B.Tech. (Computer Engg.) VIIIth Semester Examination, 2016
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	Explain about the various types of active and passive attacks on the network in detail. Find the result of multiplying $P_1 = (X^5 + X^2 + X)$ by $P_2 = (X^7 + X^4 + X^3 + X^2 + X)$ in GF(2^8) with irreducible polynomial $(X^8 + X^4 + X + 1)$.	**6**
1. (b)/ CO1	Find the value of the following (Use the method of your own choice) i. $44^{-1} \bmod 667$ ii. $17364^{41} \bmod 2134$	**6**
2. (a)/ CO2	Explain how attackers uses the following methods to attack in the network: (i) Packet sniffing (ii) Packet spoofing (iii) DNS spoofing	**6**
2. (b)/ CO2	Find the result of multiplying $P_1 = (X^5 + X^2 + X)$ by $P_2 = (X^7 + X^4 + X^3 + X^2 + X)$ in GF(2^8) with irreducible polynomial $(X^8 + X^4 + X + 1)$.	**6**
	OR	
2. (b')/ CO2	If the value of X is defines as follows: $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$. Find the suitable value of X to satisfy the above equation using Chinese Remainder Theorem.	**6**
3. (a)/ CO3	Find the order of elements and primitive roots of $a^i \equiv x \pmod 7$ defined for the group $G = \langle Z_7^*, x \rangle$.	**6**
3. (b)/ CO3	Two points on the elliptical curve $E_{23}(1,1)$ is defines as P= (3,10) and	**6**

	Q= (9,7), find the value of: (i) P+Q (ii) 2P	
	OR	
3. (b')/ CO3	What are the four different stages used in the Round 1 of the AES? Explain your answer with example for all the stages.	**6**
4. (a)/ CO4	What is digital signature? Explain the mechanism of generation of digital signature using Schnorr digital signature technique.	**6**
4. (b)/ CO4	For what purpose the Message Digest is used? Explain the process of padding and chaining variables used in SHA-1.	**6**
	OR	
4. (b')/ CO4	How dual signature is generated in SET? Also explain the procedure of verification of dual signature by merchant in SET.	**6**
5. (a)/ CO5	What is the different function block of PGP? Explain about the general packet structure of PGP.	**6**
5. (b)/ CO5	How the security is preserved in web service using SSL? Briefly describe about the Hand shake protocol of SSL.	**6**
	OR	
5. (b')/ CO5	What is digital certificate? Explain about the X.509 digital certificate model in detail.	**6**