Question Paper

Exam Date & Time: 10-Oct-2020 (09:30 AM - 01:00 PM)

BMS COLLEGE OF ENGINEERING

Autonomous Institute Affiliated to VTU, Supplementary Semester End Examinations October 2020

Cryptography and Network Security [16CS6DECNS]

Marks: 100 **Duration: 210 mins.**

Semester : VI - Computer Science And Engineering

Answer all the questions.

Instructions: 1. Answer FIVE full questions, using the given internal choices. 2. Missing data, if any, may be suitably assumed.

1)		State the security mechanisms recommended by ITU-T(X-800) for providing security services	(8)
	a)		
	b)	Given =84 and b=33, find GCD(a, b) and the values of 's' and 't' using Extended Euclidean algorithm	(6)
	c)	Determine whether the number 561 passes the Miller-Rabin test.	(6)
[OR]		State Non-Cryptanalytic attacks.	(6)
2)			
	a)		
	b)	Find the particular and general solutions to the equation 72x+56y=40	(8)
	c)	Find the solution to the set of equations using Chinese Remainder theorem : $x \equiv 3 \bmod 4$ $x \equiv 2 \bmod 3$ $x \equiv 4 \bmod 5$	(6)
3)		Using Affine cipher, encrypt the message " l u g m v" with the key pair (7, 2)	(6)
	a)		
	b)	Bob receives the cipher text "CTRPOEAETTHCSRAVLY", Bob decides to divide the cipher text into 6 characters group and then permute the characters in each group. Determine the plaintext and key used for encryption and decryption.	(8)
	c)	Describe diffusion and confusion.	(6)
[OR]		Encipher the message "ATTACKATDAWN" using Auto key cipher with initial key value (K1)=12	(6)
4)			
	a)		
	b)	Encrypt the message "GEKH" using Playfair cipher. The letters in the matrix are dropped diagonally starting from top-right hand corner.	(6)
	c)	Show that a straight D-box is invertible	(8)
5)		With a neat diagram explain structure of DES	(6)

	a)		
	b)	"Cipher keys used in DES have weaknesses". State and explain each weakness.	(8)
	c)	With a neat diagram show that Cipher FeedBack mode can be used as a stream cipher.	(6)
6)		Describe key generation in RSA cryptosystem.	(8)
	a)		
	b)	With a neat diagram explain the creation of message digest in SHA-512.	(6)
	c)	State and explain the possible attacks on digital signature.	(6)
7)		Categorize passive and active attacks.	(6)
	a)		
	b)	What will be the pattern of the cipher text in the following cases, if One-Time Pad cipher is used? (i) The plain text is made of alternating 0's and 1's (ii) The plain text is made of n 0's	(4)
	c)	State two desired properties of a block cipher.	(4)
	d)	State the criterion that cryptographic hash functions need to satisfy	(6)

-----End-----