GITA AUTONOMOUS COLLEGE, BHUBANESWAR

(Affiliated to BPUT, Odisha)

7th SemesterB.TechMid-Term Examination - 2023

Subject:Cryptography and Network Security

Branch:CSEAI, CSEDS

Time:2 Hours

FullMarks:25

Instructions:

Answer question No. 1 (Part I) any eight out of 10 bits, from (Part II) anythree out of 5 bits and any two from (Part III) out of 3bits.

The figures in the right-hand margin indicate marks

		Part – I	Marks			
01		**Short Answer Type Questions (Answer any eight out of ten)**	**(01 x 8)**	**BL**	**CO**	**PO / PSO**
	a)	Define symmetric key cipher.		1	1	1
	b)	Write difference between substitution and transposition cipher.		1	1	4
	c)	What are the differences between poly-alphabetic and mono-alphabetic cipher?		2	1	4
	d)	List four kind of cryptanalysis attacks.		1	1	9
	e)	State the Euler's Theorem.		2	2	1
	f)	Write the elements of Z_{25} and Z^*_{25}		2	2	1
	g)	Explain Denial of service.		1	1	8
	h)	Find the value of $\varphi(144)$ using Euler's Phi function.		1	2	1
	i)	Write the addition and multiplication table of Z_6		2	1	1
	j)	What is Non repudiation?		1	1	8

		Part – II	Marks			
02		**Focussed – Short answer type Questions (Answer any three out of five)**	**(03 x 03)**	**BL**	**CO**	**PO / PSO**
	a)	Why is asymmetric cryptography bad for huge data? Specify the reason?		1	1	1
	b)	Convert the given Text "COMPUTERSCIENCE" into cipher text using Rail fence Technique.		2	2	2
	c)	Encrypt the plaintext "follow the second route" with given secret key "DANCE" by using vigenere cipher.		3	1	1
	d)	Discuss the properties that are satisfied by Groups and Fields.		1	3	2
	e)	Explain Ring with an example.		1	1	1

	Part – III **Long Answer type Questions (Answer any two out of three)**	**Marks** **(04 x 2)**	**BL**	**CO**	**PO / PSO**
03	Encrypt the message “Proud To Be Indian” using play fair cipher with the keyword “ODISHA”. Fill first row and part of second row of key matrix with the given key and rest elements to be randomly filled with rest alphabets. I and J to be kept in the same cell.		3	2	2
04	Encrypt the plain text “GITA” using Hill cipher where key is given as” UGTKIJECABZYXSQV”.		1	2	2
05	State Chinese-Remainder Theorem. Solve the following set of congruences. $X \equiv 3 \mod 5$ $X \equiv 4 \mod 7$ $X \equiv 3 \mod 15$		3	1	2
06	Write Extended Euclidian Algorithm. Find multiplicative inverse of 7 in Z_{20}		3	2	1,2,3