**BÁO CÁO THỰC HÀNH**

**Môn học: Mật mã học**

**Kỳ báo cáo: Buổi 03-04 (Lab 03-04)**

**Tên chủ đề: RSA Cipher - ECC-based Digital signature with CryptoPP**

*GVHD: Nguyễn Ngọc Tự*

*Ngày báo cáo: 26/11/2021*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT209.M11.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Khải Đăng | 19521317 | 19521317@gm.uit.edu.vn |
|  |  |  |  |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Task** |  |
| 1 | RSA Cipher (Encryption/Decryption) using CryptoPP  Required: |  |
| 2 | ECC-based Digital signature with CryptoPP |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

**BÁO CÁO CHI TIẾT**

# [ WINDOWS ] Task 3: RSA Cipher (Encryption/Decryption) using CryptoPP

## Report your hardware resources

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Phần cứng laptop

## Report computation performance for all operations

**- Encryption:**

Vị trí đo:

int startCount = clock();

    for (int i = 0; i < 10000; i++)

    {

        cipher.clear();

*// Encryption*

        AutoSeededRandomPool rng;

*// Encryption*

        RSAES\_OAEP\_SHA\_Encryptor e(publicKey);

        StringSource(plain, true,

                     new PK\_EncryptorFilter(rng, e,

                                            new StringSink(cipher)) *// PK\_EncryptorFilter*

        ); *// StringSource*

*/\* Pretty Print cipher text \*/*

    }

    int stopCount = clock();

    double total = (stopCount - startCount) / double(CLOCKS\_PER\_SEC) \* 1000;

Kết quả:

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Encryption

Báo cáo hiệu xuất

Total time for 10.000 rounds: 1832 ms

Execution time: 0.1832 ms

**- Decryption:**

Vị trí đo:

*// Decryption*

    int startCount = clock();

    for (int i = 0; i < 10000; i++)

    {

*// Decryption*

        recovered.clear();

        RSAES\_OAEP\_SHA\_Decryptor d(privateKey);

        StringSource(cipher, true,

                     new PK\_DecryptorFilter(rng, d,

                                            new StringSink(recovered)) *// PK\_EncryptorFilter*

        ); *// StringSource*

    }

    int stopCount = clock();

    double total = (stopCount - startCount) / double(CLOCKS\_PER\_SEC) \* 1000;

Kết quả đo:

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả đo decryption

Báo cáo hiệu xuất

Total time for 10.000 rounds: 46071 ms

Execution time: 4.6071 ms

# [ LINUX ] Task 3: RSA Cipher (Encryption/Decryption) using CryptoPP

## Report your hardware resources

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

1. Cấu hình linux

## Report computation performance for all operations

**- Encryption:**

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Encryption

Báo cáo hiệu xuất

Total time for 10.000 rounds: 676.293 ms

Execution time: 0.0676293 ms

**- Decryption:**

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả đo decryption

Báo cáo hiệu xuất

Total time for 10.000 rounds: 45082.1 ms

Execution time: 4.50821ms

# [ WINDOWS ] ECC-based Digital signature with CryptoPP

## Report your hardware resources

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Phần cứng laptop

## Report computation performance for all operations

**- The signing function**

Vị trí đo:

int start\_s = clock();

    for (int i = 0; i < 10000; i++)

    {

        AutoSeededRandomPool prng;

        signature.erase();

        StringSource(message, true,

                     new SignerFilter(prng,

                                      ECDSA<ECP, SHA256>::Signer(privateKeys),

                                      new Base64Encoder(new StringSink(signature))));

    }

    int stop\_s = clock();

    double total = (stop\_s - start\_s) / double(CLOCKS\_PER\_SEC) \* 1000;

Kết quả đo

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

1. Ký

Báo cáo hiệu xuất

Total time for 10.000 rounds: 8638 ms

Execution time: 0.8638 ms

**- The verify function**

Vị trí đo:

 int start\_s = clock();

    for (int i = 0; i < 10000; i++)

    { *//*

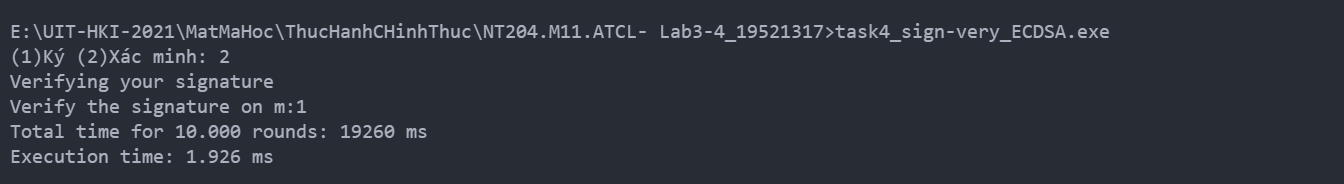
        result = VerifyMessage(publicKey\_r, message\_r, signature\_r);

    }

    int stop\_s = clock();

    double total = (stop\_s - start\_s) / double(CLOCKS\_PER\_SEC) \* 1000;

Kết quả đo

****

1. Verify

Total time for 10.000 rounds: 19260 ms

Execution time: 1.926 ms

# [ LINUX ] ECC-based Digital signature with CryptoPP

## Report your hardware resources

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

1. Phần cứng laptop

## Report computation performance for all operations

**- The signing function**

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

1. Ký

Báo cáo hiệu xuất

Total time for 10.000 rounds: 6214.67 ms

Execution time: 0.621467 ms

**- The verify function**

Kết quả đo

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

1. Verify

Total time for 10.000 rounds: 20243 ms

Execution time: 2.0243 ms

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)