K. J. Somaiya Institute of Technology, Sion, Mumbai-22 (Autonomous College Affiliated to University of Mumbai)

May-June 2024-25

(B. Tech) Program: Computer Engineering Scheme: IIB

Regular Examination: TY Semester: VI

And Course Name: Cryptography And System Security

Course Code: CEC602

Date of Exam:

Duration: 02.5 Hours Max. Marks: 60

(1)A (2)E (3)A	ructions: All questions are compulsory. Praw neat diagrams wherever applicable. Assume suitable data, if necessary. Scientific Calculator is not allowed.	\$2 LA 50 EO 50 Ad 50 Ad 50 Ad 50 Ad 60		
Q. No.	Question	Max. Marks	CO	BT level
Q1	Solve any two questions out of three: (05 marks each)	10		
a)	Solve using Vigenere Cipher Plain text -"Life is full of Surprises" and Key is "Health"	# 15 US # 21 C4 # 0A #	CO1	Ap
b)	Differentiate between MD5 and SHA-1	mp omi	CO3	U
(c)	Explain IP Spoofing attack with its Prevention.		CO5	U
Q 2	Solve any two questions out of three: (05 marks each)	10	Енстурі Ом.)	g to
a)	Explain any 2 modes of operation in block cipher with diagram	RECEIPED R	CO2	U
b) 🗆	Explain working of lamport one time password with diagram	# (al.)	CO4	U
c)	Differentiate between worm and viruses	19 5 Y09	CO6	(1 U (
Q.3	Solve any two questions out of three. (10 marks each)	20		
a)	Find integers p and q such that 51p+36q=3. Also find GCD of (51,36)		COI	Ap
b)	i) Explain steps involved in the "RSA digital signature scheme." [05M]		CO4	U
	ii) Calculate Private key of A and B and also show message signing and verification using RSA digital signature When A wishes to send message M=100 to B.Then A chooses the public key as (7,33) and B chooses the public key (13,221) [05M]		Ž.	Ap
c)	Generate the subkey for first round of AES algorithm. The key in hexadecimal is: 64 46 5a 65 82 ab 7c 73 4e 5b 47 8d 9a 12 35 57 Also find out g(w[3]) Given:		CO2	Ap

K. J. Somaiya Institute of Technology, Sion, Mumbai-22 (Autonomous College Affiliated to University of Mumbai)

May-June 2024-25

(B. Tech) Program: Computer Engineering Scheme: IIB

Regular Examination: TY Semester: VI

Course Code: CEC602

And Course Name: Cryptography And System Security

Date of Exam:

Duration: 02.5 Hours

Max. Marks: 60

		100 AND	1137	100	-					Y		de			er i	THE S		Name of Street,	-		-	_
	2005	0	, 1	2	3	4	5	6	7	8	9		ь	evirus.	d		100		1		1010 101	STATE
		63	70	77	7B	F2	6B	6F	C5	30	01	67	28	FE	D7	AB	76		-1		and the same	ACE
		CA	82	C9	70	FA	59	47	FO	AD	D4	A2	AF	90	A4	72	CO					To a
		87	FD	93	26	36	3F	F7	CC	34	A5	E5	Fi	71	08	31	15				Car In the Car	
		OB	07	23	C3	18	96	05	9A	07	12	80	E2	EB	27	82	75				tille sitt	BALL!
	985	53	D3	20	1A	18	6E	5A	AO	52	38	D6	83	29	E3	2F	84		1		aminus!	18 (P)
		00	DX.	00	ED	20	FC	B1	58	6A	CB	BE	39	44	4C	58	CF					
	7	51	A3	40	OC.	43	4D	33	85	45	F9	02	7F	- 50	30	96	A8 .					1 .0
	X	CD	DC	13	er.	5£	9D	38	F5	BC	86	DA	21	10	FF	F3	D2				1 -	0.0
	9	60	B1	dF	DV.	22	24	dist	17	C-4	A.Z	7E	3D	64	5D	19	73		1			
		EO	32	3A	DA	419	06	24	88	40	EE	88	14	DE	5E	OB	DB .					1 7 6
	ь	E7	CB	37	6D	8D	D5	dF	Ag	60	D3	AC	62	91	95	E-4	79				AD CHARGE	3.5
	C.	BA	78	25	2€	10	A6	84	06	EB	30	74	EP.	00	7A	AE	08		-		-	1
	a t	70	35	85	66	48	03	F6	OF	61	35	24	LP	48	BD	8B	BA				Solve asia	
	, e	E1	F8	98	11	69	D9	8F	94	900	12	02	69	80	CI	ED	9E				- V 191 - FG	
	and the	8C	A1	89	OD	BF	E6	42	68	41	90	20	OE.	30	22	28	DF 16				10,03 1 101	
	3005 A. S.		TAN		the i	II had	LEUM	713	1994	100			Salle -		5 0.2.	DU	10					
2.4	Solve any	v tv	vo c	mee	tion	e on	t of	the	. (10	Local			J.	AF.	2.10	TS CI	The De	1 1/	AND 48	1 2 12	
_			, ,	1403	tion	3 0 4	101	unc	e. (10	mar	ks e	ach)					-	20	1000	
1)	Evalain 6	CT	-	1.:4									100	101 (4)	10	de co	100	HOLLES T			- Caral	
1	Explain S	DOL	arc	inite	ctur	e w	ith s	uita	ible	diag	gran	an an	d ex	am	ole						CO5	U
						912.10			_	_		1	0000	All Street			0.0		4			
)	i) Encryp	t th	e pl	aint	ext	"EX	AM	l" 1	isin	Hi	11 C	inhe	er w	here	ker	v is	"IFF	H"	PI		COI	U
	[5M]		13.4									P-11			No.	10	JLI	11	1			
		ma	nom	· · · · ·	~		1					and the		DOM:					100		s mag	
	ii) Perform	III C	ner.	ypu	on a	na (lecr.	ypti	on t	Isin	g the	e kn	aps	ack	algo	rith	m for	the			1	
	Tollowing											. 18	11						1		CO2	U
	X = (1, 5,	7.	16).	. W	= 11	M	=3	0 F	lair	tev	- 1	001	1 54	11/1					1		er studies in	
		1	,			,		0,1	reerr	ILUX		001	1 L.	INI								
c)	i) Explain	an	v 5	Dro	nort				- TY			1.			180	1770	11 (6	1000	1	ried at	002	7.
	ii) Explain	all	y	110	pert	ies (01 56	ecur	e H	ash	Fun	ctio	ns	5M					-		CO3 -	U
120																					CO2	U

ngic agoziam work oxie him S

When a highes to man't breakly her to be extinct a choose for public key as (1931), and the modes the radion has a choose for public key as 1,000 person

The cred of your

Find hategors plant quinch that high-sing-8. Also find \$3.50 of \$5.50

Page 2 of 2

Seat No.: