MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL TECHNICAL UNIVERSITY OF UKRAINE

" IHORY SIKORSKY KYIV POLYTECHNIC INSTITUTE"

Artem Volokyta

Lab Work 3

Implementation and Performance Analysis of Symmetric Encryption and Hashing Algorithms

kulubecioglu Mehmet

Variant Number 10

IM-14 FIOT

Kyiv

IHORY SIKORSKY KYIV POLYTECHNIC INSTITUTE

2025

Introduction

This report explores the implementation and performance analysis of symmetric encryption algorithms (DES and AES) and a cryptographic hash function (SHA-3). The goal of this project is to understand encryption and decryption processes, analyze security properties, and compare computational efficiency.

Project Objectives:

1. Encrypt and decrypt data using the DES (Data Encryption Standard) algorithm.
2. Encrypt and decrypt data using the AES (Advanced Encryption Standard) algorithm.
3. Generate and analyze cryptographic hashes using SHA-3.
4. Compare the performance of DES, AES, and SHA-3 in terms of execution time.

Technologies Used

The following technologies were utilized in this project:

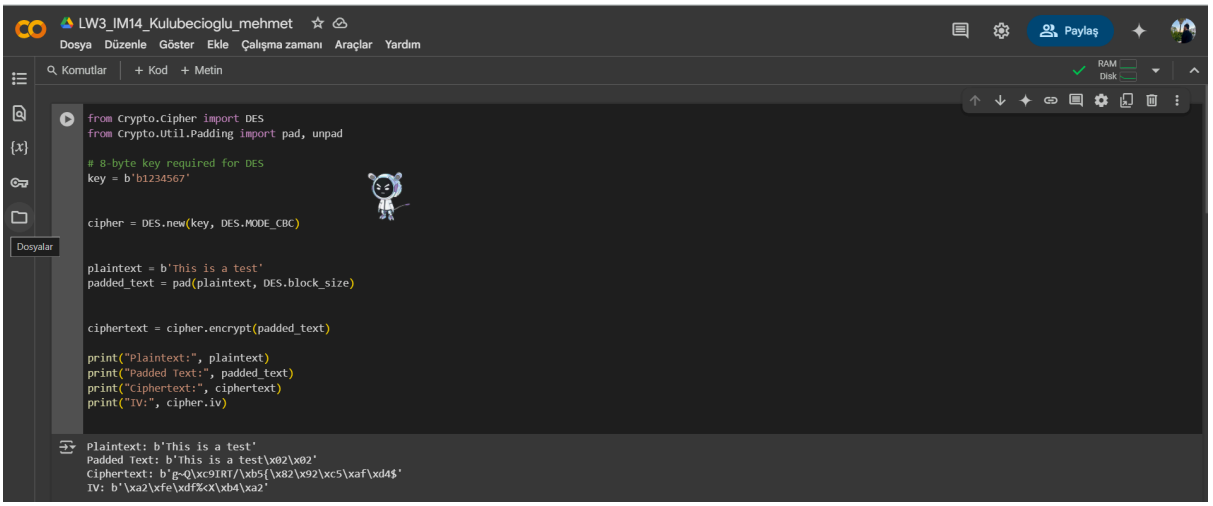
- **Python 3:** Programming language for simulation execution
- **PyCryptodome:** Library for cryptographic operations
- **Google Colab:** Environment for running and testing the code

Implementation Details

DES Encryption and Decryption

The Data Encryption Standard (DES) is a symmetric-key algorithm that encrypts data in 64-bit blocks using a 56-bit key.

DES Encryption Code:



DES Decryption Code:

4.2. SHA-3 Hashing

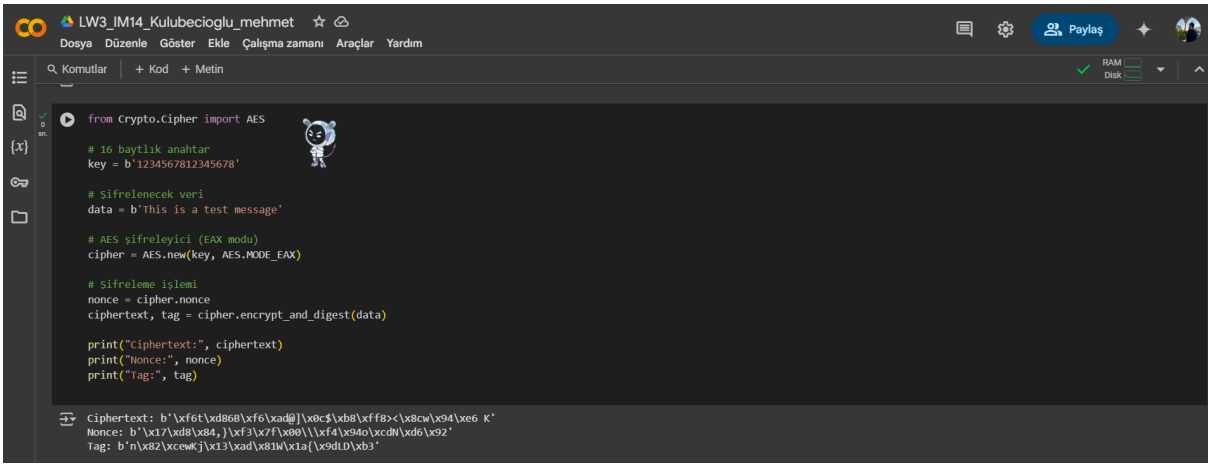
SHA-3 is a cryptographic hash function that generates a fixed-length digest, making it useful for data integrity verification.

SHA-3 Hashing Code:

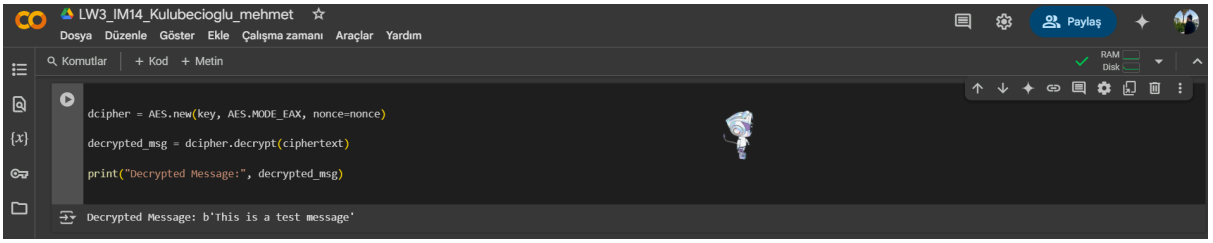
4.3. AES Encryption and Decryption

AES (Advanced Encryption Standard) is a block cipher that replaces DES and is considered more secure. It supports 128-bit, 192-bit, or 256-bit keys.

AES Encryption Code:



AES Decryption Code:

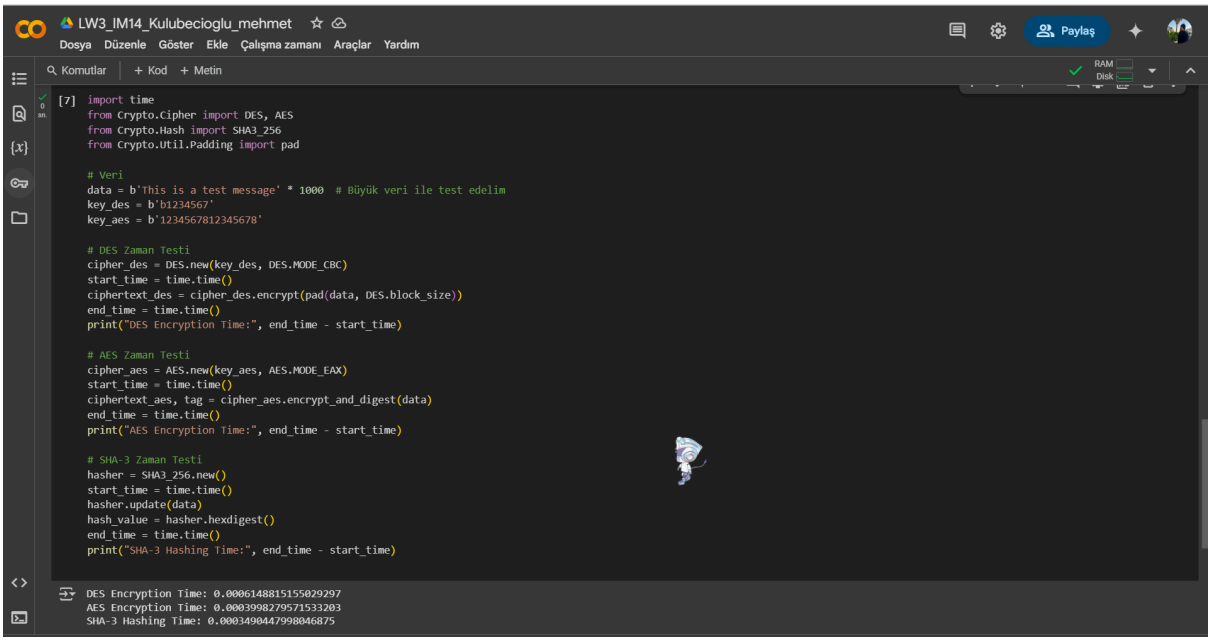


AES uses a "nonce" to ensure security and uniqueness of encrypted messages.

5. Performance Analysis

A performance comparison was conducted to analyze the execution time of DES, AES, and SHA-3.

Performance Testing Code:



Findings:

SHA-3 was the fastest operation.

AES was faster than DES, making it more efficient and secure.

DES is outdated and slower than AES.

6. Conclusion and Recommendations

Through this project, different cryptographic techniques were implemented and compared.

Key Takeaways:

AES is more secure and efficient than DES.

SHA-3 is the fastest operation and provides integrity verification.

Encryption speed varies depending on key size and block mode.

This project successfully demonstrated encryption, decryption, and hashing techniques in cybersecurity.