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

PAPER ID : 1453 Roll No. | | | | | | | | | | |

MCA

(SEMESTER-IV) THEORY EXAMINATION, 2012-13

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours] *[Total Marks : 100*

SECTION – A

1. Attempt **all** parts. **10 × 2 = 20**

   (a) What is the difference between passive and active security threats ?

   (b) What are the two general approaches to attacking a cipher ?

   (c) What is a product cipher ?

   (d) What is CAST-128 ?

   (e) What is Euler's theorem ?

   (f) What are the roles of the public and private key ?

   (g) What are some approaches for producing message authentication ?

   (h) What basic arithmetic and logical functions are used in secure hash algorithm (SHA) ?

   (i) What are typical phases of operation of a virus or worm ?

   (j) What services are provided by IPSec ?

SECTION – B

2. Attempt any **three** parts : **3 × 10 = 30**

   (a) List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

   (b) Using Fermat's theorem, find $3^{201} \bmod 11$.

   (c) Describe characteristics that are needed in a secure hash function.

   (d) What is Pretty Good Privacy (PGP) ? What sequence of steps are performed for decrypting the received message in PGP ?

SECTION – C

Attempt any **five** questions : **5 × 10 = 50**

3. Compute the bits number 1, 16, 33 and 48 at the output of the first round of the DES decryption, assuming that the cipher text block is composed of all ones and the external key is composed of all ones.

4. Encrypt the message "meet me at the usual place at ten", using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.

5. Suppose Bob uses the RSA cryptosystem with a very large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (A $\rightarrow$ 0, ..., Z $\rightarrow$ 25) and then encrypting each number separately using RSA with large e and large n. Is this method secure ? If not, describe the most efficient attack against this encryption method.

6. Use Chinese Remainder Theorem to solve the following simultaneous congruence's :

   $X \equiv 1 \bmod 5, x \equiv 5 \bmod 8, x \equiv 3 \bmod 13$

7. Explain with block diagram the message authentication code technique. Describe how the message authentication code further provides confidentiality in data.

8. Explain the Digital Signature Algorithm.

9. Explain X.509 strong authentication procedures with block diagram.
