Printed pages: 02 **Sub Code: NIT 701**

Paper Id: | 1 | 0 | 5 | 3 | **Roll No.** | | | | | | | | | | |

B.TECH.
(SEM VII) THEORY EXAMINATION 2017-18
CRYPTOGRAPHY & NETWORK SECURITY

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

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. 2 x10 = 20

a. Find GCD(1970, 1066) by using Euclid's Algorithm.
b. What are the different factors on which Cryptography depends?
c. Compute the value of 5^{17} mod 11 & 11^{17} mod 5.
d. Find the value of Euler's Totient Number $\phi(88)$.
e. What is Cryptanalysis?
f. Discuss Linear and Differential cryptanalysis.
g. What is Birthday Attack?
h. Discuss Double & Triple DES.
i. Discuss Group & Ring with suitable axioms.
j. What is Security Attack? Discus it's various types.

SECTION B

2. Attempt any *three* of the following: 10 x 3 = 30

a. How E-Mail security is achieved? Discuss S/MIME with suitable steps & block diagram.
b. Discuss DES in detail with suitable block diagram.
c. Discuss MD-5 Algorithm with all required steps and suitable block diagram.
d. Describe IDEA encryption and decryption in brief. Also explain. How can we generate cryptographically secure pseudorandom numbers?
e. What do you understand by Elgamel encryption system? Explain its encryption and decryption?

SECTION C

3. Attempt any *one* part of the following: 10 x 1 = 10

(a) Explain Digital Signature. Discuss signing & verifying process of Digital Signature Algorithm (DSA) in detail with suitable steps.
(b) Discuss X.509 digital certificate format. What is its significance in cryptography?

4. Attempt any one parts of the following: 10 x 1 = 10

(a) Why Message Authentication is required? Discuss working of MAC with suitable block diagram. Also discuss HMAC & CMAC in detail.
(b) What is Hash Function? Discuss SHA- 512 with all required steps, round function & block diagram.

5. Attempt any one parts of the following: 5 x 2 = 10

(a) Discuss Diffie Hellman key exchange method. Let q = 353, α=3, X_A= 97 and X_B = 233. Then Compute Y_A,Y_B,K_A& K_B using Diffie Hellman.
(b) Discuss Public Key Cryptosystem. Explain RSA algorithm with suitable steps. Let p= 17, q=11, e=7 and d=23. Calculate the public key & private key and

show encryption and decryption for plain text M= 88 by using RSA algorithm.

(c) What do you understand by Chinese Remainder Theorem? Solve the following congruent equations by Chinese remainder theorem:
i. X ≡ 2 mod 3
ii. X ≡ 3 mod 5

6. Attempt any *two* part of the following: 5 x 2 = 10

(a) Explain Finite field of the form GF (p) & GF (2^n) with suitable example.

(b) What is Block Cipher? Discuss Block Cipher Mode of Operations.

(c) What do you understand by Feistel cipher structure? Explain with suitable block diagram.

7. Attempt any *one* part of the following: 10 x 1 = 10

(a) What is Kerberos? Discuss Kerberos version 4 in detail.

(b) Write short note on the following:
i. SET
ii. Intrusion Detection
iii. Firewall
iv. AES