B.M.S. COLLEGE OF ENGINEERING,BANGALORE-19

Computer Science & Engineering

INTERNALS-1

Course Code: 20CS6PCCNS	**Course Title: Cryptography and Network Security**	
Semester: VI	**Maximum Marks: 40**	**Date: 16-05-2022**
Faculty Handling the Course:	Dr. Nandhini Vineeth, Prof. Namratha M, Prof. Lohith J J, Dr. Manjunath D R	

Instructions:* *Internal choice provided in Part C.

PART-A

Total 5 Marks (No Choice)

No.	**Question**	Marks
1	Demonstrate the encryption and decryption process in Feistel cipher with a neat figure.	5

PART-B

Total 15 Marks (No Choice)

No.	**Question**	**Marks**
2 a)	Consider the plaintext “an exercise”. Encrypt using the affine cipher. Use keys multiplicative key=15 and additive key =20	5
2 b)	A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks. Explain.	5
2 c)	Alice often needs to encipher plaintext made of both letters (a to z) and digits (0 to 9). a. If she uses an additive cipher, what is the key domain? What is the modulus? b. If she uses a multiplication cipher, what is the key domain? What is the modulus? c. If she uses an affine cipher, what is the key domain? What is the modulus?	5

PART- C

Total 20 Marks

No.	**Question**	**Marks**
3 a)	Multiply the following n-bit words using polynomials. (11100) × (10000) using both polynomial and binary algorithms in GF(2^4). Use ($x^5 + x^2 + 1$) as modulus.	10

OR

3 b)

i) Apply Playfair cipher to encrypt the text “Cryptanalysis is to break ciphers” using the key given below. 10

	1	**2**	**3**	**4**	**5**
1	z	q	p	f	e
2	y	r	o	g	d
3	x	s	n	h	c
4	w	t	m	i / j	b
5	v	u	l	k	a

ii) The ciphertext GEZXDS was encrypted by a Hill cipher with a 2 × 2 matrix. The plaintext is ‘solved’. Find the key matrix.

4a)

i) Use cryptanalysis, to decipher the following message. Assume that you know it is an affine cipher and that the plaintext “ab” is enciphered to “GL”. 10

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

ii) Use the extended Euclidean algorithm to find the inverse of ($x^4 + x^3 + 1$) in GF(2^5) using the modulus ($x^5 + x^2 + 1$).

OR

4b)

i) Prove that the group G = <Z_{10},*> is a cyclic group with two generators, g = 3 and g = 7. 10

ii) Consider the plaintext = "Cryptography and Network Security" (ignore spaces) and the encryption key (3, 2, 6, 1, 5, 4). Find the decryption key and the cipher text.

ALL THE BEST