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

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

B.TECH.

Theory Examination (Semester-VIII) 2015-16

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours ***Max. Marks : 100***

Note : Attempt questions from all Sections as per directions.

Section-A

Attempt all parts of this section. Answer in brief.

(2×10=20)

Q1. (a) Find gcd (1970, 1066) using Euclid's algorithm?

(b) Using Row Transposition technique & given key as "2 5 4 1 3" generate the Cipher Text for the following plain text "a convenient way to express the transposition".

(c) Perform encryption and decryption using RSA Algorithm for the following.

P=7; q=l1; e=17; M=8.

(d) What are the design parameters of Feistel cipher network?

(e) Using Playfair technique, encrypt the following message "send more money" using the key - "tarun".

(f) What is the difference between Shift Rows and Rot Word?

(g) Briefly describe Add Round Key.

(h) What are the two problems with one-time pad?

(i) Deline the classes of message authentication function.

(j) Explain in brief Symmetric and Asymmetric cryptography.

Section-B

2. Attempt any five questions from this section. (10×5=50)

(a) If n is composite and passes the Miller-Rabin (MR) primarily test for the base a. then n is called strong pseudo prime to the base a. Show that 2047 is strong pseudo prime to the base 2.

(b) What do you mean by Security Association? Specify the parameters that identify the Security Association? Explain man in the middle attack?

(c) What is the key algorithms used in S/MIME? What are the headers fields define in MME?

(d) Differentiate MAC and Hash function. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?

(e) What is message authentication code? How it differs from hash function? What are the requirements of hash function? Suggest at least one scheme to show that symmetric encryption algorithm can also be used to generate message authentication code.

(f) Compare and contrast a conventional ink based signature and a digital signature. Describe the Elgamal scheme of digital signature generation and verification. Why do signatures of the same message, signed on different occasions differ?

(g) (i) Explain the Chinese Remainder Theorem. Use it to solve: X=2 mod 3, X=3 mod 5 and X=2 mod 7.

(ii) State and prove Fermat's theorem.

(h) Why do we use X.509 authentication over PKC based authentication. Also explain the format of X.509 and how is an X.509 certificate revoked?

Section-C

Attempt any two questions from this section. (15×2=30)

3. Discuss symmetric key distribution. Also describe Diffie-Hellman Key exchange algorithm. Consider the Diffie-Hellman scheme with common prime number q=7l and primitive root a=7 :

   (a) If user A has a private key X_a=5, what is A's public key.

   (b) If the user A has private key X_b=9 then what is B's public key?

   (c) What is shared key?

4. What is DSS? Explain the two approaches of DSS. Also differentiate between ink based signature and digital signature. Explain DSA algorithm.

5. Explain the following:

   (i) ICMP

   (ii) IGMP

   (iii) ARP

   (iv) FDDI