Lab 01

CS457 Big Data Security

Assignment: Implement Symmetric Encryption

Assignment given on : 13-Jan-2025

Assignment to be shown on: 20-Jan-2025

Part 1. Handwritten Assignment

The hand written assignment will be of at least 3 pages (excluding figures) of handwritten text (max 4) covering the following points.

Write a detailed essay (handwritten) on symmetric encryption. Address the following points:

1. Core mathematical principles behind it
2. Key management challenges
3. Performance characteristics
4. Security strengths and vulnerabilities
5. Real-world applications and use cases

Part 2: Implementation

Symmetric Encryption Implementation : Implement AES-256 encryption in Python:

1. Create functions for key generation, encryption, and decryption
2. Implement proper padding mechanisms
3. Handle file input/output
4. Include error handling and validation
5. Document your code thoroughly

For each implementation do the following:

1. Identify potential vulnerabilities
2. Propose mitigation strategies
3. Analyze the impact of different key sizes
4. Discuss potential side-channel attacks

Conduct performance testing:

1. Measure encryption/decryption speeds for different input sizes
2. Compare memory usage
3. Analyze CPU utilization
4. Create visualizations of your findings
5. Provide recommendations for optimization

Submission Requirements

1. All code must be submitted via GitHub repository (I will send the instructions)
2. Include comprehensive README documentation
3. Provide test cases and sample data
4. Submit a detailed report covering all theoretical aspects
5. Include performance testing results and visualizations
6. Show the handwritten text and submit to TA. Please **staple yourself** and come to lab. Unstapled handwritten assignments / folded papers will be deduced 30% marks.