Candidate Seat No…………

CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

Sixth Semester of B. Tech (IT/CE) Examination

May 2018

IT306.02/IT306.01/IT306 Cryptography & Network Security

Date: 03.05.2018, Thursday **Time: 10:00 a.m. To 01:00 p.m.** **Maximum Marks: 70**

Instructions:

1. The question paper comprises two sections.
2. Section I and II must be attempted in separate answer sheets.
3. Make suitable assumptions and draw neat figures wherever required.
4. Use of scientific calculator is allowed.

SECTION – I

Q.1 Answer the question below. **[07]**

1. gcd(19,-5) and gcd (-19,5) are ___ and ____ respectively.

2. $\phi(187)$ = ________

3. 8^{-1} mod 17 = _________

4. 101^{17} mod 17 = _________

5. 71^{-1} mod 100 = _________

6. Find out whether 09 is a Quadratic Residue in Z_{11}*or not.

7. Diffie-Hellman key exchange protocol is based on ________.

Q.2 Attempt the following: **[14]**

a) Find an integer that has a remainder of 3 when divide by 7 and 13 & it is divisible by 12. [04]

b) Write a short note on MDC and MAC. [05]

c) Alice uses bob's RSA public key (e=7, n=143) to send some plaintext encrypted as ciphertext c=57. Show how eve can apply chosen ciphertext attack on given data. (Eve will choose random number x=17). [05]

OR

Q.2 Attempt the following: **[14]**

a) In SHA-512, we apply the conditional function on buffers E, F & G. If the left most hexadecimal digits of these buffers are 0x9, 0xA and 0xF, respectively, What is the left most digit of the result? [04]

b) What are the services provided by Digital Signature? Explain in detail. [05]

c) Given super-increasing tuple b= [7, 11, 19, 39, 79, 157, 313], r=37 and n=900. Encrypt the letter "g" using Knapsack cryptosystem. Use [4, 2, 5, 3, 1, 7, 6] as a permutation table. [05]

Q.3 Attempt the following: **[14]**

a) Use the Vigenere cipher with keyword "HEALTH" to encipher the message "Life is full of surprises". [04]

b) Write a short note on X.509 certificate revocation format. [05]

c) Using RSA digital signature scheme generate and verify digital signature for the following data: p=7, q=17, e=5, m=19 [05]

OR

Q.3 Attempt the following: **[14]**

a) In the Diffie-Hellman protocol, g=7, p=23,x=3 and y=5. What are the values of R1 and R2 & symmetric key? [04]

b) Show whether the number 201 passes the Miller-Rabin test or not. (Use base=2) [05]

c) In Elgamal encrypt and decrypt the message x=7. Use p=11, generator α=2, secret key a= 5 and random number k=4. [05]

SECTION – II

Q.4 Answer the question below. **[07]**

1. PGP can encrypt data by using a block cipher called _______ [01]
2. Greatest Common Divisor of 2024 and 748 is____________ [01]
3. What is the number of padding bits if the length of the original message is 2590 bits in SHA-512? [01]
4. Key domain of affine cipher ______ in Z_{26}. [01]
5. The encryption in the transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key. [01]
6. The input/output relation based on the given 2*2 S-box. Show the table for the inverse of S-box. [02]

S-Box	0	1
0	01	11
1	10	00

Q.5 Attempt the following: **[14]**

a) How many transformations are there in each version of AES? How many round keys are needed for each version? Fill data for the following table: [03]

AES Version	Number of Rounds	Number of Round Keys	Number of Transformations
AES-128			
AES-192			
AES-256			

b) Explain single round of DES with figure. [05]

c) Encrypt the message using Playfair cipher “The house is being sold tonight” with the key “MONARCHY”. [06]

OR

Q.5 Attempt the following: [14]

a) Write a short note on firewall. [04]

b) Write a short on encapsulating security payload (ESP). [05]

c) Explain Electronic codebook (ECB) mode and Counter (CTR) mode. [05]

Q.6 Attempt the following: [14]

a) Discuss the electronic mail system. [04]

b) Perform cryptanalysis on the given cipher text using column transposition. “ETTHEAKIMAOTYCNZNTSG” [05]

c) Write a short note on security services. [05]

OR

Q.6 Attempt the following: [14]

a) Calculate Mix column example of AES for the given data. [04]

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ ?? \\ e5 \end{bmatrix}$$

b) Perform 1st round encryption of following Plaintext (P) = 01011010 using Cipher key (K) =0101101010. [10]

Initial Permutation: 2 6 3 1 4 8 5 7 Straight P-Box= 3 5 2 7 4 10 1 9 8 6

Compression P-Box = 6 3 7 4 8 5 10 9 Expansion P-box(E/P8): 4 1 2 3 2 3 4 1

Straight P-box(P4): 2 4 3 1

S0	**0**	**1**	**2**	**3**
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S1	**0**	**1**	**2**	**3**
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

******