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~~ 03/10/2022 **Duration: 3 Hours**

RE – ~~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)	Explain Chosen Plaintext and Chosen Ciphertext attacks methods in Cryptography. **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, "Balloons for committee" using Key as "Keyword".	[10]
Q2 (a)	i. 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) i. Find Multiplicative Inverse of 8 mod 11 using extended Euclidean Algorithm. **OR** Explain AES Encryption and Decryption Algorithm along with Block diagram. Explain with examples SubBytes, ShiftRows steps in AES Algorithm.	[05] [05] [10]
Q2 (b)	Explain various ways of cascading DES to strengthen its security?	[05]
Q3 (a)	Generate public key, private key and ciphertest using RSA for given values p=3,q=11,e=3 and m=00111011. **OR** Explain Pretty Good Privacy in details.	[05] [05]
Q3 (b)	Explain Cipher Based Message Authentication Code (CMAC) in detail? **OR** Explain working of SSL protocol in details with SSL Handshake schematic and message format.	[10] [10]

Q4 (a)	Explain Digital Certificate format: X.509. What are the advantages and Limitations of Digital Signature? **OR** Why there is a Need of Mutual Authentication. Explain Kerberos Protocol in details with schematic.	[10] [10]
Q4 (b)	What is Buffer Overflow Attacks. How it occurs. How to Mitigate Buffer Overflow Attacks.	[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 various DDOS attacks and their mitigation techniques. **OR** Explain TCP SYN flooding attack?	[05] [05]

All the Best!