Printed Pages—4 **MCAE14**

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

PAPER ID : 1453 **Roll No.** □□□□□□□□□□

M.C.A.

(SEM. IV) THEORY EXAMINATION 2010-11

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note :— (1) Attempt **ALL** questions.

(2) All questions carry equal marks.

(3) Notations/Symbols/Abbreviations used have usual meaning.

(4) Make suitable assumptions, wherever required.

1. Attempt any **four** parts of the following :

(a) Briefly explain the following terms :

(i) Computationally secure cipher

(ii) Principle of confusion and diffusion

(iii) Active attack

(iv) Authentication

(v) Avalanche effect.

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

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

(d) Describe the encryption and decryption process of a block cipher in Output Feedback (OFB) mode.

(e) Answer following in context of DES cipher :

(i) What is the block size ?

(ii) What is the purpose of S-boxes and how many S-Boxes are there ?

(iii) What is the size of round keys ?

(iv) Is it possible that key schedule generated by one key is reverse of the key schedule generated by some other key ? Justify your answer.

(v) What is the importance of Initial permutation ?

(f) Determine the multiplicative inverse of 1234 mod 4321.

2. Attempt any **two** parts of the following :

(a) (i) What is Triple DES ? Why is the middle portion of Triple DES a decryption rather than an encryption ?

(ii) Draw the block diagram of single round of Blowfish cipher.

(b) (i) What are the criteria used for a pseudo random number generator ? In a linear congruential algorithm, why is the modulus 2^k-1 preferable to 2^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 :

(1) A generates a random number R and sends to the S his name A, destination B, and $E_{Ka}[R]$.

(2) S responds by sending $E_{Kb}[R]$ to A.

(3) A sends $E_R[m]$ together with $E_{Kb}[R]$ to B.

(4) B know Kb, thus decrypts $E_{Kb}[R]$ to get R and will subsequently use R to decrypt $E_R[m]$ to get m.

Analyze and comment on the security of the protocol.

(c) Describe the Diffie-Hellman protocol for distribution of secret key. Discuss how the protocol is vulnerable to Man-in-the-Middle attack.

3. Attempt any **four** parts of the following :

(a) State Chinese Remainder theorem. Use it to determine sum of x and y which are defined by following simultaneous congruences :

$$x \equiv 6 \bmod 7,\ x \equiv 7 \bmod 8,\ x \equiv 3 \bmod 9,$$

$$y \equiv 2 \bmod 7,\ y \equiv 2 \bmod 8,\ y \equiv 1 \bmod 9.$$

(b) Define Euler's totient function (Φ). State and prove Euler theorem. Determine the value of 2^{2011} mod 500.

(c) State Discrete Logarithm problem. Given that 2 is primitive root of 29. Determine all other primitive roots of 29.

(d) Describe RSA algorithm. Whether RSA encryption and decryption works or not if message m has common factor with the modulus n of the scheme. Justify your answer.

(e) Write Miller-Rabin algorithm for testing the primality of a number. Explain the basis of the algorithm.

(f) Define Group. Define cyclic group. Prove that if G is a group and $a \in G$ then order of a^{-1} is same as the order of a.

4. Attempt any **two** parts of the following :

(a) Answer following in context of digital signature algorithm of Digital Signature Standard :

(i) What are various global parameters of the algorithm and how are they decided ? Give reasons behind the decisions.

(ii) Describe signature generation and signature verification process.

(iii) What happens if the value of the parameter k (user's per message secret number) is compromised ? Explain.

(b) (i) What are the requirements for a Hash function ?

(ii) Compare the MD5 and SHA-1 hash algorithms.

(iii) Obtain the probability of collision of birthday in two classes, one with m students and the other with n students. Assume there are 365 days in a year.

(c) (i) In what order should the digital signature function and the confidentiality function be applied to a message, and why ?

(ii) How can a hash function be used to construct a block cipher with a structure similar to DES ? Discuss.

(iii) Suppose the message M consists of block M_1, M_2, M_n, each of 56 bit, in order. The 64 bit hash code of message M is given by G defined as follows :

$H_0 = C$ // 64 bit constant initial value

$H_i = DES_{Mi}[H_{i-1}]$ // DES encryption with M_i as key

$G = H_n$

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 has code.

5. Attempt any **two** parts of the following :

(a) (i) 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 ?

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

(b) (i) What is dual signature in context of Secure Electronic Transaction (SET). Describe the sequence of events that are required for a SET transaction.

(ii) What are different modes in which IPSec services can be used ? Discuss.

(c) Write short notes on any **one** of the following :

(i) Kerberos

(ii) Firewalls.