Printed Page: 2

EIT-701

Roll No. □□□□□□□□□□

B.Tech.

(SEM VII) ODD SEMESTER THEORY EXAMINATION, 2015-16

CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours *Maximum Marks: 100*

Note:

(i) *Attempt* ***ALL*** *questions.*
(ii) *All questions carry equal marks.*
(iii) *Notations/ Symbols/ Abbreviations used have usual meaning.*

Q.1. ***Attempt any FOUR parts of the following****.* **5x4=20**

a) What is Shanon’s principle of Confusion and diffusion in cryptography? Discuss.

b) Differentiate between the following.

i. Crptography and Steganography
ii. Active attack and passive attack
iii. Authentication and Authorization

c) Draw the block diagram of single round of the DES cipher.

d) Explain the OFB mode of operation of block cipher. Write the relative merit of this mode compared to CFB mode of operation.

e) The plaintext FRAYID is encrypted using 2 X 2 Hill cipher to yield ciphertext PQKUCF. Using the plaintext ciphertext pair, can you determine the key used for encryption?

f) What do you understand by Replay attack? Explain with suitable example.

Q.2. ***Attempt any FOUR parts of the following:*** **5x4=20**

a) State and Prove Fermat’s Theorem.

b) Write RSA algorithm. Will the scheme work if message is modulus have some common factor? Justify your answer.

c) What is common modulus attack in context of RSA? Choose suitable example to demonstrate how it works?

d) Define Subgroup. Prove that intersection of the subgroups of a group is also subgroup while union of the subgroups of a group may not be subgroup.

e) Given 2 is primitive root of 29. Solve the congruence

x^2 D 10 mod 29

f) Use Chinese Remainder Theorem (CRT) to determine sum of **x** and **y** defined by following simultaneous congruences.

$x \equiv 0 \bmod 7$, $x \equiv 0 \bmod 8$, $x \equiv 5 \bmod 9$,
$y \equiv 2 \bmod 0$, $y \equiv 7 \bmod 8$, $y \equiv 6 \bmod 9$

Q.3. ***Attempt any TWO parts of the following:*** **10x2=20**

a) Consider a ***n***-bit hash function H which is applied to ***k*** random inputs. Obtain the minimum value of the ***k*** for which the probability of getting strong collision is more than **0.5**.

b) Write down the requirements of following.

(i) Digital Signature
(ii) Message Authentication Code

c) Describe the signature generation and signature verification process of the digital signature scheme of Digital Signature Standard (DSS).

Q.4. ***Attempt any TWO parts of the following:*** **10x2=20**

a) Name the services offered by PGP and give the general format of a PGP Message.

b) Write the following schemes for exachange of secret key between two communication parties.

i) Diffie-Hellman scheme
ii) Needham Schreoder Protocol

b) What do you understand by a Kerberos Environment? Write the sequence of message exchanges that takes place between various Kerberos elements for getting the service of certain Server. Explain the mechanism adapted in the protocol to avoid the traveling of password in plaintext.

Q.5. ***Write short notes on any TWO of the following:*** **10x2=20**

a) Secure Electronic Transaction (SET)
b) Computer Viruses and other related threats
c) IPSec