Printed Pages : 4

MCA-E14

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

PAPER ID : **214459**

Roll No. | | | | | | | | | | |

M. C. A.

(SEM. IV) THEORY EXAMINATION, 2014-15

CRYPTOGRAPHY & NETWORK SECURITY

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

Note : (1) Attempt ALL questions.
(2) All questions carry equal marks.
(3) Notation/Symbols/Abbreviations used have usual meaning.
(4) Make suitable assumption, wherever required.

1 Attempt any four parts of the following : 5×4=20

(a) Consider the diffie-Hellman scheme with a common-prime q=11 and primitive root α=2.

(i) Show that 2 is indeed a generator.

(ii) If the user A has public key Y_A=9 what is A's private key ?

(iii) If the user B has public key Y_B=3 what is the secrete key k in between A and B.

(b) Explain Blowfish in detail.

(c) Describe the principle of differential crypt analysis.

(d) Discuss the vulnerabilities of DES.

(e) Clearly explain the following terms :

(i) Message Integrity

(ii) Steganography

(iii) Masquerading

(iv) Passive Attack

(v) Stream Cipher.

(f) What is the difference between an substitution cipher and a permutation cipher ?

2 Attempt any four parts of the following : 5×4=20

(a) What is denial of service attack ?

(b) Briefly explain the following terms :

(i) Computationally secure cipher

(ii) Principle of confusion and diffusion

(iii) Active attack.

(iv) Authentication

(v) Avalanche effect

(c) What is Trojan Horse ? What is the principle behind it ?

(d) What is a permutation cipher ? Suggest an approach to break a permutation cipher assuming that sufficient amount of ciphertexts is available to the adversary.

(e) What is repudiation ? How can it be prevented in real life ?

(f) Hill Cipher is vulnerable to chosen plaintext attack. How ?

3 Attempt any two parts of the following : 10×2=20

(a) Write RSA algorithm if N = 187 and the encryption key E=17, find out the corresponding private key.

(b) (i) What do you understand by message authentication code (MAC) ? What are the requirements of a message authentication code ?

(ii) With DSS, if same message is signed at different occasions, the signatures of the message differ. Why ?

(c) What is birthday paradox ? Explain the birthday attack on a hash function with the help of suitable example.

4 Attempt any two parts of the following : 10×2=20

(a) What do you understand by digital certificate ? What is a chain of certificates ? How is a X.509 certificate revoked ?

(b) Describe the properties of a cryptographic hashing function. Clearly describe how a cryptographic hashing function can be implemented using a block cipher.

(c) What are the five principal services provided by Pretty Good Privacy (PGP) ? Explain the PGP message generation process. Why does PGP generate a signature before compression while message encryption is applied after compression ?

5 **Write short notes on any two of the following :** **10×2=20**

(a) SHA

(b) man-in-middle attack

(c) Brute force Attack