B.Tech. (Computer Engg.) VIIIth Semester Examination, 2018
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.

CO's No./ Q.No.	**Content of Questions**	**Marks**
1. (a)/ CO1	Find the value of 2001^{35} mod 1980 using square and multiply method.	**6**
1. (b)/ CO1	Generate the elements of the field GF(2^4) using the irreducible polynomial $f(x) = x^4 + x + 1$. Also find the value of g^3/ g^8.	**6**
	OR	
1'. (a)/ CO1	Find the output of Shift rows of the AES after passing the following states as input to the Shift rows**:** $\begin{pmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{pmatrix}$	**6**
1'. (b)/ CO1	Solve the following simultaneous congruence using Chinese Remainder Theorem. $x \equiv 6 \pmod{11}$ $x \equiv 13 \pmod{16}$ $x \equiv 9 \pmod{21}$ $x \equiv 19 \pmod{25}$	**6**
2. (a)/ CO2	For the chosen value of p= 11, e1= 2, d= 3 and r= 4. Find the set of the values of public and private keys and then encrypt the plain text 7 using ElGamal cryptosystem.	**6**
2. (b)/ CO2	An elliptic curve is defined by $y^2 = x^3 + 2x + 9$ with a modulus of p=37 for the Elliptical curve cryptosystem. Determine any four points on this curve excluding infinite.	**6**
	OR	
2'. (a)/	Explain the procedure of Digital signature generation and verification	**6**

CO2	using Schnorr Digital Signature scheme.	
2’. (b)/ CO2	An elliptical curve over GF(2^3) is defined as $y^2 + xy = x^3 + ax^2 + b$ with the given value of a= g^3 and b=1. Find the value of R = P + Q, where P = (0, 1) and Q = (g^2, 1).	**6**
3. (a)/ CO3	i. For SHA-512, show the equation for the values of W_{16} and W_{19} . ii. Find the value of padding field and the value of length field if the length of the message is 1920 bits in SHA-512.	**6**
3. (b)/ CO3	How many rounds and iterations are required for hash generation in MD5? Explain about one of the rounds of MD5 in detail.	**6**
4. (a)/ CO4	What is zero knowledge authentication? Explain the Fiat-Shamir protocol used for zero knowledge authentications.	**6**
4. (b)/ CO4	In the Diffie-Hellman protocol key exchange, for g=7, p=23, x=3 and y=5: calculate i. The value of R1 and R2. ii. The value of symmetric key.	**6**
5. (a)/ CO5	Write the procedure of generation of pre-master and master secret for the Secure Socket Layer.	**6**
5. (b)/ CO5	Encode the message “WHAT IS A TEXT” using the Radix 64 encoding scheme used in PGP.	**6**