19UCS181 - VAIBHAV

The LNM Institute of Information Technology, Jaipur

Department of Computer Science & Engineering

Computer Security (CSE 6072)

End Term

2021-22 Odd Sem

Time: 180 Minutes **Date:** 10/12/2021 **Maximum Marks:** 40

Instructions:. *There are total 8 Questions. All questions are compulsory.Answer without reasoning will not be considered. For Q-1, partial marks will be given for each part only if the answer is correct and no step marking involve within the part.*

Q.1:	Alice wants to use the RSA cipher for encryption and decryption. For that purpose she has chosen two prime numbers 11 and 23. She has also chosen 21 as her public key. a) Help Alice to encrypt the message 420. b) Evaluate the private key for Alice c) Help Alice to decrypt the same message 420.	[5]
Q.2:	Suppose you have to deploy a server in a machine. There are three possible security policies (a, b and c) for deploying the server in a machine. What security policy you will choose for deploying the server in a machine. Justify your answer with the reasoning. a) The server is installed on a single machine with no Face Book application running on it. b) The server is installed on virtual machine-1 (VM1) and other properly configured Face Book application is running on virtual machine-2 (VM2). Both VM1 and VM2 are running on the same machine using hosted virtualization. c) The server is installed on a single machine with a properly configured Facebook application running on it.	[3]
Q.3:	Suppose IPSec (transport mode with no prior set-up/symmetric key) wants to encrypt message through symmetric key encryption between two machines A and B. Explain with proper reasoning about the crypto primitives and procedures for achieving confidentiality through encryption without man in middle attack.	[4]
Q.4:	Assume IPSec is deployed at two machines for the communication between them. These two machines cannot use intermediate routers/machines. Can these two machines hide their IP addresses from an adversary who is sniffing the intermediate communication channel? Explain with proper reasoning.	[4]
Q.5:	Suppose a person A wants to send a confidential message to another person B. He can use S/Mime. S/Mime uses symmetric key encryption for confidentiality. Assume there is no prior established symmetric key. How confidential message can be sent from A to B using S/Mime without man in the middle attack. Explain with proper reasoning along with the crypto primitives.	[4]

Q.6:	Explain which list (access control list or capability list) will be easier to use for the following scenarios with proper justification. a) Who has access to this object? b) What object this subject can access?	[5]
Q.7:	Assume a person decided to use TLS for the secure communication with a server. The person is using chrome browser which supports only AES encryption and server can support AES, DES encryption. Explain how the browser and server will decide about which encryption method is to be used. Explain the mechanism through which they will establish the encryption key along with crypto primitives so that there is no man in middle attack.	[5]
Q.8:	Suppose students are to be authenticated by password based authentication for attendance in classroom. The classroom has software which consists of database of user id and hash of password. Each student has to enter his/her id and password in the software for marking the attendance. Suggest how students will be authenticated for attendance by explaining crypto primitives with proper reasoning. Propose possible attacks in your design and also possible defenses for the attacks	[10]