

**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

**Instructions:**

- (1) All questions are compulsory.
- (2) Draw neat diagrams wherever applicable.
- (3) Assume suitable data, if necessary.
- (4) Scientific Calculator is not allowed.

Q. No.	Question	Max. Marks	CO	BT level
Q 1	Solve any <b>two</b> questions out of three: (05 marks each)	10		
a)	Solve using Vigenere Cipher Plain text - "Life is full of Surprises" and Key is "Health"		CO1	Ap
b)	Differentiate between MD5 and SHA-1		CO3	U
c)	Explain IP Spoofing attack with its Prevention.		CO5	U
Q 2	Solve any <b>two</b> questions out of three: (05 marks each)	10		
a)	Explain any 2 modes of operation in block cipher with diagram		CO2	U
b)	Explain working of lamport one time password with diagram		CO4	U
c)	Differentiate between worm and viruses		CO6	U
Q.3	Solve any <b>two</b> 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)		CO1	Ap
b)	i) Explain steps involved in the "RSA digital signature scheme." [05M]  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]		CO4	U  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

		Y																											
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	0	1	2	3	4	5	6	7	8	9	a	b
	0	63	7C	77	7B	F2	68	6F	C5	30	01	67	2B	FE	D7	A8	76												
	1	CA	B2	C9	7D	FA	59	47	F0	AD	DA	A2	AF	9C	A4	72	CD												
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15												
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75												
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84												
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	8E	39	4A	4C	58	CF												
	6	DO	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8												
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2												
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73												
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB												
	a	ED	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79												
	b	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08												
	c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A												
	d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E												
	e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF												
	f	BC	A1	89	0D	BF	E6	42	68	41	99	2D	0F	80	54	8B	16												
Q.4	Solve any <b>two</b> questions out of three. (10 marks each)																	20											
a)	Explain SSL architecture with suitable diagram and example																		CO5		U								
b)	i) Encrypt the plaintext "EXAM" using Hill Cipher where key is "JEFH" [5M]																		CO1		U								
	ii) Perform encryption and decryption using the knapsack algorithm for the following X = (1, 5, 7, 16), W = 11, M = 30, Plaintext = 10011 [5M]																		CO2		U								
c)	i) Explain any 5 Properties of Secure Hash Functions [5M]																		CO3		U								
	ii) Explain Needham Schroeder Protocol using neat diagram [5M]																		CO2		U								

\*\*\*\*\*