Printed pages: 2	IT701
(The paper code and roll No. to be filled in your answer book)	
Roll No.	

B TECH
(SEM VII) THEORY EXAMINATION 2016-17
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) Explain the following terms.
Steganography, Passive attack, Denial of Service, Provably Secure Cipher, Trojan horse

b) Draw the block diagram of single round of the DES cipher along with generation of key schedule. Is it possible with DES that a message encrypted by one key can be decrypted using different key?

c) Explain the CBC and OFB mode of block cipher. Write their relative advantages.

d) The cipher text YIFZMA was encrypted by Hill cipher using following matrix.
$K_{11}=9$, $K_{12}=13$, $K_{21}=2$, $K_{22}=3$.
Find the plaintext.

e) Suppose E^1 and E^2 are two encryption methods. Let K_1 and K_2 be keys and define double encryption scheme E as follows:
$E(K_1, K_2, M)= E^1(K_1,E^2(K_2,M))$
Show how a meet-in-the-middle attack can be performed on this double encryption.

f) Compare the characteristics of Link level encryption and End-to-End encryption in a network?

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

a) State Euler's theorem and hence determine last three digits of $\mathbf{7^{803}}$.

b) Use extended Euclidean algorithm to find multiplicative inverse of **550 mod 1769.**

c) Write RSA algorithm. Thereafter, write in brief the reasons behind the choices being made in various steps of the algorithm. Prove that the algorithm works even if a message is not relatively prime to the modulus of the algorithm.

d) Define cyclic group. Give one example of finite and infinite cyclic group each. Prove that order of any element of a finite cyclic group is factor of order of the group.

e) What do you understand by primitive root? Determine all the primitive roots of 25.

f) Find all the solution of the given simultaneous congruence using Chinese Remainder Theorem (CRT).
$\mathbf{x^2 \equiv 1 \bmod 7, x^2 \equiv 4 \bmod 11}$

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

a) What are requirements of a message authentication code? Give formulation of a birthday attack in a scheme where an encrypted Hash code is used for message authentication.

b) Given that user A and B share a secret key **Ka** and **Kb** respectively for secure communication with a trusted server S. Suppose user A wants to send a secret message **m** to B, A generates a random number **R** and initiates the following protocol.
Step1. A to S: **A**, **B**, $\mathbf{E_{Ka}[R].}$
Step 2. S to A: $\mathbf{E_{Kb}[R]}$
Step 3. A to B: $\mathbf{E_R[m], E_{Kb}[R]}$.
Step 4. B decrypts $\mathbf{E_{Kb}[R]}$ to get **R** and then use **R** to decrypt $\mathbf{E_R[m]}$ to get **m**.
Give your assessment on the security of the protocol.

c) Describe the signature generation and signature verification process of the digital signature scheme of Elgamal Digital Signature Algorithm. Explain why signature of the same person on the same message at different occasions differs?

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

a) Write the sequence of message exchanges that takes place in a Kerberos Environment for getting the service of certain Server. Explain how protocol handles the possibility of replay attacks and vulnerability of password travel in plaintext.

b) Give the general format of X.509 digital certificate. What do you understand by chain of certificates in PKI? How a compromised key is revoked in PKI?

c) Give the structures of Private Key ring and Public key ring of PGP explaining its various attributes. Why are the rings indexed on Key ID as well as User ID?

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

a) IPSec Protocols and Modes
b) Firewall
c) Payment Processing in Secure Electronic Transaction (SET)