Printed Pages: 2

MCA-E21

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

MCA
(SEM V) ODD SEMESTER THEORY EXAMINATION, 2015-16
CRYPTOGRAPHY AND NETWORK SECURITY

Time: *3 Hours* ***Maximum 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.*

Q.1. *Attempt any **FOUR** parts of the following:* **5x4=20**

(a) Differentiate between the following clearly:
- **(i)** Block Cipher and Stream Cipher
- **(ii)** Masquerading and Replay
- **(iii)** Passive attack and Active Attack

(b) What is monoalphabetic substitution cipher? What are the security issues of such ciphers? Discuss.

(c) Given encryption key of a transposition cipher is **(7, 3, 2, 6, 4, 8, 1, 5)**. Find the decryption key.

(d) Hill Ciphers are vulnerable to chosen plaintext attacks. How? Illustrate with suitably chosen example.

(e) Draw block level diagram to one round of Data Encryption Standard (DES) encryption and explain key characteristics of DES cipher.

(f) What are various modes of operation of Block Cipher? Explain encryption and decryption process of anyone of them.

Q.2. *Attempt any **TWO** parts of the following:* **5x4=20**

(a) Define group. Show whether set of residue class modulo 21 with respect to multiplication modulo 21 is a group or not.

(b) Determine the value of Euler totient function **$\Phi(1600)$.**

(c) What is difference between S-Box of AES and S-Box of DES.

(d) Write Miller Rabin algorithm for testing primality of given number.

(e) Write and explain RSA public key cryptosystem.

(f) Given the following simultaneous congruence.

$$x \equiv 0 \bmod 7,\ x \equiv 1 \bmod 8,\ x \equiv 3 \bmod 9,$$

Use Chinese Remainder Theorem (CRT) to determine the value of **x**.

Q.3. *Attempt any **TWO** parts of the following:* **10x2=20**

(a) What are the properties that a digital signature should satisfy? Write signature generation process of digital signature algorithm of Digital Signature Standard (DSS).

(b) What is hash function? How it is different from message authentication code? In what way, a hash function is used to obtain message authentication code?

(c) Answer the following.

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

(ii) Consider the following hash function. Messages are in the form of a sequence of decimal numbers, $M=(a_1, a_2, \ldots\ldots, a_t)$. The hash value h is calculated as:

$$h = \left(\sum_{i=1}^{t} (a_i)^2 \right) \bmod n$$

For some predefined value n, does this hash function satisfy any of the requirements for a hash function? Explain your answer.

Q.4. *Attempt any **TWO** parts of the following*: **10x2=20**

(a) Consider a Diffie-Hellman key exchange with a common prime **p = 11** and primitive root **a = 2**. The public keys of user A and B are **9** and **3** respectively. What are the private keys of A and B.? What is the shared secret key **K**?

(b) What are the five principal services provided by PGP. Give general format of a PGP message and explain why does PGP generate a signature before applying compression?

(c) What is X.509 certificate? How is a X.509 certificate issued, maintained and revoked? Describe.

Q.5. *Write short notes on any **TWO** parts of the following:* **10x2=20**

(a) Use of Dual Signature in SET
(b) Modes of IPSec
(c) Firewals