Shri Vile Parle Kelavani Mandal's

DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING

(Autonomous College Affiliated to the University of Mumbai)

NAAC Accredited with "A" Grade (CGPA : 3.18)

Academic Year (2021-22)

Year: 3 Semester: VI

Program: B. Tech. (Computer Engineering) **Max. Marks: 75**

Subject: Information Security **Time: 10:30 am to 1:30 pm**

Date: 02-07-2022 **Duration: 3 Hours**

REGULAR EXAMINATION

Instructions: Candidates should read carefully the instructions printed on the question paper and on the cover page of the Answer Book, which is provided for their use.

(1) This question paper contains **TWO** pages.
(2) All Questions are Compulsory.
(3) All questions carry equal marks.
(4) Answer to each new question is to be started on a fresh page.
(5) Figures in the brackets on the right indicate full marks.
(6) Assume suitable data wherever required, but justify it.
(7) Draw the neat labelled diagrams, wherever necessary.

Question No.		Max. Marks
Q1 (a)	What are Basic Security Goals. Explain various threats to Basic Security Goals? **OR** What are the ITU-T(X.800) Recommended Security Mechanism. Explain any three of them.	[05] [05]
Q1 (b)	Prove using Playfair Encryption and Decryption Techniques works for Plaintext- "instruments" using Key as "MONARCHY".	[10]
Q2 (a)	i. Find Multiplicative Inverse of 8 mod 11 using extended Euclidean Algorithm. ii. Apply key generation process in S-DES to find various keys. Use initial Key as 1011001101 Given P10 (3,5,2,7,4,10,1,9,8,6) P8 (6,3,7,4,8,5,10,9) **OR** Explain AES Encryption and Decryption Algorithm along with Block diagram. Discuss Round 1 in details.	[05] [05] [10]
Q2 (b)	Explain Double and Triple DES.	[05]
Q3 (a)	Generate public key, private key and ciphertest using RSA for given values p=7, q=11,e=7 and M=9 **OR** Explain Pretty Good Privacy in details.	[05] [05]
Q3 (b)	Explain MD5 algorithm is details. How it differs from SHA? **OR** Explain how to secure IP Protocol using transport and tunnel modes. Also give packet format for same.	[10] [10]
Q4 (a)	Explain RSA Digital Signature Scheme?	[10]

	OR Why there is a Need of Mutual Authentication. Explain Kerberos Protocol in details with schematic.	[10]
Q4 (b)	What is SQL Injection attack? How it occurs. How to Mitigate SQL Injection attack.	[05]
Q5 (a)	What is Man in Middle Attack. How it is possible in Diffie-Hellman protocol. Alice and Bob uses Diffie-Hellman Key Exchange technique with a common prime 71 and primitive root 7. Show that 7 is primitive root of 71. If Alice's private key is 5 and Bob's private key is 12. Find Alice's and Bob's public keys. Also find shared secret key?	[10]
Q5 (b)	Explain incomplete mediation in software security. **OR** Explain TCP SYN flooding attack?	[05] [05]

All the Best!