Printed Pages—4 **TIT701**

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

PAPER ID : 0150	Roll No.										

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION 2010-11

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note : Answer all questions.

1. Attempt any **two** parts : **(10×2=20)**

(a) (i) Explain the following terms :

(a) Message Integrity

(b) Denial of Service

(c) Fiestal Cipher.

(ii) Describe the Hill Cipher. Discuss the strength of the cipher.

(b) (i) A single bit error occurs in exactly one block of ciphertext during transmission. How will this affect the recovery of plaintext in each of the following modes :

ECB, CBC, CFB, OFB.

(ii) Prove that in a DES cipher, if plaintext block and encryption key is complemented bitwise then resulting ciphertext block is the bitwise complement of the original ciphertext block.

(c) (i) What do you understand by weak keys of DES ? Explain.

(ii) Given that encryption key in a transposition cipher is :

(2, 6, 3, 1, 4, 8, 5, 7)

Obtain the decryption key.

(iii) Describe how a meet in the middle attack can be launched on Double DES.

Answer any **two** parts : **(10×2=20)**

(a) (i) Define ring. Give an example of ring which is not field.

(ii) Compute multiplicative inverse of 77 in Z_{411}.

(b) (i) Define primitive root. Given that 2 is a primitive root of 29. What are other primitive roots of 29 ?

(ii) Give Elliptic Curve based Diffie-Hellman Key exchange algorithm.

(c) (i) Write the steps of RSA Key generation. Suppose message m and modlus n are not relatively prime, will RSA scheme work ? Give arguments in favour of your answer.

(ii) Compute 3^{201} mod11 : What is the minimum number of the multiplication required for this computation.

Answer any **two** parts : **(10×2=20)**

(a) (i) What are the requirements of a Message Authentication Code (MAC) ? List and explain them.

(ii) Give a general structure of a hash function.

(b) (i) What is the purpose of appending length of message to the message in MD5 hash algorithm ?

(ii) What are the order of efforts required to attack strong collision resistance property and weak collision resistance property of MD5 hash algorithm.

(iii) What is birthday attack ? How a birthday attack can be launched ? Illustrate with the help of one example.

(c) (i) What is digital signature ? What requirements should a digital signature scheme satisfy ?

(ii) Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. Give reasons behind choice of various parameters of the algorithm. What is the implication if same value of K (secret per message) is used to sign two different messages using DSA ?

4. Answer any **two** parts : **(10×2=20)**

(a) What are the entities that constitutes Kerberos environment ? Write down the message exchanges for obtaining ticket-granting ticket and service-granting ticket in context of kerberos version 4. Give the justifications behind choice of various elements of the messages.

(b) What is digital certificate ? Give the formats of X.509 digital certificate and X.509 certificate revocation list. Explain various fields of the formats.

(c) In context of PGP, answer the following :

(i) What is the structure of public key ring and private key ring ?

(ii) What is passphrase ?

(iii) What is difference between owner-trust field and key-legitimacy field ?

(iv) Signature is generated before compression and encryption is applied after compression. Why ?

5. Write short notes on any **two** : **(10×2=20)**

(a) IP Sec protocols and modes of operation.

(b) Secure Socket Layer.

(c) Firewalls.