USN

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute Affiliated to VTU, Belagavi)

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Department of Telecommunication Engineering

Continuous Internal Assessment Test - II

Course: **Cryptography and Network security** **Date: 11/11/2020**
Course Code**: 17TE7DECNS** Maximum marks: **50**
Semester: **VII** Duration: **90 Min**

	Note: Answer 5 full questions.	**Marks**
(a)	AES uses a ____________ bit block size and a key size of __________bits. i) 128; 128 or 256 iii) 64; 128 or 192 ii) 256; 128, 192, or 256 iv) 128; 128, 192, or 256	1x10
(b)	confusion is created by i) Permutation iii) Expansion ii) Substitution iv) Contraction	
(c)	DES follows i) Hash Algorithm iii) Key exchange algorithm ii) Feistel Cipher Structure iv) SP Networks	
(d)	Euler's totient is used to find i) Positive integers of Relative prime iii) Reminder ii) Co factor iv) Prime root	
(e)	Euclid's algorithm, is an efficient method for computing the i) Prime numbers iii) Greatest common divisor ii) Co-prime iv) Prime root	
(f)	The S-Box is used to provide confusion, as it is dependent on the unknown key. i) Diffusion iii) Expansion iii) Confusion iv) Contraction	
(g)	Which one of the following modes of operation in DES is used for operating short data? i) CFB ii) OFB iii) CBC iv) ECB	
(h)	Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not i) Authenticated ii) Joined iii) Submit iv) Separate	
(i)	Which of the following is not a DES operating mode? i) ECB ii) CFB iii) CBF iv) CBC	
(j)	n = 35; e = 5; C = 10. What is the plaintext? i) 3 ii) 7 iii) 8 iv) 5	
2	If 8 bit of plaintext is **10010101** and two sub keys are **K_1=1 0 1 0 0 1 0 0** and **K_2= 0 1 0 0 0 0 1 1,** Determine the cipher text using **S-DES.**	10
3	In Diffie-Hellman key exchange, q=11, A's private key is 4, B's private key is 7.Determine i) A's public key ii) B's Public key iii) Shared secret key.	10
4	With a neat block diagram in detail discuss about different operations used in AES encryption and decryption	10
	OR	
5	In detail discuss each steps used in RSA algorithm. In RSA algorithm system it is given that p=5, q= 13, e=7 and m=14. Find the cipher text "C" and decrypt "C" to set plain text M	10

6	a) What is the difference between diffusion and confusion? b) With neat diagram and example discuss operation of the S-boxes in function F of DES?	4 6
	OR	
7	With neat block diagram illustrate all the possible ways of distribution of public key	10