Roll No.										

Paper Code: ECS-084

B.Tech.
(SEM VIII) EVEN SEMESTER EXAMINATION, 2015-16
CRYPTOGRAPHY & NETWORK SECURITY

[Time: 3 Hours] **[Max. Marks: 100]**

Note:-

(i) Attempt all questions. All questions carry equal marks.
(ii) Notations/ Symbols/ Abbreviations used have usual meaning.
(iii) Make suitable assumptions, wherever required.

1. Attempt any four parts of the following:- **[5x4=20]**

(a) Explain the following terms :
(i) Replay Attack
(ii) Message Integrity
(iii) Computationally Secure Cipher
(iv) Steganography
(v) Principle of Confusion and Diffusion

(b) Compare the CBC, CFB and OFB modes of operation of any block cipher with due emphasis on the relative advantages and disadvantages of one over the other.

(c) Draw block level diagram to depict the structure of one round of DES Encryption along with generation of key schedule.

(d) What do you understand by weak keys and semi weak keys in context of DES?

(e) Show that encryption process with reverse key schedule in a Fiestal cipher works as decryption process.

(f) Suppose that the plaintext **FD** is encrypted to **KJ** and **WA** is encrypted to **OG** using a 2 X 2 Hill cipher. Determine the key used.

2. Attempt any four parts of the following:- **[5x4=20]**

(a) Use Extended Euclidean Algorithm to find multiplicative inverse of 1234 mod 4321.

(b) State and Prove Euler's Theorem. Determine the value of Euler totient function **Φ(2016).**

(c) Define group. Let **(G, *)** be a group and G' is nonempty subset of G. Prove that (**G', *)** is subgroup of **(G, *)** if and only if

$$a * b^{-1} \in G', \forall\, a \in G', b \in G'.$$

(d) Give the complete outline of common modulus attack on RSA public key scheme.

(e) Use Chinese Remainder Theorem to find the value of **x** which satisfies the following simultaneous congruences.

$$x \equiv 3 \bmod 7,\ x \equiv 3 \bmod 13,\ x \equiv 0 \bmod 12$$

(f) Describe the RSA cryptosystem. Will the scheme work for the messages which are not relatively primes to the modulus of the scheme? Justify your answer.

3. Attempt any two parts of the following:- **[10x2=20]**

(a) What are requirements of digital signature? Describe the Elgamal Digital Signature generation and verification process. What happens if the same value of ***k*** (user's per-message secret number) is used to sign more than one message using this scheme?

(b) What is message authentication code (MAC)? What are the requirements of a message authentication code? Determine the value of ***n*** for which the probability that at least two messages in a set of ***n*** number of messages produces the same 512-bit hash value is 0.25.

(c) Suppose the message **M** consists of block $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{M_n}$, each of 56 bit, in order. The 64 bit hash code of message **M** is given by **G** defined as follows.

$\mathbf{H_0 = C}$ // 64 bit constant initial value
$\mathbf{H_i = DES_{Mi}[H_{i-1}]}$ //DES encryption with M_i as key
$\mathbf{G = H_n}$

Can you suggest any form of birthday attack on this scheme? Assume that opponent has intercepted a message with a signature in the form of encrypted hash code.

4. Attempt any two parts of the following:- **[10x2=20]**

(a) Explain the process of message generation of sender PGP entity. Explain why does PGP use compression before enveloping the message? Also give the structure of Private Key ring and Public Key ring.

(b) What are various servers used in Kerberos? Describe the sequence of message exchanges in Kerberos. Explain how user is authenticated to various servers without sending the password to them.

(c) Attempt the following:-

(i) Users A and B use a Diffie-Hellman key exchange protocol with a chosen common prime p = 11 and a primitive root g = 2. Given that public keys of A and B are 9 and 3 respectively. Determine the private keys of A and B. Further determine the shared secret key K

(ii) In a network, user nodes 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 initiates the following protocol.

A. A generates a random number **R** and sends to the S his name **A**, destination **B**, and $\mathbf{E_{Ka}[R]}$.
B. S responds by sending $\mathbf{E_{Kb}[R]}$ to A.
C. A sends $\mathbf{E_R[m]}$ together with $\mathbf{E_{Kb}[R]}$ to B.
D. B know **Kb**, thus decrypts $\mathbf{E_{Kb}[R]}$ to get **R** and will subsequently use **R** to decrypt $\mathbf{E_R[m]}$ to get **m**.

Give your analysis and comment on the security of the protocol.

5. Write short notes on any two of the following:- **[10x2=20]**

(a) Modes of IPSec
(b) Intrusion Detection Techniques
(c) Secure Electronic Transaction