SASTRA Deemed University, Tirumalaisamudram – 613 401

CSE323R01-Computer Networking Principles & Components
CIA1 – 20.02.2025

Q. No. 01 applicable for Roll no: 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58

Q. No. 02 applicable for Roll no: 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59

Q. No. 03 applicable for Roll no: 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57

Q. No. 01. A software company is developing a secure file transfer system that allows users to send and receive confidential files over a network. To ensure data security, the system must encrypt files before transmission and decrypt them upon reception. The company has chosen Caesar (the method discussed during lab session) cipher method for encryption and decryption.

Question:

You are tasked with implementing a secure file transfer system in Java. The system should:

i. Encrypt a file before sending using Caesar Cipher
ii. Send the encrypted file over a network (e.g., save to a directory representing the receiver).
iii. Decrypt the received file back to its original form using the same secret key.

****

Q. No. 02. A company is developing a remote directory lookup system that enables a machine to request directory information from another machine over a network. The system should allow:

i. A source machine to send a directory name along with its path to a destination machine.
ii. The destination machine to receive the request and search for the directory in its file system.
iii. If the directory exists, the destination machine should:
    a. Retrieve all filenames and subdirectory names from the given path.
    b. Send the list back to the source machine.
iv. The source machine should display the received directory contents on the screen.
v. The entire communication should be secure, ensuring data confidentiality and integrity.

Question:

You are designing this secure remote directory lookup system in Java. Your implementation should:

i. Send and receive directory path requests securely over the network.
ii. Search the directory on the destination machine and retrieve all file and subdirectory names.
iii. Encrypt the communication to ensure security during transmission.
iv. Log the entire conversation (requests and responses) on both machines for record-keeping.

[Note: Use list method of File class for getting list of file names etc.]

****

Q. No. 03. A company wants to implement a secure communication system between two machines over a network. The system should allow two parties to exchange encrypted messages and maintain a log of the entire conversation on both sides. The sender machine should encrypt a message using a secure encryption algorithm before sending it. The receiver machine should decrypt the received message and send an encrypted reply. Both machines should log the entire conversation (encrypted and decrypted messages) into a file for record-keeping. The encryption and decryption processes must ensure data integrity and security against unauthorized access.

Question:

You are tasked with implementing this secure messaging system in Java. Your implementation should:

i. Encrypt outgoing messages before transmission.
ii. Decrypt incoming messages upon reception.
iii. Log both encrypted and decrypted messages into a file on each machine.
iv. Handle key management securely, ensuring only authorized parties can decrypt messages.

****