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

May-June 2024
(B.Tech.) Program: Computer Engineering Scheme I/II/IIB/III: II
Supplementary Examination: TY Semester: VI
Course Code: CEC602 and Course Name: Cryptography and System Security
Date of Exam: 29/07/2024 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.

		Max. Marks	CO	BT level
Q 1	Solve any six questions out of eight:	12		
i)	Find totient function of 91	2	CO1	Ap
ii)	Which parameters the design of Feistal cipher depends on?	2	CO2	U
iii)	A ----- attaches itself to execute files. When the infected program is executed, it replicates itself by finding other executable files to infect. a. Macro virus b. Stealth Virus c. Polymorphic virus d. Parasitic virus.	2	CO6	U
iv)	How to achieve confidentiality with Digital Signature.	2	CO4	U
v)	Explain IP spoofing.	2	CO5	U
vi)	What are the properties of secure hash function. Explain each in one line.	2	CO3	U
vii)	What is the responsibility of Change cipher Spec Protocol?	2	CO5	U
viii)	Compute GCD (831,366) using Euclid's Algorithm	2	CO1	Ap
Q.2	Solve any four questions out of six.	16		
i)	Generate the subkey for the first round of the AES algorithm. The key in hexadecimal is: 64 46 5A 65 82 AB 7C 73 4E 5B 47 8D 9A 12 35 57	4	CO2	Ap
ii)	Encrypt the text "We are the best" by applying monoalphabetic ciphers. Is cryptanalysis of this cipher easy? If yes then explain how?	4	C01	Ap

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

May-June 2024
(B.Tech.) Program: Computer Engineering Scheme I/II/IIB/III: IIB
Supplementary Examination: TY Semester: VI
Course Code: CEC602 and Course Name: Cryptography and System Security
Date of Exam: 29/07/2024 Duration: 02.5 Hours Max. Marks: 60

iii)	Explain HMAC in detail	4	CO3	U
iv)	Explain RSA digital signature scheme.	4	CO4	U
v)	Explain SSL in detail	4	CO5	U
vi)	What is buffer overflow? Explain how to investigate it through commands. Can you detect buffer overflow before it occurs? If yes, then how?	4	CO6	U
Q.3	Solve any two questions out of three.			
i)	Apply Hill cipher to encrypt the message "ESSENTIAL". The key for encryption is "ANOTHERBZ". And decrypt the encrypted message	8	CO1	Ap
ii)	Encrypt plaintext stream P = [1 2 2 2] with key = [1 2 3 6] using simplified RC4 and find out stream cipher	8	CO2	Ap
iii)	Explain four protocols of SSL.	8	CO5	U
Q.4	Solve any two questions out of three.			
i)	Differentiate between the transport mode and tunnel mode of IPSec and Explain how authentication and confidentiality are achieved using IPSec.	8	CO5	U
ii)	Find public key of Knapsack algorithm having private key [1 2 4 10 20 40], m=110 and n=31. Encrypt [100100111100101110] and decrypt the generated cipher text.	8	CO2	Ap
iii)	Explain SHA-1 algorithm in detail	8	CO3	U

****