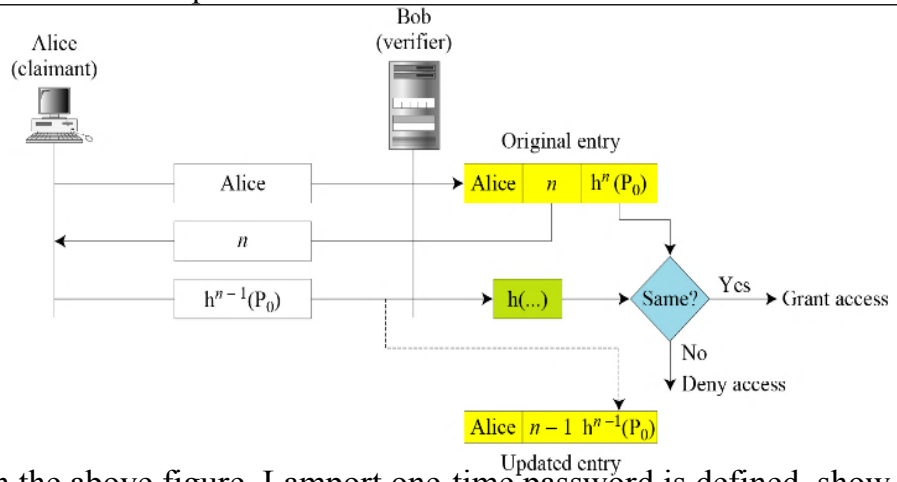
B.Tech. (Computer Engg.) VIIIth Semester Examination, 2019
Network Security
Paper No. CEN-805

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 Questions	Marks
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	Using Miller Rabin Primality Test, find the number 341 is prime or not.	**6**
	OR	
1'. (a)/ CO1	Using the properties of Discrete logarithms, find the value of $2X^{11} \equiv 22 \bmod 19$.	**6**
1'. (b)/ CO1	What are the different types of security services and security mechanisms used to provide network security?	**6**
2. (a)/ CO2	If the plain text in ASCII "COMPUTER" is supplied as input to the DES, what is the initial and inverse initial permutation of this Plain text? (Use the code for ASCII as: C: 01000011, O: 01001111, M: 01001101, P: 01010000, U: 01010101, T: 01010100, E: 01000101, R: 01010010)	**6**
2. (b)/ CO2	Jenifer creates a pair of keys for herself. She chooses p= 397 and q= 401. She calculates φ(n)= 158400. She choose e= 343 and d= 12007. Show how Ted can send a message "NO" to Jenifer if she knows e and n using RSA Cryptographic method. (Use positional value for N= 13 and O= 14)	**6**
	OR	
2'. (a)/ CO2	If the value of first, second, third and fourth words in the round of AES is given as W_{00}= 2475A2B3, W_{01}= 34755688, W_{02}= 31E21200 and W_{03}= 13AA5487. Find the value of temporary word (t) used for the round number 1.	**6**
2'. (b)/ CO2	Write the procedure for creation of digital signature and its verification by using Schnorr Digital signature scheme.	**6**
3. (a)/ CO3	If the ASCII Character "ENGG" 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 E: 01000101, N: 01001110 and G: 01000111).	**6**

3. (b)/ CO3	Explain the following with respect to MD5: i. Function to generate temporary constant ii. Values of chaining variables. iii. Compression function	**6**
4. (a)/ CO4	 In the above figure, Lamport one-time password is defined, show two more exchanges of the authentication procedure in the above OTP method.	**6**
4. (b)/ CO4	What is Kerberos? Explain the various types of the servers used in Kerberos.	**6**
5. (a)/ CO5	How security is provided by following two security protocols in IPSec? i. Authentication Header ii. Encapsulating Security Payload	**6**
5. (b)/ CO5	How the security is preserved in web service using SSL? Briefly describe about the Hand shake protocol of SSL.	**6**