

Printed Pages—4

EIT701

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

PAPER ID : 2757

Roll No.

--	--	--	--	--	--	--	--	--	--

B.Tech.

(SEM. VII) ODD SEMESTER THEORY

EXAMINATION 2013-14

CRYPTOGRAPHY AND NETWORK SECURITY*Time : 3 Hours**Total Marks : 100***Note :- Attempt all questions.**

1. Attempt any **four** questions : **(5×4=20)**
- (a) Draw the block diagram of Fiestal Structure. Discuss the characteristics of Fiestal Cipher.
 - (b) Describe at least two modes of operation of block cipher.
 - (c) Differentiate between the following :
 - (i) Block Cipher and Stream Cipher
 - (ii) Authentication and Authorization
 - (iii) Stagenography and Cryptography.
 - (d) Discuss the role of S-boxes in DES.
 - (e) Explain the playfair cipher technique. Consider a plain text message I AM A HACKER. Encrypt it with the help of keyword—COMPUTER.

EIT701/DNG-52035

1

[Turn Over

- (f) What do you mean by the Hill Cipher technique? By using Hill Cipher technique encrypt the message "AT" with the

help of key $K = \begin{bmatrix} 5 & 3 \\ 3 & 4 \end{bmatrix}$.

2. Attempt any two questions : (10×2=20)

- (a) Define a Group and Ring. Prove that the order of any subgroup of finite group divides the order of the group.

- (b) (i) Using Chinese Remainder Theorem (CRT) solve the following simultaneous congruences :

$$x \equiv 3 \pmod{9}, x \equiv 2 \pmod{10}, x \equiv 3 \pmod{11}.$$

- (ii) Write the steps of RSA key generation. Suppose message m and modulus n are not relatively prime, will RSA scheme work? Give arguments in favour of your answer.

- (c) (i) The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

- (ii) Determine $27^{-1} \pmod{100}$ using extended Euclidean algorithm.

3. Attempt any **two** questions : (10×2=20)

- (a) (i) What are the requirements of Message Authentication Code (MAC) ? List and explain them. How is it different from Hash function ?
- (ii) What is Birthday Attack ? Explain with suitable example.
- (b) Explain the sequence of steps to create message digest using SHA algorithm. You may overlook the finer detail of the steps.
- (c) What is digital signature ? Explain the requirements of digital signature. Write and explain Digital Signature Algorithm (DSA) of Digital Signature Standard.

4. Attempt any **two** questions : (10×2=20)

- (a) Explain Diffie-Hellman Key exchange technique.

User A and B use the Diffie-Hellman Key exchange technique a common prime $q = 71$ and a primitive root $\alpha = 7$

- (i) If user A has private key $X_A = 5$, what is A's public key Y_A ?

- (ii) If user B has private key $X_B = 12$, what is B's public key Y_B ?
- (iii) What is the shared secret key ?
- (b) What is Digital Certificate ? Give the format of X.509 certificate showing the various elements of the certificate. Explain the format.
- (c) Write and explain the sequence of messages used by Kerberos for authentication.
5. Write short notes on any two of the following : (10×2=20)
- (a) Secure Socket Layer (SSL)
- (b) Intrusion Detection
- (c) Modes of IP sec.