19.

(c) Explaining RSA algorithm find the private key of a user if his public key e = 31 and n = 3599.

(d) In a Diffie-Hellman key Exchange algorithm, let the prime number be 353 and one of its primitive root be 3. Let A and B select their secret keys $X_A = 97$ and $X_B = 233$. Compute :

(i) Public keys of A and B

(ii) Common secret key

(e) Explain features of key management system.

(f) What is Elliptic Curve Cryptography. Explain encryption and decryption process in this context.

3. Attempt *any two* parts of the following : **(10x2=20)**

(a) Compare the security of Hash functions and Message authentication codes against Brute force attack and crypt analysis.

(b) Explain Digital Signature Standard, its approach and algorithm.

(c) With reference to supress-relay attack what happens when the party's and KDC's clock are not synchronised ? How nonces are helpful ?

4. Attempt *any two* parts of the following : **(10x2=20)**

(a) What is the purpose of X·509 standard and how is an X·509 certificate revoked ?

(b) Why is the segmentation and reassembly function in PGP needed ? How does PGP use the concept of trust ?

(c) What entities constitute a full-service Kerberos environment.

5. Attempt *any two* parts of the following : **(10x2=20)**

(a) What are the measures used for Intrusion Detection ?

(b) Explain different types of firewalls and their configurations.

(c) What are typical phases of operation of a virus or worm and how does behaviour blocking software work ?

- o O o -