CRYPTOGRAPHY AND NETWORK SECURITY LAB SYLLABUS

Symmetric Encryption with DES

- Implement DES encryption and decryption
- Use a 64-bit key size and 64-bit block size

Symmetric Encryption with AES

- Implement AES encryption and decryption
- Support key sizes of 64, 128, or 256 bits
- Use a 64-bit block size

RSA Encryption Scheme

- Develop an RSA encryption and decryption scheme

MD5 Hash Algorithm

- Develop an MD5 hash algorithm
- Calculate the Message Authentication Code (MAC)

SHA Hash Algorithms

- Find a Message Authentication Code (MAC) for a variable-size message
- Use SHA-128 and SHA-256 hash algorithms
- Measure time consumption for varying message sizes for both SHA-128 and SHA-256

Digital Signature Standard (DSS)

- Develop DSS for verifying legal communicating parties

Diffie-Hellman Key Exchange Protocol

- Design a Diffie-Hellman multiparty key exchange protocol
- Perform a Man-in-the-Middle Attack

SSL Socket Communication

- Develop a simple client and server application using SSL socket communication

Telnet and Packet Analysis

- Develop a simple client-server model using telnet
- Capture packets transmitted with `tshark`
- Analyze the pcap file and extract transmitted data (plain text) using a packet capturing library
- Implement the scenario using SSH and observe the data

JSON Web Token (JWT)

- Develop a web application that implements JSON Web Token (JWT)