**ĐỒ ÁN 03 – LÀM QUEN VỚI OPENSSL**

**3.1. TÌM HIỂU VỀ KHÓA RSA CỦA OPENSSL**

**I. Cấu trúc của tệp chứa khóa bí mật mà OpenSSL sinh ra :**

+ Sinh khóa bí mật RSA bằng OpenSSL dùng lệnh :

$ openssl genpkey -out <priv.pem> -algorithm RSA -pkeyopt rsa\_keygen\_bits:<numbits>

+ Thực hiện tạo ra khóa bí mật 1024 bits

$ openssl genpkey -out priv.pem -algorithm RSA -pkeyopt rsa\_keygen\_bits:1024

Tệp priv.pem sẽ có dạng :

A screenshot of a computer

Description automatically generated

* 1. **Các thành phần trong file priv.pem :**

Do khi sử dụng **genpkey** command khóa bí mật được lưu ở dạng định dạng **PKCS#8** với chỉ có các kí tự nên để tìm hiểu rõ hơn các thành phần có trong file priv.pem ta sử dụng câu lệnh :

$ openssl pkey -in priv.pem -text -noout

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

**1.2. Ý nghĩa :**

Do private key sinh ra từ $ openssl genpkey -out <priv.pem> -algorithm RSA -pkeyopt rsa\_keygen\_bits:<numbits> . Openssl sử dụng thuật toán RSA tuân theo tiêu chuẩn RFC2313: PKCS #1 v1.5 nên

RSAPrivateKey ::= SEQUENCE {

modulus INTEGER, -- n

publicExponent INTEGER, -- e

privateExponent INTEGER, -- d

prime1 INTEGER, -- p

prime2 INTEGER, -- q

exponent1 INTEGER, -- d mod (p-1)

exponent2 INTEGER, -- d mod (q-1)

coefficient INTEGER -- (inverse of q) mod p

}

Với + modulus là là số n trong hệ mã RSA

+ publicExponent là số mũ công khai e

+ privateExponent là số mũ bí mật d

+ prime1 là số nguyên tố p

+ prime2 là số nguyên tố q

+ exponent1 là d mod (p-1)

+ exponent2 là d mod (q -1)

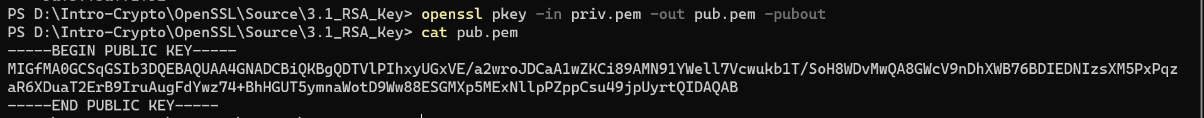
+ coffiecient là số nghịch đảo (q-1 mod p ) sử dụng định lý Số dư Trung Hoa

**II. Cấu trúc khóa công khai mà OpenSSL sinh ra :**

Sau khi có khóa bí mật, ta sẽ thực hiện sinh khóa công khai với OpenSSL bằng lệnh :

$openssl pkey -in <priv.pem> -out <pub.pem> -pubout

Tệp pub.pem sẽ có dạng :

  
Tương tự như private key **genpkey** command tạo khóa công khai cũngđược lưu ở dạng định dạng **PKCS#8** với chỉ có các kí tự.

**2.1. Các thành phần trong pub.pem :**

+ Thực ra bản chất của câu lệnh là trích xuất cách thành phần của public key (n , e) từ private key đã có.

**A screen shot of a computer code

Description automatically generated**

Các thành phần trong **pub.pem** tuân theo tiêu chuẩn RFC2313: PKCS #1 v1.5 khóa public key phải là loại ASN.1 với cấu trúc như sau :

RSAPublicKey ::= SEQUENCE {

modulus INTEGER, -- n

publicExponent INTEGER -- e

}

**2.2. Ý nghĩa :**

+ modulus số n

+ publlicExponents : số mũ công khai e

**III. Mã nguồn :**

Chương trình đọc các tệp chứa khóa bí mật <priv.pem> và khóa công khai <pub.pem> mà OpenSSL sinh ra, xuất ra màn hình các thành phần có trong tệp đó.

**3.1) Mã nguồn :**

Trong thư mục **/Source/3.1\_RSA\_Key/RSA\_Key.py**

**3.2) Ngôn ngữ lập trình :** **Python verison 3.11.4 , openssl command** sử dụng **openssl version 3.2.0**

**3.3) Môi trường chạy thử nghiệm :** Windown 11, 64 bits

**3.4) Thư viện cần cài đặt :** **cryptography**

Cách thức cài đặt :

pip install cryptography

Cách thức chạy chương trình :

$python RSA\_Key.py <priv.pem> <pub.pem>

<priv.pem> : Đường dẫn đến file private key

<pub.pem> : Đường dẫn đến file public key

**3.5) Video demo :**

Video demo được tải lên youtube, đường dẫn truy cập :

**<https://youtu.be/x4hwtbuk8BU>**

**IV. Tài liệu tham khảo :**

OPENSSL COOKBOOK, third edition, Ivan Ristic

<https://www.openssl.org/docs/man1.1.1/man1/openssl-genpkey.html>