Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India

(Autonomous College Affiliated to University of Mumbai)

Mid Semester Examination

2019-2020

Max. Marks: 20 | Duration: 60 Min

Class: M.Tech. (1st Year) | Semester: I

Course Code: CE913 | Branch: Computer Engineering

Name of the Course: Information and System Security

Instruction:

(1) All questions are compulsory

(2) Draw neat diagrams

(3) Assume suitable data if necessary

Q No.	Question	Max. Marks	CO	BL
Q.1	Suppose Bob wishes to send Alice the message "HELLO WORLD". Let p=7, and q=11. Alice chooses e=17, so her private key is d=53. In this cryptosystem, each plaintext character is represented by a number 00 (A) and 25 (Z); 26 represents a blank. i) Write the plaintext using the above given representation. ii) Consider the RSA cryptosystem and encrypt and decrypt the given plaintext.	05	CO3	BL3
	OR			
	State the difference between a session key and an interchange key. Suppose Alice and Bob wish to communicate and they share a common key using classical cryptosystem. But how do they agree on a common key? The problem is if Alice sends one to Bob, Eve the eavesdropper will see it and will be able to read the traffic between them. Give the solution to avoid this bootstrapping problem by using classical cryptographic protocol.	05	CO3	BL3
Q.2	Summarize Biba's Strict Integrity Model formalism with all relations on subjects, objects and integrity levels.	05	CO2	BL2

Q.3	Lipner's Full Model covers both confidentiality and integrity. In case of confidentiality, Lipner provides two security levels, in the following order (higher to lower): *Audit Manager (AM)*, *System Low (SL)*. He similarly defined five categories: *Development (D)*, *Production Code (PC)*, *Production Data (PD)*, *System Development (SD)* and *Software Tools (T)* for confidentiality. The model has security classifications with three integrity classifications (highest to lowest): *System Program (ISP)*, *Operational (IO)* and *System Low (ISL)*. He defined two integrity categories for distinguishing production and development software and data: *Development (ID)* and *Production (IP)*. Sketch Hasse diagrams for confidentiality and integrity classification in Lipner's Full Model.	05	CO2	BL3
Q.4	The Mumbai University (MU) is implementing an electronic voting (e-voting) system to elect their chancellor. Only the faculty of MU are allowed to vote online at a voting website that the university IT department is implementing. What are the security attributes that need to be considered for the e-voting system? Be specific. For instance, do not just say confidentiality', but enumerate which (all) kinds of information need to be kept confidential. Note that the security attributes could go beyond the classical three used in CIA-triad.	05	CO1	BL3