

Pinnacle Labs Cybersecurity Internship - Task 1 Report

Intern Information

Name: Abin Shaji Thomas

Program: Cybersecurity Internship (May 2025)

Institute: Karunya Institute of Technology and Sciences

Task: Text Encryption using AES, DES, and RSA

Project Title

SecureText - Text Encryption Tool using AES, DES, and RSA

Objective

The objective of this task was to build a cybersecurity tool capable of encrypting and decrypting text using three different cryptographic algorithms: AES (Advanced Encryption Standard), DES (Data Encryption Standard), and RSA (Rivest-Shamir-Adleman). The goal was to understand practical implementations of both symmetric and asymmetric encryption and to develop a user-friendly tool for real-world scenarios.

Technologies Used

- Python 3.12.0
- Tkinter (for GUI)
- cryptography library (for AES)
- pycryptodome library (for DES and RSA)
- Key Management (AES key, RSA keypair)

Encryption Algorithms Overview

AES (Advanced Encryption Standard):

- Symmetric encryption algorithm
- 128-bit key size
- Fast and secure

Pinnacle Labs Cybersecurity Internship - Task 1 Report

DES (Data Encryption Standard):

- Legacy symmetric encryption algorithm
- 56-bit key size
- Added for academic comparison and demonstration

RSA (Rivest-Shamir-Adleman):

- Asymmetric encryption algorithm
- 2048-bit keypair used (public and private keys)
- Commonly used for secure key exchange and digital signatures

Project Description

The SecureText application features a clean, user-friendly GUI built using Tkinter. It allows users to input text and select an encryption method (AES, DES, or RSA) from a dropdown menu. The user can then encrypt or decrypt the text using the selected method. AES keys are auto-generated and reused; DES uses a static demo key; and RSA uses a generated keypair saved to PEM files. The project runs entirely offline and provides practical encryption experience.

Learning Outcomes

- Understood the working of symmetric and asymmetric encryption.
- Learned to implement AES using Fernet from the cryptography library.
- Gained experience in using pycryptodome for DES and RSA.
- Developed a GUI application using Tkinter.
- Learned to manage cryptographic keys and secure data handling.
- Gained insight into padding, encoding (Base64), and error handling.

Conclusion

The SecureText project was successfully implemented as part of Task 1 in the Pinnacle Labs Cybersecurity Internship. This task provided real-world exposure to cryptographic concepts and Python-based cybersecurity tool development. It helped in improving both theoretical understanding and practical application of secure data handling techniques.