TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

ĐẠI HỌC QUỐC GIA HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

ꕥ

BÁO CÁO ĐỒ ÁN 03

LÀM QUEN VỚI OPENSSL

GIẢNG VIÊN: Nguyen Dinh Thuc

Lớp: 21CNTThuc

Lâm Thiều Huy 21127056

A. Tìm hiểu về khóa RSA của OpenSSL

1. Giới Thiệu

- Ngôn ngữ lập trình: python
- Các thư viện cài đặt: subprocess và crypto from openssl

2. Tệp Chứa Khóa Bí Mật (priv.pem)

2.1 Cấu Trúc Tệp

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQD3H5lv5UY7g5Q2
L6s6Lk1utal2pxcP6CuOY7mnepyGEchG7q4ASQFo8GILJVJqgUM1hnrcqbduNGsr
vJ7FSUM1ET66yWPmHW77GSP6aqQsAGQ5cBLRD0jst13q9d4mVPrUS+jyzocXUG3z
U69j8hJebfdD2am30yts/B8KGyt9XZEiMpE+6GQrTKX8fojjKojx2TGSZnkqMubr
GhL/jqRhdZjdWmZx5M9a4S+cpeP88xbD/zSxL5bLQar0+8MwRNdejMgD7DJBn69i
AFI1zOvyG49zBpa3SOFQ/yh3wP8Zf9N/JsqyCBkKpEl8Xk+Zcre4/zNDMOFgOAPD
1bzcTtu9AgMBAAECggEABkXLj78KltUirHNuTbZCKea7i/L2z2UNwfn/CuS+V1rZ
Mg+54/D2c7LyUiUa3/AzBAdLVBGMwePbuor5nrla1tx+sqANBJjHqeD7/E27qBBE
ev7Aw4S3Tabj3+RoxKFQkpXwrkUWwb09ZTlBEPDijXoOFi9OswdNqWEG6qtA4dgy
42qCq1gaHC2uTo/MVG04ZNA0WMPOdgqvwPbhZbD64ExXfzZGqV+3BNElviMHkscR
a9DHCQr0nnwHFeUutWFVmiSEoE1TVnuXza7/esB0zLgx5IGSsZ8Z7SatTzRCyO9f
fkpA9Qy9KdYpNAWcwaJwBnhHT6hRp5VhJm/urDvxAQKBgQD+BGVZxShMyvdb6q7u
lRFqe/OZ4LmnhY3lVeQqTQtGpvwG4zb69qlw76ECCYclFA1ADK0q/vYkGVR6MCay
rxqbLoQ3FsJLjT8SbRdMRpgoL0ql116Z+O7eY8hwdoweY4fcdWV3k6sqnyc+0JIb
T23Rjb/8xfFGUGfJTvpjl3KggQKBgQD5DW17hLY/zo1ip6+cHf/BHp/ufnt2LW6i
/iUAiiKiZggHdzX7u4BAjxUAhHVa1RnS4v7OFy3hlW8QngKZxFUYy8EKrtg9YCHH
7VK433Eo11yNePVw+rV+O4dxAG0gi8cdfHGltk0zlThmSS5YQxBqm4qnYRDto9pF
uASm4dAdPQKBgQCCg62zfzqiolKQFrgE+/Cz3rYeZTne2h87K3ONTIKzrY6m103j
iqMq1OTMUCrxISlhtGGxSskbaSxfj6gCfTfVbgQe7gGsogk7JXQoC8mYNBxNs6f2
wtGw0GInbrG113vyCRu2Ydg7kQSwIKhBggEx/3wam3XJo/x/kaXTT/hkgQKBgQC5
BunMt1by5pCRt8S2tm7Y2di1xdARh0VH4Io68WUzw5u5eC5p++4XiHVw8feB6QoL
a8sj74KNsohWDx4dgQg7qLydJDLQvke6ka1AXfhjAETpcfDe49PMmYtRP6DTaiUe
2eJQ27RVW0oQa9P7jK94lGAZY/rAole6LjF+jgsgfQKBgQCP3VF/mbTTOQKPI+us
PtjbjOmuZks/CAF3auSYdq+SHjEJnMJmylGTD0Bg5PMIA4gr1UEqMxWNs+XW0wS1
ks6BRhe++tkvJeC0I5AZFt9liqm6Se55QMd7InMVmnhE1t50fGIGwHQLrVHEWhEq
2KcFqYQGHP/Kgmhig5nDM4irXQ==
-----END PRIVATE KEY-----
```

2.2 Các Thành Phần và Ý Nghĩa

a. Các thành phần :

- Algorithm: RSA

- Modulus (N):

c00abce312697b87191f23a8c729ddfb1d12907365338f5bc12beb8974ab11c21776434d88f9b75bdc4de2d
28e53daff9fad155813923953880f3ae4584aed59bfc821735f2fc5ad408d3305175af8c2bf531e562c63fc8be
8e2a9f24a1ad2f14ebfd1589aabb619e3b793b8cca252c15d34e9022fd7cc8227753aa925ea91c54929885b3
7657fb9a957a046e422830d6cf6351e65b4303d58ee36bc93ecb2e40feda714f9591d420c9e6befb5ef99f17f
307ef8a2b626f99924d96f6dbd7cd6189162b1b0e9e0dfb5527961f53cc6ea14b302e4f8be6ada2c5d7f81591
7359d0ebfb8b88a875e51805d71c05b64f53cf3bedf59ea572bbe84816d8e37b15319

- Public Exponent (e): 10001

- Private Exponent (d):
30aba8027e9c982f7d98ec3f2eb6b82917cda8296ec919f89da5056d5151b7cef28648f9621133bcc6c1408e
af7ea61ea9f7c2548fa53bfd251b0308732e0e28745802ce4c1dfde1f25db6c4000ed0c3fe9c50b07350a5e54
991049440deba7e68c0698ca4aa871cd99f2183b0ed24bf17e1bc7a0ee908ce25b4eab88ac0ffcf495f66d9ba
5681c3ff5aa707823260d42804e3fe8cf512304365a2b696f4eb6ad09cda31a2e389931fa5956d66f2f958c56
92ce81d5629a7641f6a6e8e55dd5b908d9659b733c8b3f62bb0108ff5bd78545a7f8861a0cea5f782bb4944b
50dea4554e55115f6779640ed33bdf2ee56948e2eea219bf11d1cc52f9cdedb0d934f

- Prime 1 (p):
ddc249f244c2ff5006d9cc2167fd23baa94902b6ef424a5d1c37a3751d7e9a914885d164843d85c0574e3b32
e3cd01bf0a50cbcceee4f0e9d449c646701e1a3c348516e284a11714082d238055f81e2202fbeb3611189d25
1d85e463d3310a99fd27dc77ab041583729b5cd74c773e7cdbbced1bd026361c796b7fc75051d09f

- Prime 2 (q):
ddb1cad998f780814aa8b38dae1dc20cc4e8aacf743b35faa9447ecabf2dbb9a8876ef426887386e0fa70e5ff3
d850bb47c0e472e9ef6ba8b4e2201983176ed905f63210ab4d4072a16620a62e9a6ae5d58bc8bb906675c9b
d55fe9af9e6288e6b9c06fa68abcdd6702989b6e6f565a253d546618cff8d7f6be158d1df092947

- Exponent 1 (d mod (p-1)):
5b1fa5272a5e3e6f7201394258eaca2dbfb642a94d339e3f18833c65b992f68cd0923c72e36c2c73d6ec4ca32
2bc71054185e5d8f629995d5c605c5b4162fd40d40c04555c4e9d9f1ba500bb9197fd39d8a410090d8961b9
88a2263166ecf60044e8864d9e367568a8457326fd42daa88fdad84bdf827425cb370330b1ae8cdd

- Exponent 2 (d mod (q-1)):
d6a438de0cb834f6f92df50a0bb64c16c8deebe2078afc6c404e4ce447cd23822ef5d818d7d373d33bdc6692
8828bba1578b6ea3c3d346cd04b49a9798d0ab45fbfbade56db551dcaa5f92e4d2e236f56797fb357e4d7565
69a744e70f64c38780b08421160ea13029504e4183c3bc2f3a3397fd02e2ba40d056520480890229

- Coefficient (q^-1 mod p):
a8c45a857d7b2d0209eed7f422bba3a01beb81c64c2ff76d3e705c04234e41acdf7286d6f107fd4ed909c2276
9e0aa038ae4fdcd7e608365de9d66e6efbea46bebfd26cb6872dc14d634f1903a4d2c40599fed326b19f0c07e
937c454f079b98be3c8ac1e845d844958f39e7297cbc27d468c3f023983748c587e3f392029db1

b. Ý nghĩa của các thành phần :
• **Mô tả Thuật toán RSA:** Đây là một phương pháp mã hóa dựa trên khóa công khai, với độ phức tạp chính nằm ở việc phân tích các số lớn thành các thừa số nguyên tố.

• Modulus (N): N là kết quả của việc nhân hai số nguyên tố lớn p và q với nhau. Đây là trọng tâm của sự an toàn trong RSA, do khó khăn trong việc tách N ra thành p và q. N được thể hiện dưới dạng một chuỗi số hexa dài, tượng trưng cho một giá trị rất lớn.

• Hệ số Mũ Công Khai (e): Thường là một số cố định như 65537, e được dùng cùng với N trong quá trình mã hóa và tạo chữ ký.

• Hệ số Mũ Bí Mật (d): Là yếu tố then chốt của khóa bí mật, dùng cho việc giải mã và ký số. d được tính bằng cách lấy nghịch đảo mô-đun của e theo modulo (p-1)*(q-1).

• Số Nguyên tố thứ Nhất (p) và thứ Hai (q): Là hai số nguyên tố lớn và được giữ kín, chúng là những yếu tố tạo ra N. Việc bảo mật chúng là quan trọng cho độ an toàn của hệ thống.

• Hệ số Mũ 1 và 2: Là d mod (p-1) và d mod (q-1) tương ứng. Chúng được dùng trong thuật toán giải mã CRT để tăng cường tốc độ giải mã.

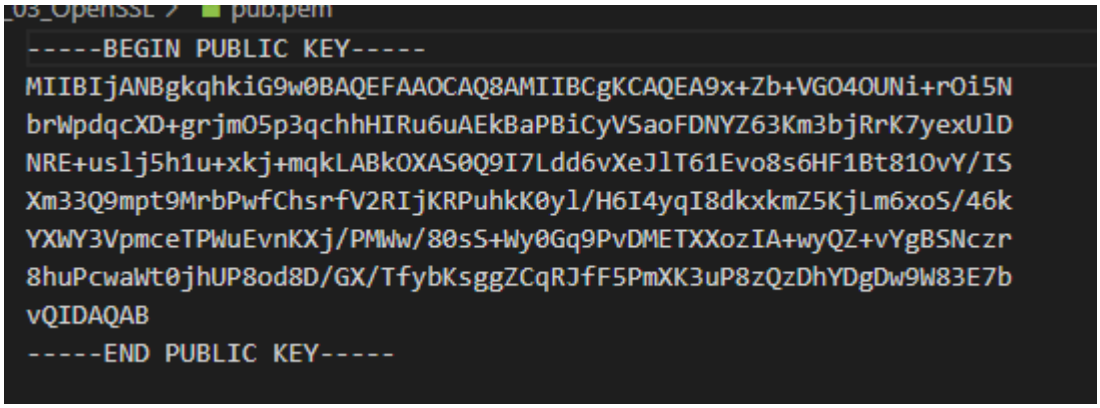
• Hệ số (q^-1 mod p): Được áp dụng trong thuật toán CRT để hỗ trợ tái tạo nhanh chóng thông điệp gốc trong quá trình giải mã.

- Tầm Quan Trọng của Khóa Bí Mật:
+ Các yếu tố của khóa bí mật đều có mối quan hệ chặt chẽ với nhau và với quy trình mã hóa/giải mã trong RSA. Độ an toàn của chúng là chìa khóa quyết định an ninh của hệ thống.
+ Modulus (N) cùng với các số nguyên tố p và q cần được giữ bí mật, vì việc lộ ra chúng có thể làm suy yếu hệ thống mã hóa.
+ Hệ số Mũ Bí Mật (d) chính là yếu tố cần thiết để giải mã và cần được bảo vệ tối đa.

c. Kết Luận:
• Việc hiểu biết chi tiết về cấu trúc và chức năng của từng bộ phận trong khóa bí mật RSA là quan trọng để đánh giá và thực hiện các biện pháp an ninh mật mã hiệu quả.
• Việc bảo vệ và quản lý khóa bí mật cần được tiến hành một cách cẩn trọng để đảm bảo sự an toàn của hệ thống mật mã.

3. Tệp Chứa Khóa Công Khai (pub.pem)

3.1 Cấu Trúc Tệp



3.2 Các Thành Phần và Ý Nghĩa

a. Các thành phần :

- Algorithm: RSA

- Modulus (N):
c00abce312697b87191f23a8c729ddfb1d12907365338f5bc12beb8974ab11c21776434d88f9b75bdc4de2d
28e53daff9fad155813923953880f3ae4584aed59bfc821735f2fc5ad408d3305175af8c2bf531e562c63fc8be
8e2a9f24a1ad2f14ebfd1589aabb619e3b793b8cca252c15d34e9022fd7cc8227753aa925ea91c54929885b3

7657fb9a957a046e422830d6cf6351e65b4303d58ee36bc93ecb2e40feda714f9591d420c9e6befb5ef99f17f
307ef8a2b626f99924d96f6dbd7cd6189162b1b0e9e0dfb5527961f53cc6ea14b302e4f8be6ada2c5d7f81591
7359d0ebfb8b88a875e51805d71c05b64f53cf3bedf59ea572bbe84816d8e37b15319

- Exponent (e): 10001

b. Ý nghĩa của các thành phần :

• Mô tả Thuật toán RSA: Đây là một phương pháp mã hóa khóa công khai phổ biến, được ứng dụng rộng rãi trong việc mã hóa dữ liệu và tạo chữ ký số.

• Modulus (N): Là phần quan trọng nhất của khóa, tạo ra từ việc nhân hai số nguyên tố được dùng trong khóa bí mật. N là yếu tố chung giữa khóa công khai và khóa bí mật.

• Hệ số Mũ Công Khai (e): Là một số nguyên nhỏ, thường là 65537. e được sử dụng kết hợp với N trong các hoạt động mã hóa và tạo chữ ký số.

- Tầm Quan Trọng của Khóa Công Khai:
+ N và e là duy nhất và quan trọng cho việc mã hóa dữ liệu.
+ Việc công khai N và e không gây rủi ro cho an ninh của khóa bí mật, tuy nhiên, chúng cần được lựa chọn một cách cẩn trọng để bảo đảm tính an toàn và bảo mật của toàn bộ hệ thống.

c. Kết Luận:

Khóa công khai trong hệ thống RSA giữ một vai trò không thể thiếu trong quá trình mã hóa và tạo chữ ký số, đóng góp vào việc đảm bảo an ninh thông tin trong giao tiếp điện tử.

B. Tìm hiểu về cách mã hóa và giải mã của OpenSSL đối với hệ mã RSA.

1. Giới Thiệu

Quy trình:

Tạo Khóa và Chứng Chỉ

I. Tạo Khóa Riêng (priv.pem): Đây là bước đầu tiên trong quá trình tạo khóa.

II. Tạo Khóa Công Khai và Chứng Chỉ (pub.pem): Tiếp theo là tạo khóa công khai cùng với chứng chỉ đi kèm.

Mã Hóa và giải mã Dữ Liệu

I. Mã Hóa:

- Dữ liệu được mã hóa dùng khóa công khai RSA.
- Có thể sử dụng lệnh openssl rsautl -encrypt -pubin -inkey public_key.pem để thực hiện việc mã hóa.
- Chỉ có người sở hữu khóa riêng mới có khả năng giải mã dữ liệu này.

II. Giải Mã:

- Dữ liệu giải mã dùng khóa riêng RSA.
- Lệnh openssl rsautl -decrypt -inkey private_key.pem được dùng cho việc giải mã.
- Điều này bảo đảm chỉ có người sở hữu khóa riêng mới có quyền truy cập vào thông tin đã được mã hóa.

2. Mã Hóa Sử Dụng Khóa Công Khai (pub.pem)

Mã Giả:

```
function encrypt(data, publicKeyFile) { publicKey =
  loadKeyFromFile(publicKeyFile)encryptedData =
  rsaEncrypt(data, publicKey) return encryptedData
}
```

Sử Dụng OpenSSL:

!openssl pkeyutl -in plain.txt -out cipher.txt -inkey pub.pem -pubin -encrypt

Sơ Đồ:

[Plain Text] --> |OpenSSL Encrypt| --> [Encrypted Data]

3. Giải Mã Sử Dụng Khóa Bí Mật (priv.pem)

Mã Giả:

```
function decrypt(encryptedData, privateKeyFile) {
    privateKey = loadKeyFromFile(privateKeyFile)
    data = rsaDecrypt(encryptedData, privateKey)
    return data
}
```

Sử Dụng OpenSSL:

! openssl pkeyutl -in cipher.txt -out decrypted.txt -inkey priv.pem -decrypt

Sơ Đồ:

[Encrypted Data] --> |OpenSSL Decrypt| --> [Decrypted Plain Text]

3. Kết Luận

OpenSSL áp dụng phương pháp mã hóa dữ liệu dựa trên khóa công khai, với mục đích bảo vệ thông tin sao cho chỉ có thể được giải mã bởi khóa riêng tương ứng. Điều này giúp đảm bảo an toàn cho dữ liệu khi truyền tải qua môi trường không bảo mật như Internet, ngăn chặn việc thông tin bị đọc hoặc bị thay đổi bởi những người không có quyền truy cập.

C. Tìm hiểu về chữ ký điện tử RSA của OpenSSL

1. Giới Thiệu

Quy trình:

Tạo Khóa và Chứng Chỉ

I. Tạo Khóa Riêng (priv.pem): Bước đầu tiên trong việc tạo khóa.

II. Tạo Khóa Công Khai và Chứng Chỉ (pub.pem): Tiếp theo, tạo ra khóa công khai cùng với chứng chỉ tương ứng.

Ký và xác thực Tệp Tin

I. Tạo Chữ Kí điện tử :

- OpenSSL dùng khóa riêng (priv.pem) để tạo ra chữ ký số cho tệp tin.
- Quá trình này bảo đảm rằng chỉ có người sở hữu khóa riêng mới có khả năng ký vào tệp tin.
- Chữ ký số này thường được gắn kèm hoặc đi kèm với tệp tin gốc.

II. Xác Thực Tệp Tin:

- Để xác thực chữ ký của tệp tin, người nhận sử dụng khóa công khai (pub.pem) của người đã ký.
- Sử dụng OpenSSL để kiểm tra và xác minh chữ ký với khóa công khai.
- Nếu chữ ký được xác minh là hợp lệ, điều này chứng tỏ rằng tệp tin đã được ký bởi chủ sở hữu của khóa riêng và không bị chỉnh sửa từ thời điểm ký.

2. Tạo Chữ Ký Điện Tử

Mã Giả:

```
function verifyMessage(messageFile, signatureFile, publicKeyFile) {
    message = loadFile(messageFile)
    signature = loadFile(signatureFile)
    publicKey = loadKey(publicKeyFile)
    isValid = rsaVerify(message, signature, publicKey)
    return isValid
}
```

Sơ Đồ:

[Message in mess_in.txt] --(RSA Sign)--> [Signature in sign.txt]

3. Xác Thực Chữ Ký Điện Tử

Mã Giả:

```
function verifyMessage(messageFile, signatureFile, publicKeyFile) {
    message = loadFile(messageFile)
    signature = loadFile(signatureFile)
    publicKey = loadKey(publicKeyFile)
    isValid = rsaVerify(message, signature, publicKey)
    return isValid
}
```

Sử Dụng OpenSSL:

```
!openssl pkeyutl -in mess_out.txt -sigfile sign.txt -inkey pub.pem -pubin -verify
```

Sơ Đồ:

[Signature in sign.txt] + [Message in mess_out.txt] --(RSA Verify)--> [Validity Status]

3. Kết Luận

Quá trình tạo chữ ký số và xác nhận chữ ký điện tử bằng OpenSSL bảo đảm rằng nội dung tin nhắn không bị biến đổi kể từ khi nó được ký, và chỉ người sở hữu khóa riêng mới có thể thực hiện việc ký này. Đây là một yếu tố then chốt trong việc đảm bảo an toàn thông tin điện tử và xác định rõ ràng tác giả của các tài liệu số.