

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 x 10 = 20**
- Find GCD(1970, 1066) by using Euclid's Algorithm.
 - What are the different factors on which Cryptography depends?
 - Compute the value of $5^{17} \bmod 11$ & $11^{17} \bmod 5$.
 - Find the value of Euler's Totient Number $\phi(88)$.
 - What is Cryptanalysis?
 - Discuss Linear and Differential cryptanalysis.
 - What is Birthday Attack?
 - Discuss Double & Triple DES.
 - Discuss Group & Ring with suitable axioms.
 - What is Security Attack? Discuss its various types.

SECTION B

- 2. Attempt any three of the following: 10 x 3 = 30**
- How E-Mail security is achieved? Discuss S/MIME with suitable steps & block diagram.
 - Discuss DES in detail with suitable block diagram.
 - Discuss MD-5 Algorithm with all required steps and suitable block diagram.
 - Describe IDEA encryption and decryption in brief. Also explain. How can we generate cryptographically secure pseudorandom numbers?
 - 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**
- Explain Digital Signature. Discuss signing & verifying process of Digital Signature Algorithm (DSA) in detail with suitable steps.
 - Discuss X.509 digital certificate format. What is its significance in cryptography?
- 4. Attempt any one parts of the following: 10 x 1 = 10**
- Why Message Authentication is required? Discuss working of MAC with suitable block diagram. Also discuss HMAC & CMAC in detail.
 - 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**
- Discuss Diffie Hellman key exchange method. Let $q = 353$, $\alpha = 3$, $X_A = 97$ and $X_B = 233$. Then Compute Y_A, Y_B, K_A & K_B using Diffie Hellman.
 - 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~~

- (c) What do you understand by Chinese Remainder Theorem? Solve the following congruent equations by Chinese remainder theorem:
- $X \equiv 2 \pmod{3}$
 - $X \equiv 3 \pmod{5}$

6. Attempt any *two* part of the following:

5 x 2 = 10

- Explain Finite field of the form $GF(p)$ & $GF(2^n)$ with suitable example.
- What is Block Cipher? Discuss Block Cipher Mode of Operations.
- 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

- What is Kerberos? Discuss Kerberos version 4 in detail.
- Write short note on the following:
 - SET
 - Intrusion Detection
 - Firewall
 - AES