**Title: Programming Symmetric and Asymmetric Cryptography (Lab 4)**

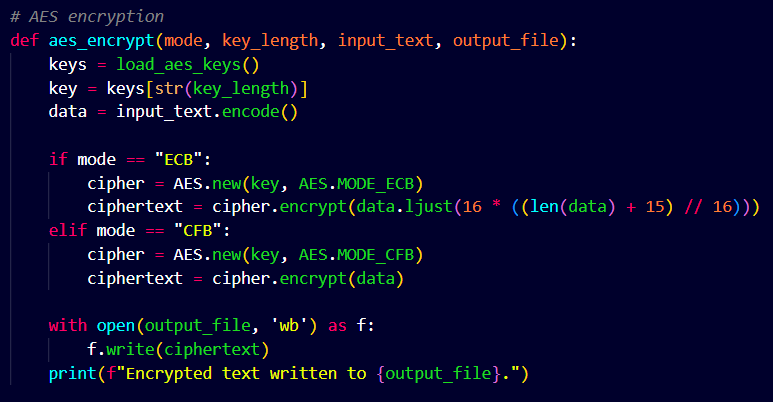
**Author:** Shattik Bandyopadhyaa  
**Reg No:** 2019831039  
**Date:** July 7, 2024

**1. Introduction**

This project provides practical experience with both symmetric and asymmetric cryptography using Python. It involves the implementation of AES encryption and decryption in ECB and CFB modes with 128-bit and 256-bit keys, RSA encryption and decryption, digital signatures, and SHA-256 hashing. The program features a command-line interface similar to OpenSSL and includes functionality to measure execution times for these operations. This report details the implementation, usage, and performance analysis of the cryptographic functions.

**2. Example code snippets**

**AES Encryption:**

****

**AES Decryption:**

A computer screen shot of a code

Description automatically generated

**RSA Encryption:**

A computer screen shot of text

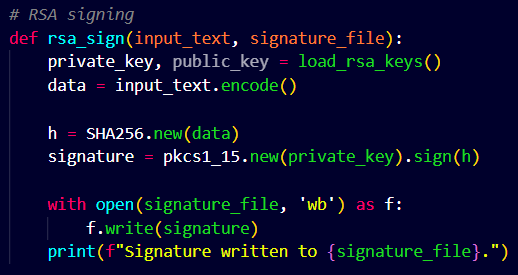
Description automatically generated

**RSA Decryption:**

**A computer screen shot of text

Description automatically generated**

**RSA Signing:**

****

**RSA Sign Verification:  
A computer screen shot of text

Description automatically generated**

**SHA-256 Hashing:**

**A computer screen with text

Description automatically generated**

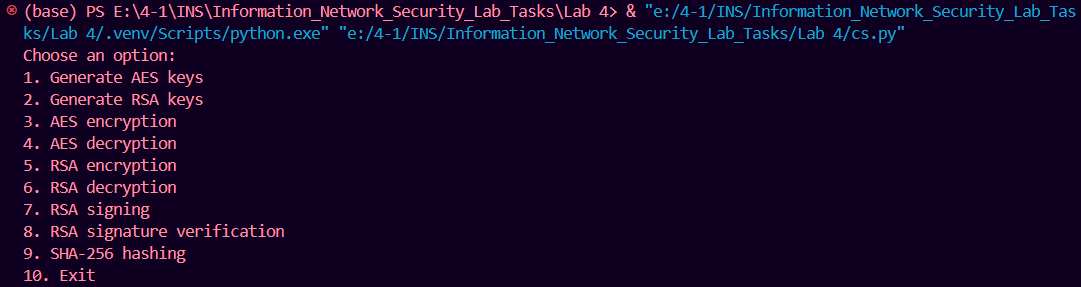
**Measuring Execution Time:**

**A screen shot of a computer program

Description automatically generated**

**3. Using the functionalities**

**When you run the program, you will be presented with a menu of options:**

****

Choose an option:

1. Generate AES keys

2. Generate RSA keys

3. AES encryption

4. AES decryption

5. RSA encryption

6. RSA decryption

7. RSA signing

8. RSA signature verification

9. SHA-256 hashing

10. Exit

Here, you can choose any of the options according to your need.

**3.1 AES encryption/decryption**

Encryption:

1. Choose option 1 for generating AES keys.

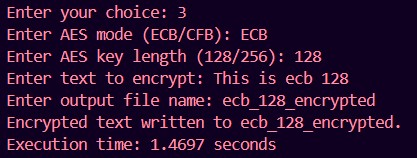
2. Choose option 3 for AES encryption.

3. Select ECB/CFB according to your need.

4. Select key length 128/256.

5. Enter text to encrypt.

6. Enter output file name.



Decryption:

1. Choose option 4 for AES decryption.

2. Select ECB/CFB according to your need.

3. Select key length 128/256.

4. Enter input file name.

A computer screen with text

Description automatically generated

**3.2 RSA encryption/decryption**

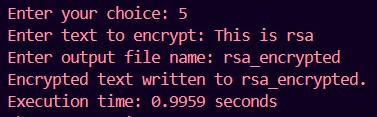
Encryption:

1. Choose option 2 for generating RSA keys.

2. Choose option 5 for RSA encryption.

3. Enter text to encrypt.

4. Enter output file name.



Decryption:

1. Choose option 6 for RSA decryption.

2. Enter input file name.

A black background with pink text

Description automatically generated

**3.3 RSA Signature**

Signing:

1. Choose option 7 for RSA signing.

2. Enter text to sign.

3. Enter signature file name.

A computer screen with text

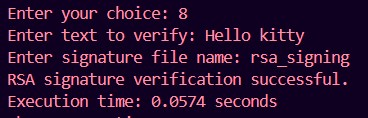
Description automatically generated

Signature verification:

1. Choose option 8 for signature verification.

2. Enter text to verify.

3. Enter signature file name.

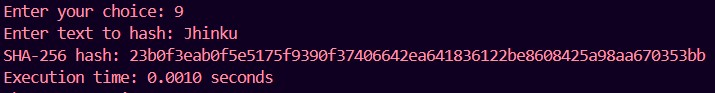


**3.4 SHA-256 Hashing**

Hashing:

1. Choose option 9 for sha256 hashing.

2. Enter text to hash.



**4. Analyzing execution time**

In this section, we will see the execution time for different cryptographic operations.

AES encryption:

|  |  |  |  |
| --- | --- | --- | --- |
| Operation | Key Length (bits) | Mode | Time (seconds) |
| Encryption | 128 | ECB | 1.4697 |
| Encryption | 128 | CFB | 1.2120 |
| Encryption | 256 | ECB | 0.0020 |
| Encryption | 256 | CFB | 0.0073 |

AES decryption:

|  |  |  |  |
| --- | --- | --- | --- |
| Operation | Key Length (bits) | Mode | Time (seconds) |
| Decryption | 128 | ECB | 0.0160 |
| Decryption | 128 | CFB | 0.0137 |
| Decryption | 256 | ECB | 0.0091 |
| Decryption | 256 | CFB | 0.0196 |

RSA encryption/decryption:

|  |  |
| --- | --- |
| Operation | Time (seconds) |
| Encryption | 0.9959 |
| Decryption | 0.0709 |

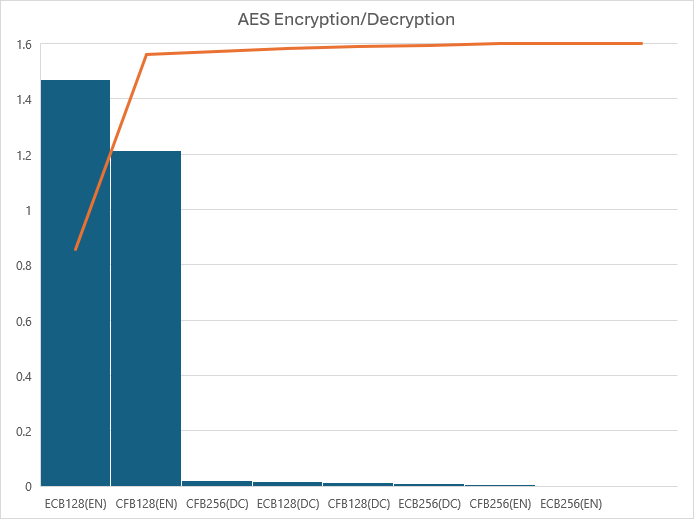
RSA Signature:

|  |  |
| --- | --- |
| Operation | Time (seconds) |
| Signature generation | 1.7593 |
| Signature verification | 0.0574 |

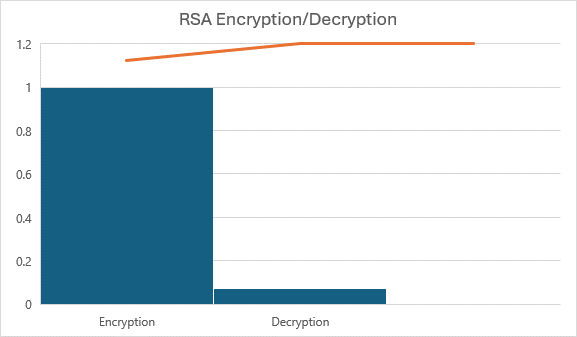
SHA-256 Hashing

|  |  |
| --- | --- |
| Operation | Time (seconds) |
| SHA-Hashing | 0.0010 |

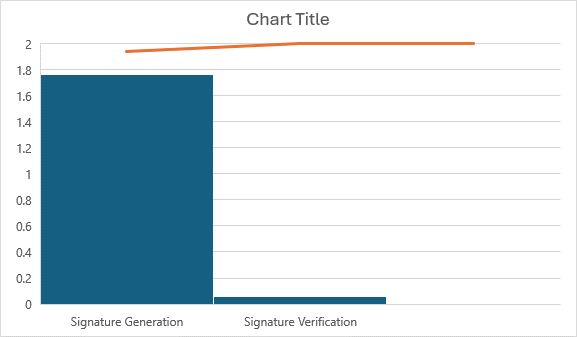
**5. Plotting**

****

**Fig:** AES encryption/decryption

****

**Fig:** RSA encryption/decryption

****

**Fig:** RSA Signature Generation/Verification

**6. Conclusion**

I have collected the necessary resources from the following sites:

[**https://brilliant.org/wiki/rsa-encryption/**](https://brilliant.org/wiki/rsa-encryption/)

[**https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption**](https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption)

[**https://cryptobook.nakov.com/digital-signatures/rsa-sign-verify-examples**](https://cryptobook.nakov.com/digital-signatures/rsa-sign-verify-examples)