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

PAPER ID : 110854 **Roll No.** | | | | | | | | | | |

B.Tech.

(SEM. VIII) THEORY EXAMINATION 2013-14

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note :– All questions carry equal marks.

1. Attempt any **four** parts of the following : **(5×4=20)**

   (a) What are the essential ingredients of a symmetic cipher ? List two basic functions used in encryption algorithm.

   (b) A Hill Cipher uses the following key for enciphering the message:

   $$K=\begin{bmatrix}3 & 2\\ 5 & 7\end{bmatrix}$$

   Obtain the decryption key to be used for deciphering the cipher text.

   (c) Describe the operation of key generation and the single round function f_R of simple DES.

   (d) What is an Initialization Vector (IV) ? What is its significance ?

   (e) What do you mean by Block Ciphers ? What are the different modes of Block Ciphers ? How does it differ from stream cipher ?

   (f) Discuss the Shannon's theory of confusion and diffusion.

2. Attempt any **four** parts of the following : **(5×4=20)**

(a) Solve the following simultaneous congruence using Chinese remainder theorem

$x \equiv 1 \bmod 2$

$x \equiv 1 \bmod 3$

$x \equiv 1 \bmod 5$

$x \equiv 1 \bmod 7$

(b) Explain Fermat's theorem and using it find $30^{201} \bmod 11$

(c) Find all primitive roots of number 23

(d) Explain Euclid Algorithm. Find gcd of 1970 and 1066 by using Euclid Algorithm.

(e) What do you mean by Primality Testing ?

(f) Discuss the security of RSA algorithm.

3. Attempt any **two** parts of the following : **(10×2=20)**

(a) What do you mean by MAC ? Explain what characteristics are needed in a secure Hash function.

(b) What do you mean by Direct and Arbitrated Digital Signature ? Illustrate with some suitable application.

(c) In MD 5 algorithm, What is the number of padding bits if the length of original message is 2590 bits ? Do we need padding if the length of the original message is already a multiple of 512 bits.

4. Attempt any **two** parts of the following : **(10×2=20)**

(a) What is the segmentation and reassembly function in PGP needed ? How does PGP use the concept of twist ?

(b) What is Kerberos ? What entities constitute a full service Kerberos environment ?

(c) What is Digital Certificate ? Give the format of X.509 certificate showing the important element of the certificate. Explain the format.

5. Attempt any **two** parts of the following : **(10×2=20)**

(a) Describe the basic approaches to bundling SAS ? List the difference between transparent mode and tunnel mode.

(b) What do you mean by SSL and SET ? What is the difference between SSL connection and SSL session ? Discuss SSL protocol architecture.

(c) Write notes on the following :

(i) Intrusion detection

(ii) Viruses and related threats.