**ĐỒ ÁN 03 – LÀM QUEN VỚI OPENSSL**

**3.2. TÌM HIỂU VỀ MÃ HÓA KHÓA CÔNG KHAI RSA CỦA OPENSSL**

**I. Cách OpenSSL mã hóa các tệp tin :**

Sau khi đã có khóa công khai RSA chứa trong tệp <pub.pem> Ta thực hiện mã hóa với câu lệnh :

**$openssl pkeyutl -in <plain> -out <cipher> -inkey <pub.pem> -pubin -encrypt**

Trong đó:

• <plain> là tệp chứa bản rõ

• <cipher> là tệp chứa bản mã sau khi được mã hóa

• <pub.pem> là tệp tin chứa khóa công khai RSA mà OpenSSL sinh ra.

Theo tài liệu tham khảo của openssl pkeyutl nhận vào khóa công khai <pub.pem> được tạo ở phần 3.1 sử dụng RSA padding scheme : PCKS#1 v1.5

Len(n) bytes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0x00 | 0x002 | Random non-zero bytes | 0x00 | Message |

Padding used for RSA encryption

**Các bước thực hiện mã hóa**

**+Bước 1 :** Thông điệp đọc từ <plain> sẽ chuyển về mã nhị phân và được thêm vào padding như ở trên ta được thông điệp mới tạm gọi là m

**+Bước 2 :** Từ file <pub.pem> có được n, e ( modulus , public exponent)

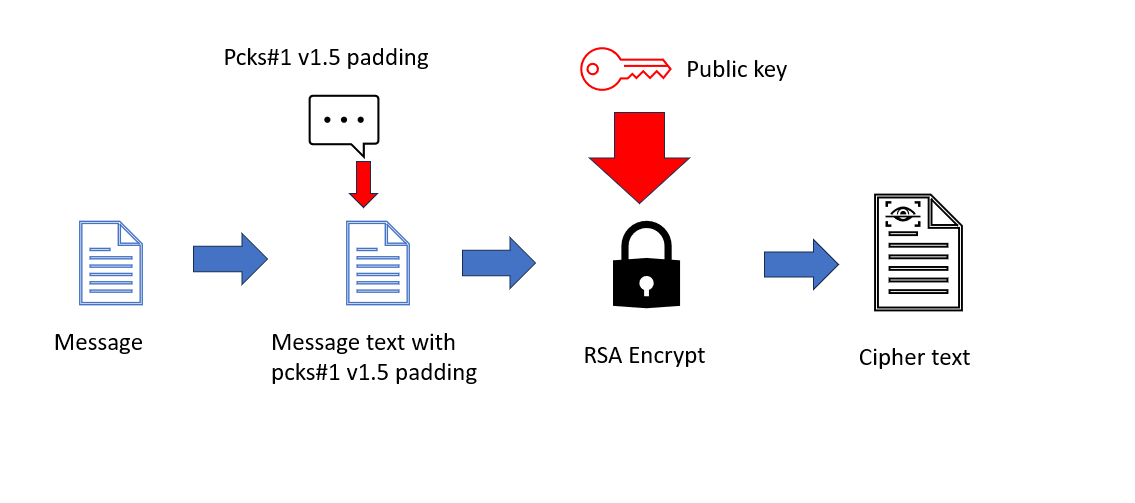
Thực hiện mã hóa theo thuật toán RSA

Public exponent

c = me mod (n)

ciphertext message đã thêm padding modulus

**+Bước 3 :** Lưu c đã được mã hóa vào <cipher >



*H1. Sơ đồ minh họa OpenSSL Encrypt sử dụng thuật toán RSA*

**II. Cách OpenSSL giải mã các tệp tin :**

Sau khi đã có khóa bí mật RSA chứa trong tệp <priv.pem> ta thực hiện việc giải mã với với câu lệnh :

**$ openssl pkeyutl -in <cipher> -out <plain> -inkey <priv.pem> -decrypt**

Trong đó :

• <cipher> là tệp chứa bản mã,

• <plain> là tệp chứa bản rõ sau khi được giải mã.

• <priv.pem> là tệp tin chứa khóa bí mật RSA mà OpenSSL sinh ra.

**Các bước thực hiện giải mã :**

**+ Bước 1 :** Từ file <priv.pem> có được n, d ( modulus, private exponent)

**+ Bước 2** : Đọc và file <cipher>và thực hiện giải mã theo thuật toán RSA

Private exponent

m = cd mod (n)

message with padding ciphertext modulus

**+ Bước 3 :** Chuỗi thông điệp thu được vẫn còn padding scheme : PCKS#1 v1.5

Len(n) bytes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0x00 | 0x002 | Random non-zero bytes | 0x00 | Message |

Padding used for RSA encryption

Thực hiện cắt bỏ phần padding và thu được thông điệp cần giải mã message

+ **Bước 4 :** Ghi thông điệp đã giải mã vào file <plain>

A diagram of a computer security system

Description automatically generated

**III. Mã nguồn**

**3.1) Mã nguồn :**

Chương trình mã hóa đọc tệp chứa khóa công khai <pub.pem> và

tệp chứa bản rõ <plain>, xuất ra tệp chứa bản mã sau khi mã hóa <cipher>.

Trong thư mục : **Source/3.2\_RSA\_Encrypt\_Decrypt/RSA\_Encrypt.py**

Chương trình giải mã đọc tệp chứa khóa bí mật <priv.pem> và tệp

chứa bản mã <cipher>, xuất ra tệp chứa bản rõ sau khi giải mã <plain>.

Trong thư mục : **Source/3.2\_RSA\_Encrypt\_Decrypt/RSA\_Decrypt.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\_Encrypt.py <pub.pem> <plain> <cipher>

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

<plain> : Đường dẫn đến file chứa bản rõ plaintext

<cipher> : Đường dẫn đến file chứa thông điệp mà chương trình đã mã hóa

$python RSA\_Decrypt.py <priv.pem> <cipher> <decrypt>

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

<cipher> : Đường dẫn đến file chứa thông điệp mã hóa

<decrypt> : Đường dẫn đến file chứa thông điệp mà chương trình đã giải mã

**3.5) Video demo :**

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

<https://youtu.be/Uby9ANUvO6M>

**IV) Tài liệu tham khảo :**

<https://www.rfc-editor.org/rfc/rfc2313>

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