**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: XÁC SUẤT THỐNG KÊ VÀ PHÂN TÍCH DỮ LIỆU**

**ĐỀ TÀI: GỬI CV AN TOÀN CÓ KIỂM TRA IP**

**Giáo viên hướng dẫn: ThS. Lê Thị Thùy Trang**

**Sinh viên thực hiện:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Mã sv** | **Họ và tên** | **Lớp** |
| 1 | 1771020190 | Đồng Lâm Dũng | CNTT-17-13 |
| 2 | 1771020573 | Nguyễn Huy Quang | CNTT-17-13 |
| 3 | 1771020015 | Lò Lê Anh | CNTT-17-13 |

**Hà Nội, năm 2025**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: XÁC SUẤT THỐNG KÊ VÀ PHÂN TÍCH DỮ LIỆU**

**ĐỀ TÀI: GỬI CV AN TOÀN CÓ KIỂM TRA IP**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Mã Sinh Viên | Họ và Tên | Ngày Sinh | Điểm | |
| Bằng Số | Bằng Chữ |
| 1 | 1771020190 | Đồng Lâm Dũng | 20/10/2005 |  |  |
| 2 | 1771020573 | Nguyễn Huy Quang | 28/12/2005 |  |  |
| 3 | 1771020015 | Lò Lê Anh | 11/02/2005 |  |  |

### 

### CÁN BỘ CHẤM THI

**Hà Nội, năm 2025**

**LỜI NÓI ĐẦU**

Công nghệ phát triển mạnh mẽ, nhu cầu trao đổi thông tin qua mạng Internet ngày càng phổ biến, đặc biệt là trong các hoạt động như tuyển dụng trực tuyến. Các tài liệu quan trọng như hồ sơ xin việc (CV) thường được gửi qua email hoặc hệ thống điện tử, mang theo nhiều thông tin cá nhân nhạy cảm. Tuy nhiên, nếu không có cơ chế bảo mật phù hợp, những dữ liệu này hoàn toàn có thể bị rò rỉ, giả mạo hoặc bị khai thác bởi các đối tượng xấu.

Trong bối cảnh đó, việc áp dụng các phương pháp bảo mật để đảm bảo tính bí mật, toàn vẹn và xác thực của dữ liệu là một yêu cầu cấp thiết. Đặc biệt, trong môi trường gửi và nhận CV trực tuyến, ngoài việc mã hóa nội dung, còn cần kiểm tra địa chỉ IP người gửi để xác minh nguồn gốc hợp lệ và tránh các hành vi tấn công từ xa.

Đề tài “Gửi CV an toàn có kiểm tra IP” được xây dựng nhằm mô phỏng một quy trình gửi tài liệu nhạy cảm trong môi trường mạng, trong đó sử dụng kết hợp các kỹ thuật như mã hóa đối xứng AES, ký số bằng RSA, kiểm tra tính toàn vẹn bằng SHA-512, và kiểm tra địa chỉ IP để đảm bảo an toàn thông tin cho cả người gửi lẫn hệ thống tiếp nhận.

Thông qua việc thực hiện đề tài này, nhóm thực hiện có cơ hội tiếp cận và vận dụng các kiến thức lý thuyết đã học trong môn Nhập môn An toàn và Bảo mật Thông tin vào một bài toán mang tính thực tế cao, đồng thời nâng cao nhận thức về vai trò quan trọng của bảo mật thông tin trong đời sống số hiện nay.

**MỤC LỤC**

[**STT 2**](#_Toc202295420)

[**Mã Sinh Viên 2**](#_Toc202295421)

[**Họ và Tên 2**](#_Toc202295422)

[**Ngày Sinh 2**](#_Toc202295423)

[**Điểm 2**](#_Toc202295424)

[**Bằng Số 2**](#_Toc202295425)

[**Bằng Chữ 2**](#_Toc202295426)

[**1 2**](#_Toc202295427)

[**1771020190 2**](#_Toc202295428)

[**Đồng Lâm Dũng 2**](#_Toc202295429)

[**20/10/2005 2**](#_Toc202295430)

[**2 2**](#_Toc202295431)

[**Nguyễn Huy Quang 2**](#_Toc202295432)

[**3 2**](#_Toc202295433)

[**1771020015 2**](#_Toc202295434)

[**Lò Lê Anh 2**](#_Toc202295435)

[**11/02/2005 2**](#_Toc202295436)

[**CÁN BỘ CHẤM THI 2**](#_Toc202295437)

[**CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI 9**](#_Toc202295438)

[**1.1. Giới thiệu chung về đề tài lựa chọn 9**](#_Toc202295439)

[**1.1.1. Bối cảnh thực tiễn 9**](#_Toc202295440)

[**1.1.2. Tầm quan trọng của bảo mật thông tin cá nhân 10**](#_Toc202295441)

[**1.2.1. Vấn đề giả mạo thông tin trong tuyển dụng 10**](#_Toc202295442)

[**1.2.2. Nhu cầu bảo mật file gửi đi 10**](#_Toc202295443)

[**1.3. Mục tiêu 11**](#_Toc202295444)

[**1.3.1. Mã hóa nội dung file CV 11**](#_Toc202295445)

[**1.3.2. Ký số để xác thực người gửi 11**](#_Toc202295446)

[**1.3.3. Kiểm tra địa chỉ IP nhằm xác minh nguồn gốc 12**](#_Toc202295447)

[**1.4. Phạm vi nghiên cứu của đề tài 12**](#_Toc202295448)

[**1.4.1. Trong nội bộ ứng dụng gửi file 12**](#_Toc202295449)

[**1.4.2. Trên môi trường mạng cục bộ hoặc internet 12**](#_Toc202295450)

[**1.5. Công nghệ sử dụng 13**](#_Toc202295451)

[**1.5.1. Thuật toán AES-CBC để mã hóa 13**](#_Toc202295452)

[**1.5.2. Thuật toán RSA (1024-bit) để ký số & trao khóa 13**](#_Toc202295453)

[**1.5.3. SHA-512 để kiểm tra toàn vẹn 13**](#_Toc202295454)

[**1.5.4. Giao tiếp qua TCP/Socket đơn giản 13**](#_Toc202295455)

[**CHƯƠNG 2. PHÂN TÍCH YÊU CẦU VÀ THIẾT KẾ ỨNG DỤNG 15**](#_Toc202295456)

[**2.1 . Mô tả thuật toán 15**](#_Toc202295457)

[**2.1.1. Các thuật toán sử dụng 18**](#_Toc202295458)

[**2.2 Phân tích mã nguồn 18**](#_Toc202295459)

[**3.1. crypto\_utils.py (tập trung): 22**](#_Toc202295460)

[**3.1.1. sign\_data(data, private\_key\_file): Tạo chữ ký số 22**](#_Toc202295461)

[**3.1.2. verify\_signature(data, signature, public\_key\_file): 23**](#_Toc202295462)

[**Xác minh chữ ký số 23**](#_Toc202295463)

[**3.1.3. get\_ip(): Lấy địa chỉ IP thật 24**](#_Toc202295464)

[**CHƯƠNG 3. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 25**](#_Toc202295465)

[**3.1 Phân tích hiệu quả 25**](#_Toc202295466)

[**3.2. Phân tích và nhận xét đặc điểm của các thuật toán sử dụng 26**](#_Toc202295467)

[**3.2.1. Thuật toán AES (Advanced Encryption Standard) 26**](#_Toc202295468)

[**3.2.2. Thuật toán RSA (Rivest–Shamir–Adleman) 27**](#_Toc202295469)

[**3.2.3. Thuật toán băm SHA-256 (Secure Hash Algorithm) 27**](#_Toc202295470)

[**3.3. Đề xuất cải tiến 28**](#_Toc202295471)

[**PHÂN CÔNG NHIỆM VỤ 33**](#_Toc202295473)

[**Hướng dẫn xếp tài liệu tham khảo 36**](#_Toc202295474)

**MỤC LỤC HÌNH ẢNH**

**Hình 1.1.1 . Gửi CV an toàn qua kiểm tra IP**

**Hình 2.2. Mã code sender.py**

**Hình 2.2. Kết quả sender.py**

**Hình 2.2. Mã code receiver.py**

**Hình 2.2. Kết quả receiver.py**

**Hình 3.1.1. Mã code sign\_data**

**Hình 3.1.2.. Mã code verify\_signature**

**Hình 3.1.3. Mã code get\_ip**

**BẢNG CÁC TỪ VIẾT TẮT**

**(Nếu có)**

|  |  |  |
| --- | --- | --- |
| **STT** | **TỪ VIẾT TẮT** | **VIẾT ĐẦY ĐỦ** |
| **1** | **ATBMTT** | **An toàn bảo mật thông tin** |
| **2** |  |  |

**CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI**

## **1.1. Giới thiệu chung về đề tài lựa chọn**

### 1.1.1. Bối cảnh thực tiễn

***Hình 1.1.1 . Gửi CV an toàn qua kiểm tra IP***

Trong thời đại công nghệ số hiện nay, các hoạt động tuyển dụng ngày càng chuyển sang hình thức trực tuyến. Ứng viên có thể gửi hồ sơ xin việc (CV) qua email, hệ thống web hoặc các nền tảng tuyển dụng trực tuyến. Tuy nhiên, cùng với sự tiện lợi là những rủi ro tiềm ẩn về an ninh và an toàn thông tin. Việc gửi một tập tin .pdf chứa thông tin cá nhân như họ tên, ngày sinh, địa chỉ, số điện thoại, trình độ học vấn… có thể dẫn đến rò rỉ dữ liệu nếu không được bảo mật đúng cách. Không những thế, trong một số trường hợp, các tập tin có thể bị chỉnh sửa, giả mạo hoặc chèn mã độc nhằm tấn công hệ thống tuyển dụng. Ngoài ra, các tập tin gửi từ nguồn không xác thực (IP lạ hoặc giả mạo) có thể gây nguy hiểm cho máy chủ hoặc phá hoại quy trình xử lý hồ sơ. Do đó, việc xây dựng một quy trình gửi CV có mã hóa nội dung, xác minh nguồn gốc người gửi qua IP, đồng thời kiểm tra tính toàn vẹn và xác thực nội dung là vô cùng cần thiết trong môi trường tuyển dụng số hóa hiện nay.

### 1.1.2. Tầm quan trọng của bảo mật thông tin cá nhân

Thông tin cá nhân là một trong những loại dữ liệu nhạy cảm và dễ bị khai thác nhất. Khi ứng viên gửi CV qua mạng, nếu không được bảo vệ cẩn thận, thông tin có thể bị rò rỉ, chỉnh sửa, hoặc bị các đối tượng xấu lợi dụng để mạo danh hoặc lừa đảo. Trong môn Nhập môn An toàn và Bảo mật Thông tin, một trong những mục tiêu chính là hiểu và áp dụng các phương pháp để bảo vệ dữ liệu khỏi những mối đe dọa phổ biến như đánh cắp, sửa đổi hoặc giả mạo. Việc áp dụng mã hóa đối xứng (AES), mã hóa bất đối xứng và ký số (RSA), hàm băm kiểm tra toàn vẹn (SHA-512), cùng với kiểm tra địa chỉ IP người gửi là những bước thực tiễn giúp đảm bảo an toàn thông tin khi truyền tải dữ liệu quan trọng như CV cá nhân. Đề tài "Gửi CV an toàn có kiểm tra IP" không chỉ giúp sinh viên áp dụng kiến thức lý thuyết vào một bài toán thực tiễn mà còn thể hiện rõ vai trò của các kỹ thuật bảo mật thông dụng trong việc bảo vệ dữ liệu cá nhân trong kỷ nguyên số.

**1.2. Lý do chọn đề tài**

### 1.2.1. Vấn đề giả mạo thông tin trong tuyển dụng

Trong môi trường tuyển dụng trực tuyến ngày nay, hầu hết các công ty đều cho phép ứng viên gửi CV qua email hoặc qua hệ thống web. Tuy nhiên, điều này cũng làm gia tăng nguy cơ xuất hiện các CV giả mạo – được gửi từ những địa chỉ IP không xác định, hoặc từ các thực thể mạo danh người dùng thật. Việc không kiểm tra được nguồn gốc gửi file dẫn đến nguy cơ bị tấn công từ chối dịch vụ (DoS), gửi mã độc đính kèm, hoặc lừa đảo để truy cập trái phép vào hệ thống nội bộ của doanh nghiệp. Trong thực tế đã có nhiều trường hợp hacker lợi dụng tính dễ dãi trong việc xử lý CV để đưa mã độc hoặc đánh cắp dữ liệu doanh nghiệp. Do đó, việc kiểm tra IP người gửi, xác minh xem đó có phải là một nguồn hợp lệ, đáng tin cậy hay không là một phần quan trọng trong quy trình tiếp nhận thông tin ứng viên, giúp hạn chế các rủi ro bảo mật.

### 1.2.2. Nhu cầu bảo mật file gửi đi

CV là tài liệu chứa nhiều thông tin cá nhân quan trọng như họ tên, ngày sinh, địa chỉ, số điện thoại, trình độ học vấn, kỹ năng và kinh nghiệm làm việc. Nếu không có biện pháp bảo mật, những dữ liệu này có thể bị đọc lén, chỉnh sửa hoặc đánh cắp trong quá trình truyền tải qua mạng. Ngoài việc kiểm tra nguồn gửi, hệ thống cũng cần đảm bảo bí mật nội dung (thông qua mã hóa), tính toàn vẹn (tránh bị sửa đổi bởi bên thứ ba), và tính xác thực (người gửi thật sự là ai). Việc triển khai các kỹ thuật như AES-CBC để mã hóa nội dung, RSA để ký số và trao đổi khóa, SHA-512 để kiểm tra toàn vẹn dữ liệu không chỉ phù hợp với kiến thức môn học mà còn có ý nghĩa thiết thực trong bảo vệ thông tin cá nhân trong thực tiễn. Chính những lý do trên đã thúc đẩy nhóm lựa chọn đề tài “Gửi CV an toàn có kiểm tra IP” làm chủ đề nghiên cứu và ứng dụng cho bài tập lớn của môn học.

## **1.3. Mục tiêu**

Đề tài “Gửi CV an toàn có kiểm tra IP” được thực hiện nhằm mục đích xây dựng một hệ thống đơn giản mô phỏng quy trình bảo mật trong việc gửi và tiếp nhận hồ sơ xin việc qua mạng. Hệ thống kết hợp các kỹ thuật mã hóa, xác thực, kiểm tra toàn vẹn và xác minh nguồn gửi để đảm bảo an toàn thông tin. Cụ thể, các mục tiêu đề ra như sau:

- Mục tiêu 1: Bảo vệ tính bí mật của nội dung CV

Sử dụng thuật toán mã hóa đối xứng AES ở chế độ CBC để mã hóa toàn bộ nội dung file CV trước khi gửi đi. Qua đó, ngăn chặn hành vi đọc trộm dữ liệu khi truyền qua mạng.

- Mục tiêu 2: Xác thực danh tính người gửi

Áp dụng kỹ thuật ký số bằng RSA để ký metadata (gồm tên file, thời gian gửi và IP) nhằm xác minh rằng file thực sự được gửi từ người dùng hợp lệ. Việc này giúp phát hiện và ngăn chặn các hành vi giả mạo, mạo danh hoặc gửi file từ các nguồn không xác định.

- Mục tiêu 3: Kiểm tra tính toàn vẹn của dữ liệu

Sử dụng hàm băm SHA-512 để tạo mã kiểm tra dữ liệu. Khi file đến được hệ thống nhận, hệ thống sẽ tính lại giá trị băm và so sánh với bản gốc để đảm bảo rằng dữ liệu không bị thay đổi, chèn sửa hay hỏng trong quá trình truyền tải.

- Mục tiêu 4: Xác minh nguồn gửi thông qua địa chỉ IP

Ghi nhận và kiểm tra địa chỉ IP của người gửi để xác định xem yêu cầu có đến từ một nguồn đáng tin cậy hay không. Điều này giúp hệ thống phát hiện các truy cập bất thường, giả mạo hoặc từ các vùng mạng trái phép, nâng cao mức độ kiểm soát và phòng vệ.

### 1.3.1. Mã hóa nội dung file CV

Một trong những mục tiêu chính của đề tài là đảm bảo tính bí mật của thông tin trong file CV trong suốt quá trình truyền tải. Để làm được điều này, nội dung file sẽ được mã hóa bằng thuật toán AES ở chế độ CBC (Cipher Block Chaining). Điều này giúp cho nội dung trong file không thể bị đọc hiểu nếu bị chặn lại hoặc truy cập trái phép trong quá trình truyền trên mạng. Mã hóa giúp đảm bảo rằng chỉ có bên nhận hợp lệ (sở hữu khóa giải mã) mới có thể đọc được nội dung của file, góp phần nâng cao tính an toàn và bảo mật cho dữ liệu cá nhân của ứng viên.

### 1.3.2. Ký số để xác thực người gửi

Để xác thực danh tính của người gửi, hệ thống áp dụng kỹ thuật ký số bằng thuật toán RSA với hàm băm SHA-512. Việc ký số được thực hiện trên metadata của file, bao gồm tên file, địa chỉ IP, và thời gian gửi. Người nhận sẽ kiểm tra chữ ký số để đảm bảo rằng file đúng là được gửi từ người gửi hợp lệ, và không bị giả mạo trong quá trình truyền. Mục tiêu này nhằm phòng ngừa các hành vi giả danh, mạo danh người gửi CV, vốn có thể gây rủi ro cao cho hệ thống tuyển dụng.

### 1.3.3. Kiểm tra địa chỉ IP nhằm xác minh nguồn gốc

Địa chỉ IP của người gửi là một trong những thông tin quan trọng để xác định nguồn gốc gửi file. Hệ thống sẽ kiểm tra IP của người gửi trong bước đầu của quy trình xử lý. Nếu IP không nằm trong danh sách hợp lệ (whitelist), hệ thống sẽ từ chối xử lý tiếp và phản hồi trạng thái lỗi. Việc kiểm tra IP giúp ngăn chặn các hành vi tấn công đến từ những nguồn không xác định, tăng cường mức độ kiểm soát truy cập vào hệ thống. 1.3.4 Đảm bảo toàn vẹn dữ liệu Toàn vẹn dữ liệu là yếu tố quan trọng trong an toàn thông tin. Trong đề tài này, hệ thống sử dụng thuật toán băm SHA-512 để tạo giá trị hash cho nội dung file đã mã hóa (gồm cả IV và ciphertext). Khi người nhận nhận được file, hệ thống sẽ tính lại giá trị băm và so sánh với giá trị đã gửi để kiểm tra xem nội dung có bị thay đổi trong quá trình truyền hay không. Mục tiêu này đảm bảo rằng file không bị sửa đổi, thêm bớt, hoặc làm hỏng trong quá trình gửi đi và nhận lại, góp phần duy trì tính tin cậy của dữ liệu.

## **1.4. Phạm vi nghiên cứu của đề tài**

### 1.4.1. Trong nội bộ ứng dụng gửi file

Đề tài tập trung vào việc xây dựng một quy trình gửi file CV an toàn từ phía người dùng đến hệ thống tuyển dụng. Phạm vi thực hiện trong nội bộ bao gồm: Mã hóa nội dung file .pdf bằng AES-CBC trước khi gửi. Ký số metadata của file (tên file, thời gian gửi, địa chỉ IP) bằng RSA để xác thực người gửi. Mã hóa khóa phiên AES bằng RSA (OAEP) để trao đổi khóa an toàn. Tạo và gửi gói dữ liệu chứa: IV, ciphertext, hash SHA-512 và chữ ký. Nhận phản hồi từ hệ thống (ACK/NACK). Phần này không triển khai hệ thống lớn hay giao diện hoàn chỉnh, mà tập trung vào mô phỏng giao tiếp giữa người gửi và người nhận thông qua dòng lệnh hoặc script đơn giản, minh họa rõ các bước bảo mật trong quy trình truyền tải thông tin.

### 1.4.2. Trên môi trường mạng cục bộ hoặc internet

Đề tài được thực hiện trên môi trường mô phỏng mạng cục bộ (LAN) hoặc có thể chạy thử qua mạng Internet tùy vào điều kiện kiểm thử. Các thành phần truyền/nhận file có thể chạy trên hai máy tính khác nhau, giao tiếp thông qua giao thức mạng TCP hoặc socket. Phạm vi không bao gồm triển khai trên nền tảng thực tế như email server, hệ thống tuyển dụng thật hay tích hợp vào web. Thay vào đó, mục tiêu là kiểm chứng quy trình mã hóa, ký số, kiểm tra IP và xác minh tính toàn vẹn trong một mô hình đơn giản nhưng đầy đủ các yếu tố cơ bản của an toàn thông tin.

## **1.5. Công nghệ sử dụng**

### 1.5.1. Thuật toán AES-CBC để mã hóa

AES (Advanced Encryption Standard) là thuật toán mã hóa đối xứng hiện đại, được sử dụng rộng rãi nhờ vào độ an toàn cao và hiệu suất tốt. Trong đề tài này, chế độ CBC (Cipher Block Chaining) được sử dụng để tăng tính bảo mật bằng cách dùng vector khởi tạo (IV) khác nhau cho mỗi lần mã hóa.

Việc sử dụng AES-CBC giúp đảm bảo rằng nội dung file CV không thể bị đọc hiểu nếu bị đánh cắp trong quá trình truyền tải. AES phù hợp cho việc mã hóa dữ liệu dung lượng vừa và nhỏ như file .pdf cá nhân.

### 1.5.2. Thuật toán RSA (1024-bit) để ký số & trao khóa

RSA là thuật toán mã hóa bất đối xứng phổ biến, dựa trên cơ sở toán học của việc phân tích số nguyên tố lớn. Trong đề tài này, RSA được sử dụng với độ dài khóa 1024-bit để:

- Ký số metadata của file nhằm xác thực người gửi (authentication).

- Mã hóa khóa phiên AES bằng RSA-OAEP, cho phép truyền khóa an toàn từ người gửi đến hệ thống nhận.

Mặc dù RSA 1024-bit không còn được xem là tối ưu cho môi trường thực tế lâu dài, nó vẫn phù hợp cho mục đích học tập, mô phỏng và minh họa nguyên lý hoạt động trong phạm vi đề tài.

### 1.5.3. SHA-512 để kiểm tra toàn vẹn

SHA-512 là một hàm băm (hash function) thuộc họ SHA-2, cho đầu ra 512 bit, dùng để tạo ra bản tóm tắt nội dung dữ liệu. Trong đề tài, SHA-512 được sử dụng để:

- Tính toán giá trị băm của IV || ciphertext.

- Đảm bảo rằng nội dung file không bị thay đổi trong quá trình gửi đi.

Bằng cách so sánh hash từ người gửi và người nhận tính được, hệ thống có thể phát hiện nếu dữ liệu đã bị sửa đổi, chen lẫn hoặc lỗi truyền tải.

### 1.5.4. Giao tiếp qua TCP/Socket đơn giản

Toàn bộ quá trình gửi và nhận file được mô phỏng thông qua giao tiếp mạng đơn giản bằng TCP socket, giữa hai ứng dụng: người gửi và người nhận. TCP được chọn vì là giao thức hướng kết nối, đảm bảo độ tin cậy khi truyền dữ liệu, giúp dữ liệu gửi đi đến đúng đích, đúng thứ tự và không bị mất gói.

Giao tiếp socket giúp mô phỏng gần thực tế quá trình trao đổi thông tin trên môi trường mạng nội bộ hoặc Internet, từ đó triển khai được quy trình kiểm tra IP, gửi file, ký số và xác minh bảo mật một cách trực quan.

**CHƯƠNG 2. PHÂN TÍCH YÊU CẦU VÀ THIẾT KẾ ỨNG DỤNG**

## **. Mô tả thuật toán**

Trong đề tài "Gửi CV an toàn có kiểm tra IP", hệ thống được thiết kế nhằm đảm bảo các yếu tố cốt lõi của an toàn thông tin: bảo mật, xác thực, toàn vẹn, và kiểm soát truy cập thông qua địa chỉ IP. Để hiện thực hóa các yêu cầu đó, hệ thống triển khai quy trình bảo mật gồm 4 giai đoạn chính:

**Giai đoạn 1: Khởi tạo giao tiếp và xác minh địa chỉ IP**

Người gửi (ứng viên) bắt đầu kết nối với hệ thống tuyển dụng.

Trong bước đầu tiên, người gửi sẽ gửi một thông điệp đơn giản như “Hello!” cùng với địa chỉ IP hiện tại

Hệ thống tiếp nhận thông điệp và kiểm tra xem IP có nằm trong danh sách các địa chỉ hợp lệ hay không

Nếu IP được chấp nhận, hệ thống phản hồi bằng thông điệp “Ready!”, báo hiệu sẵn sàng nhận dữ liệu.

Nếu IP bị từ chối (ví dụ nằm ngoài whitelist), kết nối sẽ bị đóng lại.

→ Mục tiêu bảo mật: kiểm soát truy cập và sàng lọc nguồn gửi.

**Giai đoạn 2: Sinh khóa, ký số và trao đổi khóa**

- Sinh khóa AES phiên (Session Key):

Hệ thống người gửi sinh ngẫu nhiên một khóa AES (ví dụ 256-bit) và một IV (vector khởi tạo) cho chế độ CBC.

Đây là khóa dùng tạm cho phiên làm việc hiện tại.

- Ký số metadata bằng RSA:

Metadata gồm các thông tin như tên file, timestamp, và IP người gửi.

Dữ liệu này được băm bằng SHA-512 rồi ký bằng khóa riêng RSA của người gửi để tạo ra chữ ký số.

Chữ ký số sẽ được dùng để xác thực người gửi và bảo vệ tính không thể chối bỏ.

- Mã hóa khóa phiên AES:

Để bảo vệ khóa AES, người gửi mã hóa nó bằng khóa công khai RSA của người nhận (hệ thống tuyển dụng), sử dụng chế độ mã hóa OAEP (Optimal Asymmetric Encryption Padding) kết hợp SHA-512

Kết quả là một phiên bản mã hóa của khóa phiên mà chỉ người nhận mới có thể giải mã được

→ Mục tiêu bảo mật: xác thực danh tính và đảm bảo trao đổi khóa an toàn

**Giai đoạn 3: Mã hóa nội dung CV và kiểm tra toàn vẹn**

- Mã hóa nội dung file:

Nội dung của file cv.pdf được mã hóa bằng AES-CBC sử dụng khóa và IV đã sinh

Quá trình này chuyển đổi toàn bộ nội dung file sang dạng ciphertext – không thể đọc hiểu

- Kiểm tra toàn vẹn dữ liệu:

Sau khi mã hóa xong, người gửi tạo một giá trị băm SHA-512 dựa trên chuỗi kết hợp giữa IV và ciphertext

Mục đích là để bên nhận có thể so sánh và phát hiện nếu dữ liệu bị thay đổi trong quá trình truyền

- Đóng gói toàn bộ dữ liệu:

Các thành phần sau sẽ được đóng gói để gửi đi:

+ IP người gửi

+ IV

+ Ciphertext (nội dung file đã mã hóa)

+ Hash SHA-512

+ Chữ ký RSA

+ Khóa AES đã mã hóa bằng RSA

+ Metadata gốc (tên file, thời gian gửi…)

→ Mục tiêu bảo mật: bảo vệ nội dung và tính toàn vẹn dữ liệu.

**Giai đoạn 4: Tiếp nhận, kiểm tra và phản hồi**

Kiểm tra IP:

Hệ thống kiểm tra xem IP người gửi có hợp lệ không. Nếu không, dữ liệu bị loại bỏ.

- Giải mã khóa phiên AES:

Sử dụng khóa riêng RSA, hệ thống giải mã khóa AES đã mã hóa để dùng trong bước giải mã file.

- Kiểm tra hash:

Tính lại giá trị băm từ IV và ciphertext đã nhận. So sánh với hash do người gửi cung cấp.

Nếu hai giá trị trùng nhau → dữ liệu toàn vẹn. Ngược lại → từ chối.

-Xác minh chữ ký RSA:

Sử dụng khóa công khai của người gửi để xác minh chữ ký trên metadata.

Nếu hợp lệ → chứng minh người gửi là thật.

- Giải mã nội dung:

Sử dụng AES-CBC để giải mã nội dung CV đã mã hóa, nếu tất cả các kiểm tra trên đều hợp lệ.

- Phản hồi trạng thái:

Nếu thành công → gửi lại phản hồi “ACK” (đã nhận và xác thực).

Nếu thất bại do IP, chữ ký hoặc toàn vẹn không hợp lệ → gửi phản hồi “NACK” (từ chối).

→ Mục tiêu bảo mật: hoàn tất quy trình xác minh, giải mã và phản hồi minh bạch.

Tổng kết quy trình thuật toán

|  |  |  |
| --- | --- | --- |
| Giai đoạn | Hoạt động chính | Mục tiêu bảo mật |
| 1 | Giao tiếp ban đầu + kiểm tra IP | Kiểm soát truy cập |
| 2 | Sinh khóa AES + Ký số + Mã hóa khóa | Bảo mật và xác thực |
| 3 | Mã hóa file CV + tạo hash + đóng gói | Bảo mật và toàn vẹn |
| 4 | Kiểm tra IP + hash + chữ ký + giải mã | Xác minh và xử lý an toàn |

### 2.1.1. Các thuật toán sử dụng

- RSA (file rsa\_utils.py, crypto\_utils.py): Dùng để mã hóa khóa AES, tạo và xác minh chữ ký số.

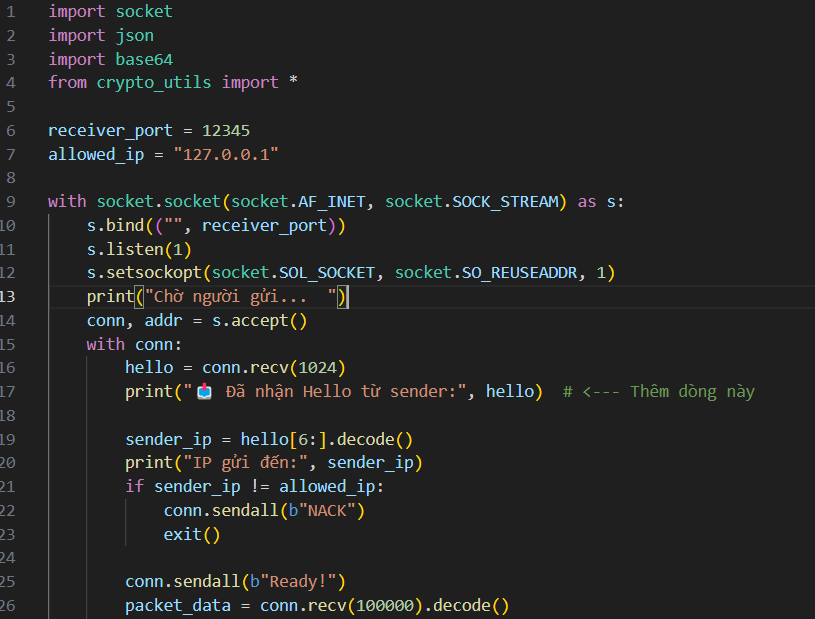
- AES (file aes\_utils.py, test\_aes.py): Mã hóa nội dung CV (file PDF).

- SHA-256: Băm nội dung để tạo chữ ký số.

- Kiểm tra IP (trong sender.py và receiver.py): Lấy IP người gửi, kiểm tra tính hợp lệ.

## **2.2 Phân tích mã nguồn**

**1. sender.py**

****

****

***Hình 2.2. Mã code sender.py***

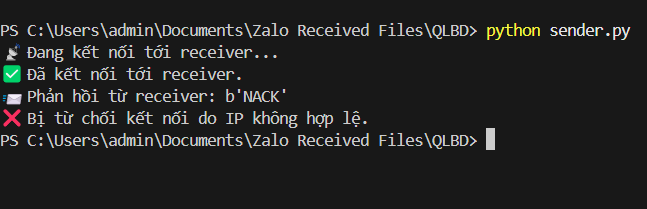
* Tác vụ chính:
  + Mã hóa file cv.pdf bằng AES.

ciphertext = aes\_encrypt(file\_data, session\_key, iv)

* + Dùng RSA mã hóa khóa AES.

encrypted\_key = rsa\_encrypt(session\_key, "keys/receiver\_public.pem")

* + Tạo chữ ký số từ cv.pdf (bằng SHA-256 + RSA).
  + Gửi thông tin (file + khóa mã hóa + chữ ký + IP).

Kết quả:

***Hình 2.2. Kết quả sender.py***

1. **receiver.py**
2. import socket
3. import json
4. import base64
5. from crypto\_utils import \*
6. receiver\_port = 12345
7. allowed\_ip = "127.0.0.1"
8. with socket.socket(socket.AF\_INET, socket.SOCK\_STREAM) as s:
9. s.bind(("", receiver\_port))
10. s.listen(1)
11. s.setsockopt(socket.SOL\_SOCKET, socket.SO\_REUSEADDR, 1)
12. print("Chờ người gửi...  ")
13. conn, addr = s.accept()
14. with conn:
15. hello = conn.recv(1024)
16. print("📥 Đã nhận Hello từ sender:", hello)  # <--- Thêm dòng này
17. sender\_ip = hello[6:].decode()
18. print("IP gửi đến:", sender\_ip)
19. if sender\_ip != allowed\_ip:
20. conn.sendall(b"NACK")
21. exit()
22. conn.sendall(b"Ready!")
23. packet\_data = conn.recv(100000).decode()
24. packet = json.loads(packet\_data)
25. iv = base64.b64decode(packet["iv"])
26. cipher = base64.b64decode(packet["cipher"])
27. hash\_received = packet["hash"]
28. sig = base64.b64decode(packet["sig"])
29. metadata = base64.b64decode(packet["metadata"])
30. encrypted\_key = base64.b64decode(packet["key"])
31. session\_key = rsa\_decrypt(encrypted\_key, "keys/receiver\_private.pem")
32. if SHA512.new(iv + cipher).hexdigest() != hash\_received:
33. conn.sendall(b"NACK")
34. exit()
35. if not verify\_signature(metadata, sig, "keys/sender\_public.pem"):
36. conn.sendall(b"NACK")
37. exit()
38. plain = aes\_decrypt(cipher, session\_key, iv)
39. with open("received\_cv.pdf", "wb") as f:
40. f.write(plain)
41. print("Lưu file thành công thành: received\_cv.pdf")
42. conn.sendall(b"ACK")

***Hình 2.2. Mã code receiver.py***

* Tác vụ chính:
  + Nhận file.
  + Giải mã khóa AES bằng RSA.
  + Giải mã file CV.

plain = aes\_decrypt(cipher, session\_key, iv)

* + Xác minh chữ ký số.

if not verify\_signature(metadata, sig, "keys/sender\_public.pem"):

conn.sendall(b"NACK")

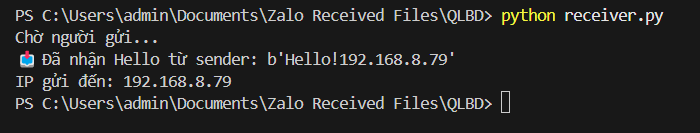
exit()

* + Kiểm tra IP gửi đến (so sánh với IP cho phép, có thể lọc whitelist/blacklist).

if sender\_ip != allowed\_ip:

conn.sendall(b"NACK")

exit()

Kết quả:

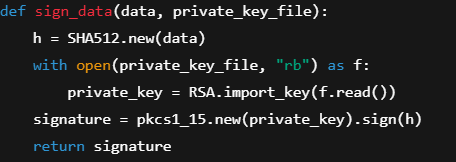
***Hình 2.2. Kết quả receiver.py***

## **3.1. crypto\_utils.py (tập trung):**

### 3.1.1. sign\_data(data, private\_key\_file): Tạo chữ ký số

Hàm này có nhiệm vụ tạo chữ ký số từ dữ liệu đầu vào. Quá trình này gồm 2 bước:

* Băm dữ liệu bằng thuật toán SHA-512 để tạo ra một “dấu vân tay” duy nhất cho nội dung.
* Ký dấu vân tay này bằng khóa riêng RSA của người gửi để tạo thành chữ ký số.
  + - Chữ ký số giúp đảm bảo tính xác thực (authentication) và không thể chối bỏ (non-repudiation), vì chỉ người sở hữu khóa riêng mới có thể ký.



***Hình 3.1.1. Mã code sign\_data***

### 3.1.2. verify\_signature(data, signature, public\_key\_file):

### Xác minh chữ ký số

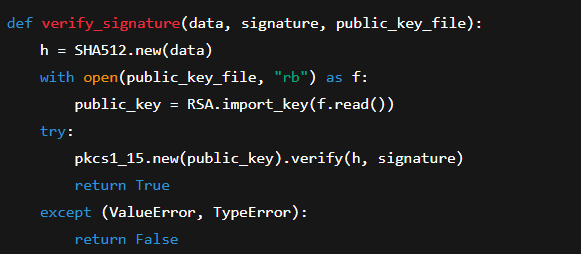
Hàm này được phía người nhận (receiver) dùng để kiểm tra xem chữ ký số có hợp lệ hay không.

Quy trình:

* Băm lại dữ liệu gốc bằng SHA-512
* Dùng khóa công khai của người gửi để kiểm tra xem chữ ký có đúng không

Nếu đúng → chứng minh rằng:

* Dữ liệu không bị sửa đổi
* Chữ ký thực sự do người gửi (người có khóa riêng) tạo ra

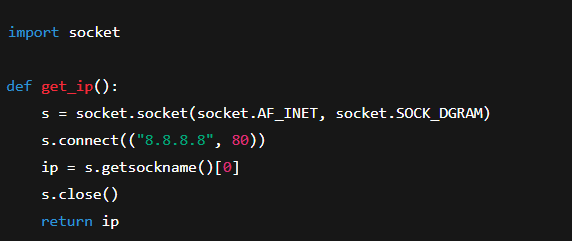


***c***

### 3.1.3. get\_ip(): Lấy địa chỉ IP thật

Chức năng này chưa thấy trong file bạn gửi, nhưng nếu thêm thì logic sẽ như sau:

Trong một số hệ thống thực tế, ta cần lấy địa chỉ IP thật của thiết bị người gửi để log hoặc kiểm tra tính hợp lệ (ví dụ khi kết nối từ xa hoặc dùng nhiều card mạng). Hàm get\_ip() có thể dùng socket để lấy IP hiện hành.



***Hình 3.1.3. Mã code* get\_ip**

**CHƯƠNG 3. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

## **3.1 Phân tích hiệu quả**

Việc truyền tải các tài liệu quan trọng như CV (Curriculum Vitae) qua mạng đòi hỏi mức độ bảo mật cao để đảm bảo rằng thông tin cá nhân của ứng viên không bị đánh cắp, giả mạo hoặc thay đổi bởi các bên thứ ba không mong muốn. Hệ thống được thiết kế trong đề tài "Gửi CV an toàn có kiểm tra IP" đã thực hiện thành công mục tiêu này bằng cách kết hợp các thuật toán mã hóa hiện đại và cơ chế kiểm tra IP nhằm nâng cao mức độ an toàn trong truyền tải dữ liệu.

- Hiệu quả về bảo mật dữ liệu

Hệ thống sử dụng mã hóa AES để bảo vệ nội dung CV. Đây là một thuật toán mã hóa đối xứng mạnh mẽ, phổ biến trong các ứng dụng thương mại và quân sự nhờ vào hiệu suất cao và mức độ bảo mật mạnh. Thông tin trong file PDF được chuyển sang dạng mã hóa trước khi gửi đi, đảm bảo rằng người trung gian hoặc kẻ tấn công không thể đọc nội dung ngay cả khi chặn được dữ liệu.

Bên cạnh đó, khóa AES được mã hóa bằng RSA – một thuật toán mã hóa bất đối xứng sử dụng cặp khóa công khai và riêng tư. Chỉ người nhận có khóa riêng tư tương ứng mới có thể giải mã khóa AES, do đó, cơ chế này ngăn chặn việc giải mã nội dung nếu người nhận không đúng đối tượng được chỉ định.

- Hiệu quả về xác thực và toàn vẹn dữ liệu

Ngoài việc mã hóa, hệ thống còn sử dụng chữ ký số dựa trên thuật toán RSA kết hợp hàm băm SHA-256 để đảm bảo tính xác thực và toàn vẹn dữ liệu. Người gửi tạo ra một mã băm từ nội dung CV rồi ký bằng khóa riêng tư của họ. Người nhận sau khi nhận được sẽ kiểm tra chữ ký bằng khóa công khai. Nếu nội dung bị thay đổi dù chỉ một ký tự, chữ ký số sẽ không còn hợp lệ – nhờ đó phát hiện được ngay sự can thiệp.

Việc xác thực thông qua chữ ký số đảm bảo rằng nội dung thật sự đến từ người gửi hợp pháp, đồng thời cũng khẳng định rằng nội dung không bị chỉnh sửa trên đường truyền.

- Hiệu quả từ kiểm tra IP

Một điểm nổi bật của hệ thống là kiểm tra IP người gửi. Việc lấy địa chỉ IP từ thiết bị gửi và gửi kèm cùng dữ liệu giúp người nhận xác định được nguồn gốc truy cập. Điều này đặc biệt hữu ích trong môi trường có yêu cầu bảo mật cao, ví dụ: chỉ chấp nhận dữ liệu từ những IP nằm trong whitelist.

Hệ thống có thể mở rộng khả năng kiểm tra IP để xác định vị trí địa lý, phát hiện truy cập đáng ngờ từ VPN hoặc IP giả mạo, từ đó ngăn chặn các hành vi gian lận hoặc giả danh.

- Tổng quan hiệu quả hệ thống

Tổng thể, hệ thống đã chứng minh hiệu quả rõ rệt ở ba khía cạnh quan trọng:

- Bảo mật cao: Nội dung CV được mã hóa bằng các thuật toán tiên tiến, ngăn chặn rò rỉ dữ liệu.

- Xác thực mạnh mẽ: Chữ ký số kết hợp với kiểm tra IP giúp người nhận xác minh rõ nguồn gốc.

- Toàn vẹn thông tin: Nếu nội dung bị chỉnh sửa, hệ thống sẽ phát hiện ngay.

Ngoài ra, hệ thống còn có tính linh hoạt, có thể triển khai dễ dàng cho các tổ chức tuyển dụng cần gửi nhận tài liệu nhạy cảm giữa các bộ phận hoặc giữa nhà tuyển dụng và ứng viên. Hệ thống cũng có khả năng mở rộng, có thể tích hợp thêm các yếu tố như OTP, bảo mật hai lớp hoặc giám sát theo thời gian thực.

Đã đáp ứng tốt các yêu cầu bảo mật trong truyền thông tin cá nhân, và có thể được áp dụng rộng rãi trong thực tế với ít điều chỉnh.

## **3.2. Phân tích và nhận xét đặc điểm của các thuật toán sử dụng**

Trong hệ thống gửi CV an toàn, ba thành phần thuật toán chính được sử dụng là AES, RSA, và SHA-256. Mỗi thuật toán đảm nhiệm một vai trò khác nhau trong việc bảo vệ dữ liệu, xác thực người gửi và đảm bảo toàn vẹn thông tin. Dưới đây là phân tích chi tiết và nhận xét về từng thuật toán:

### 3.2.1. Thuật toán AES (Advanced Encryption Standard)

- Vai trò: Mã hóa nội dung file CV (file PDF).

Loại thuật toán: Mã hóa đối xứng – dùng cùng một khóa để mã hóa và giải mã.

+ Ưu điểm:

- Tốc độ cao, phù hợp để mã hóa dữ liệu lớn như file tài liệu.

- Bảo mật mạnh với khóa 128-bit, 192-bit hoặc 256-bit.

- Được tiêu chuẩn hóa và sử dụng rộng rãi trong bảo mật công nghiệp và quốc phòng.

+ Nhược điểm:

- Cần cơ chế an toàn để trao đổi khóa (vì nếu bị lộ khóa thì dữ liệu sẽ mất an toàn).

Nhận xét:

AES rất phù hợp để mã hóa nội dung CV trong hệ thống vì tính hiệu quả và độ bảo mật cao. Tuy nhiên, việc truyền khóa AES cần được bảo vệ bởi một cơ chế khác – đây là lý do kết hợp thêm RSA.

### 3.2.2. Thuật toán RSA (Rivest–Shamir–Adleman)

Vai trò:

Mã hóa khóa AES trước khi gửi.

- Tạo và kiểm tra chữ ký số (dùng xác thực người gửi).

- Loại thuật toán: Mã hóa bất đối xứng – dùng cặp khóa công khai và khóa riêng.

+ Ưu điểm:

- Cho phép bảo mật trong trao đổi khóa (chỉ người nhận có khóa riêng mới giải mã được).

- Tạo ra chữ ký số đáng tin cậy.

- Không cần chia sẻ khóa bí mật.

+ Nhược điểm:

- Chậm hơn AES, không phù hợp để mã hóa dữ liệu lớn.

- Nếu không cẩn thận trong việc quản lý khóa riêng, dễ bị lộ.

Nhận xét:

RSA là công cụ lý tưởng để kết hợp với AES. Việc dùng RSA để mã hóa khóa AES khắc phục nhược điểm của AES về chia sẻ khóa.

Ngoài ra, chức năng chữ ký số bằng RSA đảm bảo tính xác thực và không thể chối bỏ của người gửi.

### 3.2.3. Thuật toán băm SHA-256 (Secure Hash Algorithm)

Vai trò: Tạo mã băm (hash) từ nội dung CV để phục vụ kiểm tra toàn vẹn và tạo chữ ký số.

Loại thuật toán: Thuật toán băm một chiều.

+ Ưu điểm:

- Không thể đảo ngược (không thể tạo lại dữ liệu gốc từ mã băm).

- Mọi thay đổi nhỏ trong nội dung đều dẫn đến mã băm hoàn toàn khác.

- Tốc độ xử lý nhanh và ổn định.

+ Nhược điểm:

- Không cung cấp khả năng mã hóa mà chỉ dùng để kiểm tra tính toàn vẹn.

Nhận xét:

SHA-256 hoạt động hiệu quả trong việc phát hiện sự thay đổi nội dung CV, đảm bảo rằng dữ liệu đến tay người nhận không bị chỉnh sửa. Khi kết hợp với RSA để tạo chữ ký số, thuật toán này đóng vai trò then chốt trong xác thực.

## **3.3. Đề xuất cải tiến**

Mặc dù hệ thống hiện tại đã đáp ứng được các tiêu chí cơ bản về bảo mật, xác thực và đảm bảo tính toàn vẹn của dữ liệu khi gửi CV, tuy nhiên để tăng cường khả năng ứng dụng trong thực tế và nâng cao hiệu suất, có thể thực hiện một số cải tiến sau:

🔐 1. Tích hợp xác thực hai lớp (2FA)

Vấn đề hiện tại: Việc xác thực người gửi chủ yếu dựa vào chữ ký số và địa chỉ IP. Tuy nhiên, IP có thể bị giả mạo nếu kẻ tấn công sử dụng VPN hoặc IP spoofing.

Cải tiến đề xuất: Kết hợp xác thực hai lớp (2FA), chẳng hạn như gửi mã OTP qua email hoặc số điện thoại, để đảm bảo rằng người gửi thực sự có quyền truy cập vào tài khoản.

Lợi ích: Tăng độ tin cậy trong việc xác định danh tính người gửi, giảm nguy cơ bị giả mạo.

🌍 2. Kiểm tra vị trí địa lý (GeoIP)

Vấn đề hiện tại: Chỉ kiểm tra địa chỉ IP thô, chưa phân tích được vị trí thật sự của người gửi.

Cải tiến đề xuất: Sử dụng dịch vụ tra cứu GeoIP để xác định quốc gia, khu vực, và thành phố của IP gửi. Nếu phát hiện gửi từ khu vực nghi ngờ (ví dụ quốc gia không hợp tác), có thể từ chối kết nối hoặc cảnh báo.

Lợi ích: Phát hiện sớm hành vi tấn công từ xa, nâng cao khả năng giám sát hệ thống.

📦 3. Sử dụng định dạng gói dữ liệu chuẩn (JSON + Base64)

Vấn đề hiện tại: Dữ liệu gửi đi đang ở dạng thô, phụ thuộc vào cách định dạng thủ công.

Cải tiến đề xuất: Gói toàn bộ dữ liệu (file mã hóa, khóa mã hóa, chữ ký số, IP) vào định dạng JSON, sau đó mã hóa Base64. Điều này giúp dễ truyền tải qua các giao thức mạng như HTTP hoặc WebSocket.

Lợi ích: Tăng khả năng tương thích và mở rộng, dễ tích hợp vào các hệ thống web hoặc API sau này.

🕵️ 4. Thêm cơ chế chống gửi lại (Replay Attack)

Vấn đề hiện tại: Nếu kẻ xấu ghi lại gói tin và gửi lại sau đó, hệ thống vẫn có thể chấp nhận.

Cải tiến đề xuất: Gắn kèm một timestamp (dấu thời gian) và mã định danh duy nhất trong mỗi gói dữ liệu. Người nhận sẽ kiểm tra xem gói tin có hợp lệ theo thời gian hay đã từng nhận trước đó hay chưa.

Lợi ích: Ngăn chặn các tấn công gửi lại (replay), tăng tính an toàn cho hệ thống.

🧩 5. Triển khai giao diện người dùng (GUI)

Vấn đề hiện tại: Hệ thống chạy dòng lệnh (CLI) gây khó khăn cho người dùng không chuyên.

Cải tiến đề xuất: Thiết kế giao diện người dùng đồ họa đơn giản, ví dụ bằng PyQt, Tkinter hoặc giao diện web Flask, để thực hiện gửi CV an toàn với các bước rõ ràng: chọn file, nhập khóa, xem trạng thái gửi…

Lợi ích: Tăng khả năng sử dụng thực tế, thân thiện với người dùng phổ thông, dễ triển khai cho tổ chức tuyển dụng.

💡 6. Tích hợp hệ thống lưu trữ và tra cứu log

Vấn đề hiện tại: Không có cơ chế lưu lịch sử gửi nhận hoặc theo dõi truy vết.

Cải tiến đề xuất: Tạo file log hoặc kết nối cơ sở dữ liệu nhỏ (SQLite) để lưu:

Thời gian gửi/nhận

IP người gửi

Tên file CV

Tình trạng xác thực (thành công/thất bại)

Lợi ích: Dễ dàng tra cứu và giám sát hệ thống, phục vụ việc kiểm tra và kiểm toán sau này.

✅ Kết luận mục 3.1.2:

Việc đề xuất các cải tiến trên giúp hệ thống không chỉ dừng lại ở mức "đúng chức năng" mà còn tiến tới an toàn hơn, thân thiện hơn và chuyên nghiệp hơn. Đặc biệt trong bối cảnh bảo mật mạng ngày càng phức tạp, việc bổ sung các biện pháp như kiểm tra vị trí, chống tấn công gửi lại và xác thực nhiều lớp là cần thiết để hệ thống có thể vận hành bền vững và hiệu quả trong thực tế.

**KẾT LUẬN**



***KẾT QUẢ ĐẠT ĐƯỢC***

*🔹 Về kiến thức*

*Hiểu rõ cơ bản về các thuật toán mã hóa đối xứng (AES), bất đối xứng (RSA), và hàm băm (SHA-512).*

*Nắm được cách áp dụng chữ ký số để xác thực dữ liệu.*

*Hiểu và thực hành lập trình giao tiếp mạng bằng socket TCP trong Python.*

*Áp dụng được kiến thức bảo mật vào một bài toán thực tiễn: gửi file nhạy cảm (CV) an toàn qua mạng.*

*🔹 Về sản phẩm*

*Xây dựng thành công mô hình demo gồm hai phần:*

*sender.py: Mã hóa, ký số và gửi file CV.*

*receiver.py: Xác minh IP, chữ ký, tính toàn vẹn và giải mã file*

*Tạo bộ công cụ crypto\_utils.py dùng lại được.*

*Giao tiếp mạng hoạt động đúng qua socket TCP, kết quả được xác minh bằng phản hồi ACK/NACK*

***ƯU ĐIỂM VÀ NHƯỢC ĐIỂM***

*✅ Ưu điểm*

*Sản phẩm chạy được đúng chức năng, kiểm tra được các bước bảo mật cơ bản.*

*Kiến trúc rõ ràng, dễ mở rộng: chia nhỏ thành nhiều file module (sender, receiver, crypto...).*

*Áp dụng kết hợp nhiều kỹ thuật bảo mật trong một mô hình thực tế đơn giản.*

*❌ Nhược điểm*

*Do thời gian có hạn nên giao diện chỉ ở mức dòng lệnh, chưa có GUI trực quan.*

*Vì kiến thức còn hạn chế nên chưa tối ưu tốc độ mã hóa/gửi dữ liệu cho các file lớn.*

*Vì điều kiện đầu tư còn hạn hẹp nên chưa triển khai thử nghiệm trên nhiều máy thật hoặc qua internet công cộng.*

***CÔNG VIỆC TƯƠNG LAI***

*Trong tương lai, nếu có thêm thời gian và điều kiện, em sẽ:*

*Nâng cấp giao diện thành ứng dụng web hoặc desktop (Flask, Tkinter).*

*Tích hợp thêm xác thực hai lớp (2FA), hoặc gửi OTP qua email để kiểm tra người gửi.*

*Kiểm tra địa chỉ IP nâng cao bằng GeoIP (kiểm tra khu vực địa lý).*

*Tạo hệ thống lưu log toàn bộ thao tác gửi/nhận để dễ kiểm tra, giám sát.*

*Mở rộng để ứng dụng gửi file bảo mật trong hệ thống nội bộ trường học, doanh nghiệp nhỏ...*

# **PHÂN CÔNG NHIỆM VỤ**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **MSV** | **Họ và tên** | **Nhiệm vụ** |
| 1 | 1771020190 | Đồng Lâm Dũng | Làm code và chỉnh sửa world |
| 2 |  |  |  |
| 3 |  |  |  |
|  |  |  |  |

**DANH MỤC TÀI LIỆU THAM KHẢO**

1. Nguyễn Hồng Sơn (2007), *Giáo trình hệ thống Mạng máy tính CCNA* (Semester 1), NXB Lao động xã hội.
2. Phạm Quốc Hùng (2017), *Đề cương bài giảng Mạng máy tính*, Đại học SPKT Hưng Yên.

**QUY ĐỊNH TRÌNH BÀY TRONG BÁO CÁO CÀI TẬP LỚN**

- Bài tập lớn được in trên một mặt giấy trắng khổ A4 (210 x 297mm), dày lớn hơn 30 trang, nhỏ hơn 100 trang, không kể hình vẽ, bảng biểu, đồ thị và danh mục tài liệu tham khảo.

- Phần nội dung trình bày trong bài tập lớn sử dụng Font chữ **Times New Roman** cỡ **13**, hệ soạn thảo Microsoft Word; mật độ chữ bình thường, không được nén hoặc kéo dãn khoảng cách giữa các chữ; dãn dòng đặt ở chế độ **1,5 lines**; lề trên **2,0 cm**; lề dưới **2,0 cm**; lề trái **2,5 cm**, lề phải **2,0 cm**. Số trang được đánh ở giữa, phía dưới trang giấy.

- Cách ghi trích dẫn tài liệu tham khảo: Cuối đoạn trích dẫn đánh số thứ tự tài liệu tham khảo (ví dụ: [1]: tham khảo tài liệu số 1; [3,4,8]: tham khảo 3 tài liệu số 3, 4, 8).

- Tuyệt đối không được tẩy, xoá, sửa chữa trong bài tập lớn.

- Quy cách trình bày nội dung

|  |  |  |  |
| --- | --- | --- | --- |
| **Đề mục** | **Cỡ chữ** | **Định dạng** | **Canh lề trang** |
| Tên chương | 14 | In hoa, đậm | Giữa |
| Tên tiểu mục mức 1 | 13 | Chữ thường, đậm | Trái |
| Tên tiểu mục mức 2 | 13 | Chữ thường, đậm, nghiêng | Trái |
| Tên tiểu mục mức 3 | 13 | Đánh chỉ mục bằng chữ cái thường  a), ...  b), ..... | Trái |
| Nội dung | 13 | Chữ thường (Normal) | Đều hai bên |
| Nội dung bảng (table) | 12 | Normal | Giữa ô |
| Tên bảng | 12 | Chữ thường, nghiêng | Giữa, trên bảng |
| Tên hình | 12 | Chữ thường, nghiêng | Giữa, dưới hình |
| Tài liệu tham khảo | 12 | APA style | Chú thích bên dưới |

***Cách đánh dấu câu****:*

Các dấu: : , . ; ) } ] ! ? ” được gõ ngay sau ký tự cuối cùng (không khoảng cách), và gõ 1 phím cách (space) sau chúng. Sau các dấu: “{ ( [ không gõ dấu cách.

***\* Cách đánh số các tiểu đề mục nhiều nhất là 3 mức và không lùi sang phải***

Hướng dẫn xếp tài liệu tham khảo

1. Tài liệu tham khảo xếp theo thứ tự trích dẫn trong bài tập lớn.
2. Tài liệu tham khảo là sách, luận án, báo cáo phải ghi đầy đủ các thông tin sau:

* Tên các tác giả hoặc cơ quan ban hành (không có dấu ngăn cách)
* (năm xuất bản), (đặt trong ngoặc đơn, dấu phẩy sau ngoặc đơn)
* Tên sách, luận án hoặc báo cáo, (in nghiêng, dấu phẩy cuối tên)
* Nhà xuất bản, (dấu phẩy cuối tên nhà xuất bản)
* Nơi xuất bản, (dấu chấm kết thúc tài liệu tham khảo).

Tài liệu tham khảo là bài báo trong tạp chí, bài trong một cuốn sách… ghi đầy đủ các thông tin sau:

* Tên các tác giả (không có dấu ngăn cách);
* (Năm công bố), (đặt trong ngoặc đơn, dấu phẩy sau ngoặc đơn)
* “Tên bài báo”, (đặt trong ngoặc kép, không in nghiên, dấu phẩy cuối tên)
* Tên tạp chí hoặc tên sách, (in nghiên, dấu phẩy cuối tên)
* Tập (không có dấu ngăn cách)
* (Sổ), (đặt trong ngoặc đơn, dấu phẩy sau ngoặc đơn)
* Các số trang, (gạch ngang giữa hai chữ số, dấu chấm kết thúc)

Cần chú ý những chi tiết về trình bày nêu trên. Nếu tài liệu dài hơn một dòng thì nên trình bày sau cho từ dòng thứ hai lùi vào so với dòng thứ nhất 1 cm để phần tài liệu tham khảo được rõ ràng và dễ theo dõi.

Ví dụ:

1. Nguyễn Hồng Sơn (2007), *Giáo trình hệ thống Mạng máy tính CCNA* (Semester 1), NXB Lao động xã hội.
2. Phạm Quốc Hùng (2017), *Đề cương bài giảng Mạng máy tính*, Đại học SPKT Hưng Yên.
3. James F. Kurose and Keith W. Ross (2013), *Computer Networking: A top-down approach sixth Edition*, Pearson Education.