B.Tech. (Computer Engg.) VIIIth Semester Examination, 2021
Network Security
Paper No. CEN-805

Time: Three Hours **Maximum Marks: 60**

Write your roll no. immediately on receipt of this question paper

Note: Attempt all question. All questions carry equal marks. Assume suitable missing data, if any.

Q.No./CO's No.	Content of Questions	Marks
1. (a)/ CO1	Using the Extended Euclidean algorithm, find the greatest common divisor and the value of s and t for the given values 84 and 320.	**6**
1. (b)/ CO1	Find the solutions for the following linear equations: i. $256x \equiv 442 \pmod{60}$ ii. $232x+42 \equiv 248 \pmod{50}$	**6**
	OR	
1'. (a)/ CO1	For a defined Galois Field over GF (2^8) having 8 elements. Using Extended Euclidean algorithm, find the inverse of (x^5) modulo $x^8 + x^4 + x^3 + x + 1$.	**6**
1'. (b)/ CO1	Find the determinant and multiplicative invers of the following residue matrix over Z_{10}. $\begin{pmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{pmatrix}$	**6**
2. (a)/ CO2	Show the following hexadecimal data: AAAA BBBB CCCC DDDD after passing it through initial permutation and inverse initial permutation in DES.	**6**
2. (b)/ CO2	Find the value of RCon [11] and RCon[12] constants for the AES-192 and the value of RCon [13] and RCon[14] for AES-256 implementations. Use X^{11-1} mod prime and X^{12-1} mod prime, in which the prime is the irreducible polynomial ($X^8 + X^4 + X^3 + X + 1$) for AES 192 and use X^{13-1} mod prime and X^{14-1} mod prime, in which the prime is the irreducible polynomial ($X^8 + X^4 + X^3 + X + 1$) for AES 256	**6**
	OR	
2'. (a)/ CO2	Find the order of elements and primitive roots of $a^i \equiv x \pmod 7$ defined for the group $G = <Z_7^*, x)$.	**6**
2'. (b)/ CO2	Find the value of x for the following sets of congruence using the Chinese remainder Theorem. $X \equiv 6 \pmod{11}$ $X \equiv 13 \pmod{16}$ $X \equiv 9 \pmod{21}$ $X \equiv 19 \pmod{25}$	**6**

3. (a)/ CO3	Assume an attacker knows that m=3, he has intercepted three plain text/cipher text blocks from the same message as shown below: [05 07 10] <------> [03 06 00] [13 17 07] <------> [14 16 09] [05 00 04] <------> [03 17 11] Find the value of matrix for key k using Hill ciphering technique.	**6**
3. (b)/ CO3	Assume an attacker intercepts the cipher text " EEMYNTAACTTKONSHITZG" using Brute-Force attack. Find the original message using Transposition ciphering method.	**6**
4. (a)/ CO4	Using the value of p=23 and q=29, for RSA: i. Find the value of public key. ii. Find the value of private key. iii. Encrypt the message "attack" using the key pair calculated in part i.	**6**
4. (b)/ CO4	Two points on the elliptical curve $E_{23}(1,1)$ is defines as P= (3,10) and Q= (9,7), find the value of: (i) P+Q (ii) 4P	**6**
5. (a)/ CO5	If the ASCII Character "COMPUTERENGINEERING" is passed as a message to the SHA-512 as input, find the values in HEX assigned to the words W0, W1, W2, ----------W15 for the defined message. (Use ASCII code for A: 01000001, B: 01000010, C: 01000011----------).	**6**
5. (b)/ CO5	i. If the size of the message is 1000 bits in MD5, What will be the size of padding bits? ii. Write the value of chaining variables used in MD5.	**6**