BÁO CÁO BÀI TẬP

**Môn học: Mật mã học**

**Kỳ báo cáo: Buổi 03 (Session 03)**

**Tên chủ đề: RSA Algorithm**

*Ngày báo cáo: 09/04/2023*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT219.N22.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Trần Anh Đức | 21521964 | 21521964@gm.uit.edu.vn |
| 2 | Nguyễn Hữu Tiến | 21590479 | 21590479@gm.uit.edu.vn |
| 3 | Lê Thanh Duẩn | 19521370 | 19521370@gm.uit.edu.vn |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Run Sample Program | 100% | Thanh Duẩn |
| 2 | Encrypt with public key & decrypt with private key | 100% | Hữu Tiến |
| 3 | Read input from file | 100% | Hữu Tiến |
| 4 | Read input from user | 100% | Anh Đức |
| 5 | Support UTF 16 for input | 100% | Anh Đức |
| 6 | Read key from file | 100% | Anh Đức |
| 7 |  |  |  |
| 8 |  |  |  |

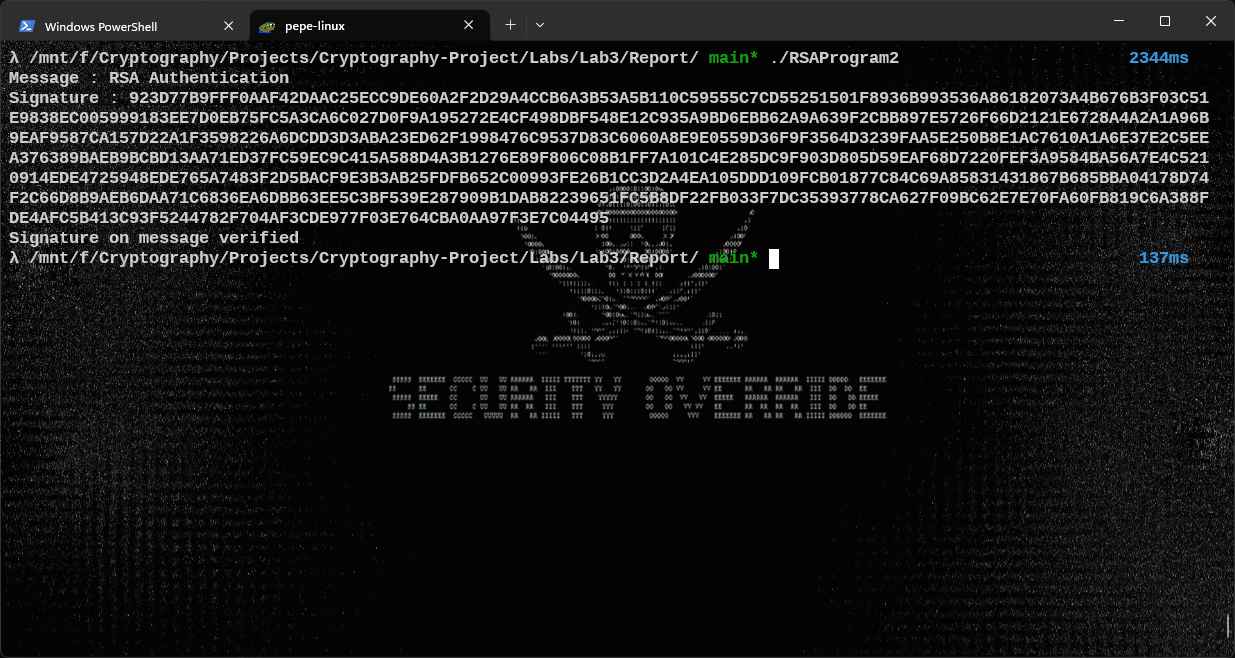
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

**1. Exercise 1:**

**Text

Description automatically generated**

**2. Exercise 2:**

****

**Sign and verify message with RSA-SS.**

**3. Exercise 3 :**

**Text

Description automatically generated**

**Function to read input from file :**

string InputFromFile(wstring wfilename)

{

    wcin.ignore();

    string plain, filename;

    filename = wstring\_to\_string(wfilename);

    FileSource file(filename.data(), true, new StringSink(plain));

    cout << "Reading plaintext from file " << filename << endl;

    return plain;

}

**4. Exercise 4 and 5:**

**Text

Description automatically generated**

**Function to read input from user :**

string InputFromScreen()

{

    wstring wplain;

    wcout << "Input text: ";

    getline(wcin, wplain);

    wcin.ignore(10, L'\n');

    if (wplain == L"" || wplain == L"\n" || wplain == L"\r\n")

    {

        wcerr << L"Sussy text!" << endl;

        exit(1);

    }

    return wstring\_to\_string(wplain);

}

**5. Exercise 6 :**

**Text

Description automatically generated**

**Use keygen program from offical cryptopp site to generate and save key to file.**

**- rsa-private.key**

**- rsa-public.key**

        RSA::PrivateKey rsaPrivate;

        rsaPrivate.GenerateRandomWithKeySize(rnd, 3072);

        RSA::PublicKey rsaPublic(rsaPrivate);

        SavePrivateKey("rsa-private.key", rsaPrivate);

        SavePublicKey("rsa-public.key", rsaPublic);

**Then using LoadPrivateKey() and LoadPublicKey() to use the keys for Encryption/Decryption**

void LoadPrivateKey(const string& filename, PrivateKey& key)

{

    ByteQueue queue;

    Load(filename, queue);

    key.Load(queue);

}

void LoadPublicKey(const string& filename, PublicKey& key)

{

    ByteQueue queue;

    Load(filename, queue);

    key.Load(queue);

}

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