B.Tech. (Computer Engg.) VIIIth Semester Examination, 2017

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.	**Statements of the Questions**	**Marks**
1. (a)/ CO1	Find multiplicative inverse of $(x^3 + x + 1)$ in $GF(2^4)$ with the modulus $(x^4 + x + 1)$ using Extended Euclidean algorithm.	**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**
	OR	
1'. (a)/ CO1	Solve the following equation to find the value of x, y and z. $3x + 5y + 7z \equiv 3 \pmod{16}$ $x + 4y + 13z \equiv 5 \pmod{16}$ $2x + 7y + 3z \equiv 4 \pmod{16}$	**6**
1'. (b)/ CO1	) Find the results of the following. **(i)** $5X^{12} + 6X \equiv 8 \bmod 23$ **(ii)** $320^{23} \bmod 461$	**6**
2. (a)/ CO2	What is IDEA? Explain the sub key generation process for each round of IDEA.	**6**
2. (b)/ CO2	Show the following hexadecimal data: AAAA BBBB CCCC DDDD after passing it through initial permutation and inverse initial permutation in DES.	**6**
3. (a)/ CO3	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	**6**

	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	
3. (b)/ CO3	Explain about the functioning of one iteration and compression function used in SHA-512.	**6**
4. (a)/ CO4	Consider an ElGamal cryptosystem with a common prime q= 71 and a primitive root α= 7. **i.** If B has public key Y_B = 3 and A choose the random integer k= 2, what is the cipher text for M=30? **ii.** If A now chooses a different value of k so that the encoding of M= 30 is C= (59, C_2), What is the value of C_2?	**6**
4. (b)/ CO4	Given the super-increasing tuple b= [7,11,23,43,87,173,357], and modulus n= 1001, Encrypt and decrypt the letter "b" using the knapsack cryptosystem. Use [7 6 5 1 2 3 4] as the permutation table and 7-bit representation of character "b" as [1, 1, 0, 0, 0, 1, 0].	**6**
	OR	
4'. (a)/ CO4	In the elliptical curve E(g^4,1) over the GF(2^4) field, over the irreducible polynomial is $x^4 + x + 1$. **i.** Find the equation of the curve. **ii.** Find any six points on the curve. **iii.** Generate the pair of public key and private key. (Choose $e1 = (g^3, g^8)$ and $d = 2$.)	**6**
4'. (b)/ CO4	Suppose that user A has to sign the hash value of the message H = 99; with the private key k = 87 and the ephemeral key as x = 101 and g = 3, q = 119 as primitive element in Z_{239}. Calculate A's signature and also verify the signature using DSA digital signature scheme.	**6**
5. (a)/ CO5	List the name of all seven types of packet used in PGP. Explain about any two of them.	**6**
5. (b)/ CO5	What is Blind Digital signature? Explain the blind digital signature generation and verification process using RSA.	**6**