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

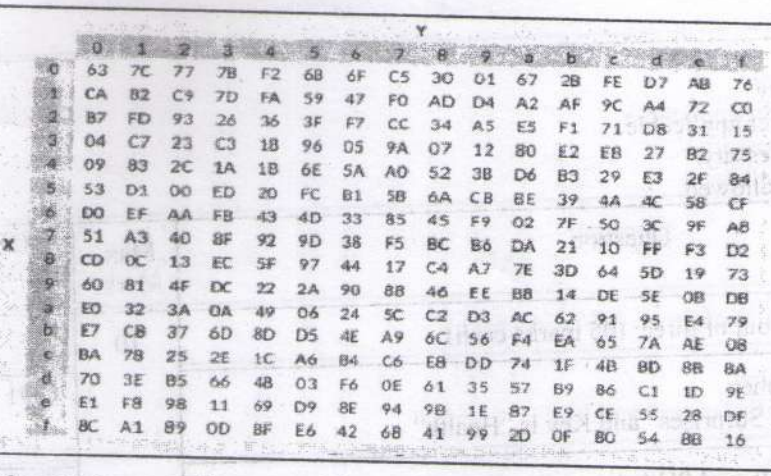
Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.
(4) Scientific Calculator is not allowed.

Q. No.	Question	Max. Marks	CO	BT level
Q 1	Solve any **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"		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 **two** 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 **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)		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 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

Seat No.:

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

				
Q.4	Solve any **two** 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] ii) Perform encryption and decryption using the knapsack algorithm for the following X = (1, 5, 7, 16), W = 11, M = 30, Plaintext = 10011 [5M]		CO1 CO2	U U
c)	i) Explain any 5 Properties of Secure Hash Functions [5M] ii) Explain Needham Schroeder Protocol using neat diagram [5M]		CO3 CO2	U U

****

Seat No.: