BỘ GIÁO DỤC VÀ ĐÀO TẠO



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á

KHOA: CÔNG NGHỆ THÔNG TIN

**BÀI TẬP LỚN**

**HỌC PHẦN: AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI SỐ 23: NGHIÊN CỨU CHỮ KÝ SỐ TRONG VIỆC QUẢN LÝ TÀI LIỆU HỢP ĐỒNG NHÂN VIÊN**

|  |  |  |
| --- | --- | --- |
| **Sinh viên thực hiện** | **Lớp** | **Khóa** |
| **Phạm Đại Dương** | **DCCNTT 13.10.4** | **13** |
| **Lương Trọng Duy** | **DCCNTT 13.10.4** | **13** |
| **Bùi Khánh Hùng** | **DCCNTT 13.10.4** | **13** |
| **Hoàng Quang Hơp** | **DCCNTT 13.10.4** | **13** |
| **Hoàng Minh Đức** | **DCCNTT 13.10.4** | **13** |

**Bắc Ninh, năm 2024**

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ ĐÔNG Á

KHOA: CÔNG NGHỆ THÔNG TIN

**BÀI TẬP LỚN**

**HỌC PHẦN: AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI SỐ 23: NGHIÊN CỨU CHỮ KÝ SỐ TRONG VIỆC QUẢN LÝ TÀI LIỆU HỢP ĐỒNG NHÂN VIÊN**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **STT** | | **Sinh viên thực hiện** | **Mã sinh**  **viên** | | **Điểm bằng số** | **Điểm bằng chữ** | |
| **1** | | **Phạm Đại Dương** | **20220617** | |  |  | |
| **2** | | **Lương Trọng Duy** | **20220696** | |  |  | |
| **3** | | **Bùi Khánh Hùng** | **20220656** | |  |  | |
| **4** | | **Hoàng Quang Hợp** | **20220589** | |  |  | |
| **5** | | **Hoàng Minh Đức** | **20220577** | |  |  | |
| **CÁN BỘ CHẤM 1**  *(Ký và ghi rõ họ tên)* | | | **CÁN BỘ CHẤM 2**  *(Ký và ghi rõ họ tên)* | | |

# MỤC LỤC

[MỤC LỤC 1](#_Toc175693148)

[DANH MỤC CÁC TỪ VIẾT TẮT 2](#_Toc175693149)

[DANH MỤC HÌNH ẢNH VÀ BẢNG BIỂU 2](#_Toc175693150)

[LỜI CẢM ƠN 3](#_Toc175693151)

[LỜI CAM ĐOAN 4](#_Toc175693152)

[LỜI MỞ ĐẦU 5](#_Toc175693153)

[CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI 1](#_Toc175693154)

[1.1 Giới thiệu: 1](#_Toc175693155)

[1.2 Lý do chọn đề tài: 2](#_Toc175693156)

[1.3 Mục tiêu nghiên cứu: 4](#_Toc175693157)

[1.4 Phạm vi và ý nghĩa đề tài: 5](#_Toc175693158)

[CHƯƠNG 2. GIỚI THIỆU VỀ THUẬT TOÁN 7](#_Toc175693159)

[2.1 Khái niệm về an toàn thông tin: 7](#_Toc175693160)

[2.2 Sự cần thiết của an toàn thông tin: 7](#_Toc175693161)

[2.3 Mục đích của an toàn thông tin: 8](#_Toc175693162)

[2.4 Khái niệm về thuật toám RSA 9](#_Toc175693163)

[2.5 Khái niệm về chữ ký số: 11](#_Toc175693164)

[2.6 Ưu điểm và ứng dụng của chữ ký số trong quản lý tài liệu: 12](#_Toc175693165)

[2.7 Mối quan hệ giữa chữ ký số và an ninh mạng: 14](#_Toc175693166)

[CHƯƠNG 3 . THIẾT KẾ VÀ TRIỂN KHAI ỨNG DỤNG 16](#_Toc175693167)

[3.1 Mô tả tổng quan về ứng dụng "Quản lý Hợp đồng Ứng dụng chữ kí số" 16](#_Toc175693168)

[3.2 Phân tích các yêu cầu chức năng và phi chức năng 17](#_Toc175693169)

[3.3 Cài đặt 19](#_Toc175693170)

[3.3.1. Giới thiệu về ngôn ngữ c# 19](#_Toc175693171)

[3.3.2 Giải thích các hàm trong code: 22](#_Toc175693172)

[3.4 Mô tả giao diện người dùng và các tính năng chính của ứng dụng 26](#_Toc175693173)

[3.4.1 Giao diện Người dùng: 26](#_Toc175693174)

[3.4.2 Tính năng chính: 29](#_Toc175693175)

[3.5 Mối quan hệ giữa chữ ký số và an ninh mạng 31](#_Toc175693176)

[CHƯƠNG 4. KẾT LUẬN 34](#_Toc175693177)

[4.1 Kết quả đạt được 34](#_Toc175693178)

[4.2 Hướng phát triển 36](#_Toc175693179)

[TÀI LIỆU THAM KHẢO 37](#_Toc175693180)

# DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |
| --- | --- |
| **Chữ viết tắt** | **Giải thích** |
| RSA | Rivest-Shamir-Adleman |
| DSA | Digital Signature Algorithm |
| ECDSA | (Elliptic Curve Digital Signature Algorithm) |
| SHA | Secure Hash Algorithm |

Bảng 1. Danh mục các từ viết tắt

# DANH MỤC HÌNH ẢNH VÀ BẢNG BIỂU

|  |  |  |  |
| --- | --- | --- | --- |
| Số hiệu | Tên | Trang | Chương |
| Bảng 1 | Danh mục các từ viết tắt | ii |  |
| Bảng 2 | Bảng danh mục hình ảnh và bảng biểu | ii |  |
| Hình 2.1 | Hình ảnh ví dụ minh họa mô tả quá trình mã hóa và giải mã của hình thuật toán RSA | 8 | 2 |
| Hình 3.1 | Giao diện chương trình | 23 | 3 |

Bảng 2. Danh mục hình ảnh và bảng biểu

# LỜI CẢM ƠN

Chúng em muốn bày tỏ lòng biết ơn chân thành tới Khoa Công Nghệ Thông Tin, Trường Đại học Công Nghệ Đông Á, nơi đã mang đến cho chúng em không chỉ là một môi trường học tập, mà còn là một mái nhà thứ hai, nơi mà chúng em đã được trang bị kiến thức, kỹ năng và tinh thần đam mê.

Đặc biệt, chúng em muốn gửi lời biết ơn sâu sắc đến Giảng viên môn học Nguyễn Viết Hùng, người đã dành sự tận tâm và sự tận tụy để chia sẻ kiến thức, kinh nghiệm và sự truyền cảm hứng với chúng em. Thầy không chỉ là một người thầy mà còn là một người bạn đồng hành, luôn sẵn sàng hỗ trợ và động viên chúng em vượt qua mọi khó khăn và thách thức.

Những bài học và kiến thức mà chúng em đã học được từ thầy không chỉ giúp chúng em phát triển bản thân mà còn là nguồn động viên mạnh mẽ để chúng em tiếp tục bước đi trên con đường sự nghiệp của mình.

Xin chân thành cảm ơn!

# LỜI CAM ĐOAN

Chúng em cam đoan rằng mọi thông tin và kết quả trong bài tập lớn này là hoàn toàn trung thực và được nghiên cứu một cách cẩn thận. Tất cả các ý kiến, phân tích và kết luận đều dựa trên nghiên cứu đúng đắn và không sao chép từ bất kỳ nguồn nào khác.

Chúng em đã và đang thực hiện đề tài này với tinh thần trách nhiệm cao nhất và sự tôn trọng đối với kiến thức và công sức của các nhà nghiên cứu trước đó. Bất kỳ thông tin hay ý kiến nào được trích dẫn từ các nguồn khác đều được chỉ ra một cách rõ ràng và đúng đắn.

Chúng em cam kết sẽ tiếp tục nghiên cứu và phát triển đề tài này, cũng như tuân thủ các nguyên tắc và quy định đạo đức trong việc thực hiện nghiên cứu khoa học. Bài tập lớn này được thực hiện với mong muốn đóng góp vào sự phát triển của lĩnh vực công nghệ thông tin và xã hội.

Chúng em xin chân thành cảm ơn sự quan tâm và hỗ trợ từ phía quý thầy cô, bạn bè và gia đình trong suốt thời gian thực hiện đề tài này. Mong rằng, thông qua bài tập lớn này, chúng em có thể góp phần vào việc nâng cao hiểu biết và ứng dụng thực tiễn của thuật toán RSA và chữ ký điện tử.

# LỜI MỞ ĐẦU

Trong thời đại số hóa ngày nay, việc quản lý tài liệu hợp đồng không chỉ là một phần quan trọng của hoạt động kinh doanh mà còn là một thách thức đối với nhiều tổ chức, đặc biệt là trong lĩnh vực an ninh mạng. Việc đảm bảo tính toàn vẹn, bảo mật và tin cậy của các hợp đồng nhân viên đòi hỏi sự chính xác, hiệu quả và an toàn trong quá trình quản lý và xử lý.

Nắm vững kiến thức cơ bản: Tìm hiểu về các thuật toán chính trong mã hóa chữ ký số như RSA, Băm SHA-256và các thuật toán khác. Áp dụng vào thực tế: Hiểu cách triển khai các thuật toán mã hóa chữ ký số trong các ứng dụng và hệ thống thực tế, bao gồm cả quy trình triển khai và các vấn đề cần xem xét. Phân tích và đánh giá: Phân tích các ưu và nhược điểm của từng thuật toán, đánh giá hiệu suất và độ an toàn của chúng trong các tình huống cụ thể. Nâng cao kiến thức: Khám phá các phương pháp và công nghệ mới trong lĩnh vực mã hóa chữ ký số và đề xuất hướng phát triển trong tương lai Qua dự án này, chúng ta hy vọng có được cái nhìn toàn diện về mã hóa chữ ký số và khả năng áp dụng kiến thức này vào việc bảo vệ thông tin và giao tiếp an toàn trong môi trường kỹ thuật số ngày nay

Trong bối cảnh đó, việc áp dụng công nghệ chữ ký số trong quản lý tài liệu hợp đồng trở thành một xu hướng không thể phủ nhận. Công nghệ này không chỉ giúp tăng cường tính bảo mật và tin cậy của các hợp đồng mà còn tạo ra những tiện ích và lợi ích rất lớn cho các tổ chức và cá nhân trong quá trình quản lý hợp đồng.

Trong báo cáo này, chúng tôi sẽ trình bày về đề tài "Quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng sử dụng chữ ký số", bao gồm lý do chọn đề tài, mục tiêu nghiên cứu, phạm vi và ý nghĩa của đề tài. Chúng tôi cũng sẽ phân tích các khái niệm cơ bản về chữ ký số, ưu điểm và ứng dụng của chúng trong quản lý tài liệu hợp đồng, cùng với mối quan hệ giữa chữ ký số và an ninh mạng.

Thông qua việc nghiên cứu và thảo luận, hy vọng rằng báo cáo này sẽ cung cấp cái nhìn tổng quan và hiểu biết sâu sắc hơn về vai trò và ứng dụng của chữ ký số trong quản lý tài liệu hợp đồng trong lĩnh vực an ninh mạng.

# CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI

## 1.1 Giới thiệu:

Trong một thế giới ngày càng phụ thuộc vào công nghệ thông tin, việc bảo vệ dữ liệu và xác thực danh tính trở nên cực kỳ quan trọng. Mã hóa chữ ký số là một phương tiện hiệu quả để đảm bảo tính toàn vẹn và xác thực của thông tin điện tử trong các hệ thống thông tin. Trong phần này, chúng ta sẽ khám phá các thuật toán phổ biến được sử dụng trong môn học An toàn Bảo mật Thông tin, tập trung vào việc mã hóa chữ ký số.

Đề tài " Nghiên cứu chữ ký số trong việc quản lý tài liệu hợp đồng nhân viên " là một lĩnh vực nghiên cứu quan trọng trong lĩnh vực an ninh mạng và bảo mật thông tin. Mã hóa chữ ký số là quá trình sử dụng một thuật toán mã hóa đặc biệt để tạo ra một dạng mã số duy nhất, được gọi là chữ ký số, từ một tập hợp các dữ liệu đầu vào. Chữ ký số này sau đó được sử dụng để xác minh tính toàn vẹn, nguyên tắc và nguồn gốc của dữ liệu Các thuật toán về mã hóa chữ ký số bao gồm nhiều phương pháp khác nhau như RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), ECDSA (Elliptic Curve Digital Signature Algorithm), và nhiều thuật toán khác. Mỗi thuật toán có những đặc điểm riêng và cách thức hoạt động khác nhau, nhưng chung mục tiêu của chúng là đảm bảo tính toàn vẹn và xác thực của thông tin Nghiên cứu về các thuật toán mã hóa chữ ký số không chỉ giúp hiểu rõ về cách thức hoạt động của từng thuật toán mà còn giúp phát triển các ứng dụng và hệ thống bảo mật thông tin hiệu quả. Đồng thời, nó cũng đóng vai trò quan trọng trong việc bảo vệ thông tin cá nhân, giao dịch điện tử và các hoạt động trực tuyến khác trước các mối đe dọa từ hacker và các hoạt động giả mạo.

## 1.2 Lý do chọn đề tài:

Nhu cầu về chữ ký điện tử ngày càng gia tăng trong kỷ nguyên số, khi giao dịch điện tử trở nên phổ biến. Việc đảm bảo an toàn, xác thực cho các giao dịch đóng vai trò then chốt trong thúc đẩy thương mại điện tử và kinh tế số. Tuy nhiên, phiếu thu truyền thống dưới dạng giấy tờ tiềm ẩn nguy cơ giả mạo, thất lạc, ảnh hưởng đến hoạt động tài chính doanh nghiệp.

An ninh thông tin là yếu tố cốt lõi đối với hoạt động của cả cá nhân lẫn tổ chức. Một việc làm sai lầm trong việc bảo vệ thông tin có thể dẫn đến hậu quả nghiêm trọng như mất thông tin quan trọng, tổn thất tài chính và danh tiếng, hoặc thậm chí là thất thoát dữ liệu cá nhân của khách hàng Mã hóa chữ ký số đóng vai trò quan trọng trong việc bảo vệ thông tin. Chúng giúp xác minh nguồn gốc và tính toàn vẹn của dữ liệu, đảm bảo rằng thông tin không bị sửa đổi hay giả mạo trong quá trình truyền tải Sự phổ biến của chữ ký số.

Nghiên cứu ứng dụng chữ ký điện tử RSA cho Nghiên cứu thuật toán RSA vào ứng dụng chữ ký số trong việc quản lý hợp đồng nhân viên là giải pháp thiết yếu cho vấn đề này. Thuật toán RSA đã được chứng minh tính an toàn, hiệu quả cao, dễ dàng triển khai với công nghệ hiện đại. Việc áp dụng chữ ký điện tử RSA mang lại nhiều lợi ích:

Nâng cao tính bảo mật: Bảo vệ thông tin thanh toán khỏi giả mạo, thay đổi hoặc truy cập trái phép.

Tăng cường tính xác thực: Xác thực nguồn gốc, danh tính người tạo phiếu thu, truy xuất nguồn gốc giao dịch dễ dàng.

Tiết kiệm thời gian, chi phí: Giảm thiểu thủ tục giấy tờ, tự động hóa quy trình xử lý phiếu thu.

Nâng cao uy tín thương hiệu: Thể hiện sự chuyên nghiệp trong quản lý tài chính, thu hút khách hàng và đối tác.

Trong thế giới kỹ thuật số hiện nay, giao dịch trực tuyến và việc truyền tải thông tin qua mạng đã trở nên phổ biến hơn bao giờ hết Chữ ký số là một cách hiệu quả để xác thực danh tính và tính toàn vẹn của thông tin trong các giao dịch trực tuyến, từ việc ký kết hợp đồng đến xác thực tài khoản trực tuyến khả năng áp dụng rộng rãi.

Việc lựa chọn đề tài về chữ ký số trong quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng được thực hiện với nhiều lý do đáng chú ý. Dưới đây là một số điểm cần lưu ý:

**Tính cấp thiết của bảo mật thông tin:**

Trong môi trường công nghệ thông tin ngày càng phát triển, bảo mật thông tin trở thành một yếu tố không thể thiếu. Trong ngành an ninh mạng đặc biệt, việc bảo vệ thông tin và đảm bảo tính toàn vẹn của dữ liệu là vô cùng quan trọng để ngăn chặn các cuộc tấn công mạng và đảm bảo sự tin cậy của hệ thống.

Tăng cường tính chính xác và xác thực của hợp đồng: Chữ ký số là một công cụ quan trọng trong việc xác định và xác thực danh tính của các bên tham gia vào một hợp đồng. Việc sử dụng chữ ký số giúp tăng cường tính chính xác của thông tin và ngăn chặn việc làm giả mạo hợp đồng.

**Hiệu quả trong quản lý tài liệu:**

Việc áp dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên giúp tạo ra một quy trình quản lý hiệu quả, giảm thiểu sự phụ thuộc vào tài liệu giấy tờ và tối ưu hóa quá trình xử lý dữ liệu.

Sự phát triển của công nghệ: Công nghệ chữ ký số ngày càng được ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau. Việc nghiên cứu về cách sử dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng không chỉ mang lại lợi ích ngay trong thời điểm hiện tại mà còn giúp chuẩn bị cho sự phát triển và tích hợp công nghệ mới trong tương lai.

**Yêu cầu pháp lý và tuân thủ:**

Trong nhiều quốc gia, việc sử dụng chữ ký số đã được pháp luật công nhận và điều chỉnh một cách cụ thể. Việc nghiên cứu và áp dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên cũng giúp đảm bảo tuân thủ các quy định pháp lý liên quan đồng thời tăng cường sự tin cậy và uy tín của tổ chức.

Trên cơ sở những lý do trên, việc nghiên cứu và áp dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng trở thành một phần quan trọng và không thể thiếu trong quá trình xây dựng và phát triển hệ thống quản lý thông tin hiện đại.

## 1.3 Mục tiêu nghiên cứu:

Tìm hiểu lý thuyết: Bắt đầu bằng việc nghiên cứu về thuật toán RSA và khái niệm chữ ký điện tử. Tìm hiểu cách hoạt động của thuật toán RSA, các phép toán và quy trình tạo ra cặp khóa, mã hóa và giải mã. Đồng thời, hiểu về cách tạo chữ ký điện tử, xác minh chữ ký và các ứng dụng của chữ ký điện tử trong thực tế.

Mục tiêu của nghiên cứu về chữ ký số trong quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng có thể được phác thảo như sau:

**Phân tích và đánh giá tính ứng dụng của chữ ký số:** Mục tiêu đầu tiên của nghiên cứu là phân tích và đánh giá hiệu quả của việc sử dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên. Qua đó, xác định được những ưu điểm và hạn chế của việc áp dụng chữ ký số trong ngữ cảnh cụ thể này.

**Xây dựng hệ thống quản lý tài liệu hợp đồng dựa trên chữ ký số:** Mục tiêu tiếp theo là xây dựng một hệ thống quản lý tài liệu hợp đồng nhân viên tích hợp công nghệ chữ ký số. Qua đó, cung cấp một giải pháp thiết thực cho việc quản lý tài liệu một cách an toàn, hiệu quả và linh hoạt.

**Nghiên cứu và áp dụng các biện pháp bảo mật:** Mục tiêu này tập trung vào nghiên cứu và áp dụng các biện pháp bảo mật hiệu quả nhằm bảo vệ tính toàn vẹn và bảo mật của tài liệu hợp đồng đã được ký kết bằng chữ ký số. Điều này bao gồm cả việc nghiên cứu các phương pháp mã hóa và xác thực thông tin.

**Đánh giá và so sánh với các phương pháp truyền thống:** Mục tiêu cuối cùng là đánh giá và so sánh hiệu quả của hệ thống quản lý tài liệu hợp đồng dựa trên chữ ký số với các phương pháp quản lý truyền thống khác. Điều này giúp cung cấp cái nhìn tổng quan về ưu điểm và hạn chế của phương pháp mới so với các phương pháp truyền thống.

Tổng cộng, mục tiêu của nghiên cứu là xây dựng và đánh giá một hệ thống quản lý tài liệu hợp đồng nhân viên dựa trên chữ ký số trong ngành an ninh mạng, đồng thời đề xuất các biện pháp cải tiến và phát triển cho quy trình quản lý tài liệu hiện tại.

## 1.4 Phạm vi và ý nghĩa đề tài:

**Phạm vi của đề tài:**

Quản lý tài liệu hợp đồng: Đề tài tập trung vào việc nghiên cứu và áp dụng chữ ký số trong quản lý tài liệu hợp đồng của nhân viên trong ngành an ninh mạng. Phạm vi này bao gồm cả việc xây dựng hệ thống quản lý, xử lý và lưu trữ các tài liệu hợp đồng một cách an toàn và hiệu quả.

Bảo mật thông tin: Đề tài cũng chú trọng vào các biện pháp bảo mật thông tin, bao gồm việc xác định, mã hóa và bảo vệ tính toàn vẹn của dữ liệu tài liệu hợp đồng. Phạm vi này cũng bao gồm việc xác thực danh tính của các bên tham gia vào quá trình ký kết hợp đồng.

**Ý nghĩa của đề tài:**

Tăng cường tính toàn vẹn và tin cậy của tài liệu: Việc áp dụng chữ ký số giúp tăng cường tính toàn vẹn và tin cậy của tài liệu hợp đồng, từ đó giúp ngăn chặn các vấn đề liên quan đến làm giả mạo và thay đổi tài liệu.

Nâng cao hiệu quả quản lý tài liệu: Bằng cách tự động hóa quá trình ký kết và xác thực hợp đồng, đề tài giúp tăng cường hiệu quả trong quản lý tài liệu, giảm thiểu thời gian và chi phí cũng như nguy cơ phát sinh từ việc sử dụng tài liệu giấy tờ truyền thống.

Đáp ứng yêu cầu pháp lý và tiêu chuẩn: Sử dụng chữ ký số không chỉ giúp đáp ứng yêu cầu pháp lý và tiêu chuẩn về bảo mật thông tin mà còn giúp tăng cường sự tin cậy và uy tín của tổ chức trong việc quản lý hợp đồng nhân viên.

Đóng góp vào sự phát triển công nghệ: Nghiên cứu và áp dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên cũng đóng góp vào sự phát triển và tiếp cận mới mẻ của công nghệ trong lĩnh vực quản lý thông tin và an ninh mạng.

Tổng cộng, việc nghiên cứu và áp dụng chữ ký số trong quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng không chỉ mang lại lợi ích ngay trong thời điểm hiện tại mà còn đóng góp vào sự phát triển bền vững của tổ chức và ngành công nghiệp.

# CHƯƠNG 2. GIỚI THIỆUVỀ THUẬT TOÁN

## 2.1 Khái niệm về an toàn thông tin:

An toàn thông tin là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,…

An toàn thông tin liên quan đến hai khía cạnh đó là an toàn về mặt vật lý và an toàn về mặt kỹ thuật.

Mục tiêu cơ bản của an toàn thông tin:

Đảm bảo tính bảo mật.

Đảm bảo tính toàn vẹn.

Đảm bảo tính xác thực.

Đảm bảo tính sẵn sàng.

## 2.2 Sự cần thiết của an toàn thông tin:

Hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, là tài sản quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do. Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

## 2.3 Mục đích của an toàn thông tin:

Bảo vệ tài nguyên của hệ thống

Các hệ thống máy tính lưu giữ rất nhiều thông tin và tài nguyên cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Đối với rất nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý và sử dụng bởi các chương trình phần mềm.

Các tấn công vào hệ thống có thể xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng.

Bảo đảm tính riêng tư

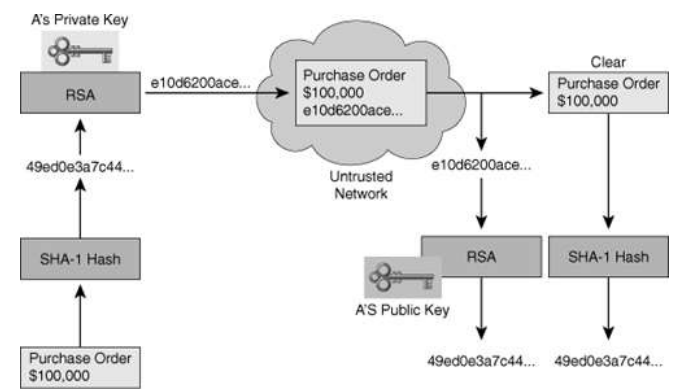
Các hệ thống máy tính lưu giữ rất nhiều thông tin cá nhân cần được giữ bí mật. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,...

Tính riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin về khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin cá nhân được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những thông tin cá nhân.

## 2.4 Khái niệm về thuật toám RSA

RSA là một thuật toán hay còn gọi là hệ mã hóa đối xứng được sử dụng cho các mục đích bảo mật. Nó cho phép mã hóa khóa công khai và được sử dụng phổ biến, rộng rãi để đảm bảo an toàn cho các dữ liệu nhạy cảm đặc biệt là những dữ liệu gửi qua mạng Internet.

Năm 1997 RSA lần đầu tiên được ra mắt bởi Ron Rivest, Adi Shamir và Leonard Adleman. Cái tên RSA là bắt nguồn từ ba chữ cái đầu trong tên của ba nhà khoa học. Mật mã khóa công khai sử dụng hai key khác nhau là public key (khóa công khai) và private key (khóa riêng tư). Public key có thể được chia sẻ với mọi người, riêng private key thì cần phải giữ bí mật.



Hình 2.1 Hình ảnh ví dụ minh họa mô tả quá trình mã hóa và giải mã của hình thuật toán RSA

Hình ảnh 1 mô tả quy trình mã hóa và giải mã thông tin trong một giao dịch mua hàng trực tuyến sử dụng công nghệ **RSA** và **SHA-1 Hash**. Dưới đây là các bước chi tiết:

**Mã hóa RSA**: Đơn đặt hàng với giá trị “100,000 đô la” được mã hóa bằng **khóa riêng tư của A**, tạo ra một chuỗi mã hóa.

**Mạng không an toàn**: Chuỗi mã hóa này sau đó được gửi qua một mạng không an toàn.

**Giải mã RSA**: Khi nhận được, chuỗi mã hóa được giải mã bằng **khóa công khai của A** để lấy lại thông tin đơn đặt hàng rõ ràng.

**Xác minh SHA-1 Hash**: Quá trình giải mã bao gồm cả việc giải mã RSA và xác minh bằng SHA-1 Hash.

Quy trình này đảm bảo rằng thông tin đơn đặt hàng được bảo mật trong khi truyền qua mạng không an toàn. Đây là một phần của các biện pháp bảo mật thông tin trong giao dịch điện tử.

## 2.5 Khái niệm về chữ ký số:

Chữ ký số là một phần của hệ thống mã hóa công khai (public key infrastructure - PKI) được sử dụng để xác thực tính toàn vẹn và nguồn gốc của dữ liệu điện tử. Trong bối cảnh ngày nay, khi việc trao đổi thông tin trên mạng Internet trở nên phổ biến, việc sử dụng chữ ký số là một phương tiện quan trọng để đảm bảo tính bảo mật và tin cậy của thông tin.

**Nguyên lý hoạt động:**

Chữ ký số được tạo ra bằng cách sử dụng một cặp khóa: khóa riêng (private key) và khóa công khai (public key). Khóa riêng được giữ bí mật và chỉ được sử dụng để tạo chữ ký, trong khi khóa công khai được công khai và được sử dụng để xác thực chữ ký.

Quá trình tạo chữ ký số thường bắt đầu bằng việc tạo một bản tóm tắt (hash) của dữ liệu cần ký. Sau đó, khóa riêng được sử dụng để ký bản tóm tắt này, tạo ra chữ ký số. Chữ ký số này có thể được xác thực bằng cách sử dụng khóa công khai tương ứng.

**Tính toàn vẹn và xác thực:**

Chữ ký số giúp xác định rằng dữ liệu không bị thay đổi từ khi được ký kết. Bằng cách so sánh giá trị băm (hash) của dữ liệu với giá trị băm của dữ liệu ban đầu được ký kết, người nhận có thể xác nhận tính toàn vẹn của dữ liệu.

Đồng thời, chữ ký số cũng xác định nguồn gốc của dữ liệu bằng cách xác minh rằng chữ ký được tạo ra bằng khóa riêng của người ký, và có thể được xác thực bằng khóa công khai tương ứng.

**Áp dụng và ứng dụng:**

Chữ ký số được sử dụng trong nhiều lĩnh vực, từ giao dịch tài chính trực tuyến đến chính phủ điện tử và hợp đồng kỹ thuật số.

Trong lĩnh vực quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng, chữ ký số giúp đảm bảo tính toàn vẹn và uy tín của các hợp đồng, từ việc ký kết cho đến xác thực và bảo vệ chúng khỏi sự thay đổi trái phép.

**Thách thức và cải tiến:**

Mặc dù chữ ký số mang lại nhiều lợi ích, nhưng vẫn còn một số thách thức như quản lý và bảo mật khóa riêng, đảm bảo tính toàn vẹn của khóa công khai và nguy cơ của việc mất mát hoặc lạm dụng chữ ký.

Cải tiến trong công nghệ mã hóa và quản lý khóa, cùng với việc thúc đẩy sự nhận thức và đào tạo về an ninh thông tin, có thể giúp giải quyết những thách thức này và nâng cao hiệu quả của việc sử dụng chữ ký số.

## 2.6 Ưu điểm và ứng dụng của chữ ký số trong quản lý tài liệu:

**Ưu điểm của chữ ký số trong quản lý tài liệu:**

Bảo mật cao: Chữ ký số giúp xác thực danh tính của người ký và đảm bảo tính toàn vẹn của dữ liệu. Điều này ngăn chặn các cuộc tấn công giả mạo và thay đổi dữ liệu.

Pháp lý công nhận: Trong nhiều quốc gia, chữ ký số đã được công nhận pháp lý và có giá trị tương đương với chữ ký truyền thống trên giấy tờ.

Tiết kiệm thời gian và chi phí: Quá trình ký kết và xác thực tài liệu thông qua chữ ký số diễn ra nhanh chóng và tự động hóa, giảm thiểu thời gian và chi phí so với việc sử dụng giấy tờ truyền thống.

Tích hợp dễ dàng: Chữ ký số có thể dễ dàng tích hợp vào các hệ thống quản lý tài liệu hiện có, từ các ứng dụng email đến hệ thống quản lý hợp đồng.

Tính linh hoạt: Chữ ký số có thể áp dụng cho mọi loại tài liệu điện tử, từ hợp đồng đến bản ghi nhật ký và tài liệu báo cáo.

**Ứng dụng của chữ ký số trong quản lý tài liệu:**

Hợp đồng điện tử: Chữ ký số cho phép việc ký kết các hợp đồng điện tử một cách an toàn và hiệu quả, từ việc thuê nhà đến các giao dịch thương mại quốc tế.

Quản lý tài liệu doanh nghiệp: Các doanh nghiệp có thể sử dụng chữ ký số để ký kết và xác thực các tài liệu như hợp đồng lao động, tài liệu báo cáo và tài liệu quản lý nhân sự.

Giao dịch tài chính trực tuyến: Chữ ký số cho phép việc thực hiện các giao dịch tài chính trực tuyến một cách an toàn và tin cậy, bao gồm việc chuyển khoản tiền, mua bán chứng khoán và thực hiện giao dịch ngân hàng.

Bảo mật thông tin cá nhân: Chữ ký số cũng có thể được sử dụng để bảo vệ thông tin cá nhân trong các tài liệu như hồ sơ y tế điện tử và tài liệu tài sản cá nhân.

Quản lý văn bản công quốc gia: Chữ ký số được sử dụng trong các hệ thống quản lý văn bản công quốc gia để đảm bảo tính bảo mật và tin cậy của thông tin trong các tài liệu quan trọng của chính phủ.

## 2.7 Mối quan hệ giữa chữ ký số và an ninh mạng:

Mối quan hệ giữa chữ ký số và an ninh mạng là một phần quan trọng của việc đảm bảo tính toàn vẹn, bảo mật và tin cậy của thông tin trên mạng. Dưới đây là một số điểm cần lưu ý về mối quan hệ này:

**Bảo mật thông tin:**

Chữ ký số đóng vai trò quan trọng trong việc bảo mật thông tin trên mạng bằng cách xác thực danh tính của người gửi và đảm bảo tính toàn vẹn của dữ liệu trước khi nó được chấp nhận hoặc truyền đi.

Ngăn chặn tấn công giả mạo: Chữ ký số giúp ngăn chặn các cuộc tấn công giả mạo thông tin bằng cách đảm bảo rằng dữ liệu không bị thay đổi và chỉ được tạo ra bởi người đã được xác thực.

**Xác thực truy cập:**

Chữ ký số cung cấp một phương tiện để xác thực danh tính của người dùng và đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào các tài nguyên hoặc dịch vụ trên mạng.

Bảo vệ quyền riêng tư: Chữ ký số giúp bảo vệ quyền riêng tư của người dùng bằng cách đảm bảo rằng thông tin cá nhân chỉ được chia sẻ với những người đã được ủy quyền và không bị sửa đổi trong quá trình truyền tải.

Hợp pháp hóa giao dịch trực tuyến: Sử dụng chữ ký số giúp hợp pháp hóa các giao dịch trực tuyến bằng cách cung cấp một phương tiện để xác thực và chứng nhận tính xác thực của các bên tham gia vào giao dịch.

Quản lý chứng chỉ số: An ninh mạng liên quan đến việc quản lý các chứng chỉ số để đảm bảo tính bảo mật và tin cậy của hệ thống PKI và chữ ký số.

Đối phó với các cuộc tấn công mạng: Chữ ký số có thể được sử dụng trong các biện pháp phòng ngừa và đối phó với các cuộc tấn công mạng như lừa đảo, phá hoại hoặc xâm nhập.

Tóm lại, chữ ký số đóng vai trò quan trọng trong việc bảo vệ và bảo mật thông tin trên mạng, đồng thời đóng góp vào việc thúc đẩy sự tin cậy và tính hợp pháp của các hoạt động trực tuyến.

# CHƯƠNG 3 . THIẾT KẾ VÀ TRIỂN KHAI ỨNG DỤNG

## 3.1 Mô tả tổng quan về ứng dụng "Quản lý Hợp đồng Ứng dụng chữ kí số"

Ứng dụng "Quản lý Hợp đồng Ứng dụng chữ ký số" được thiết kế nhằm mục đích hỗ trợ quá trình quản lý và xử lý các tài liệu hợp đồng nhân viên trong ngành an ninh mạng một cách an toàn, hiệu quả và tiện lợi. Dưới đây là mô tả tổng quan về ứng dụng này:

**Mục tiêu chính:**

Xây dựng một hệ thống quản lý tài liệu hợp đồng nhân viên tích hợp công nghệ chữ ký số.

Hỗ trợ quá trình ký kết, xác thực và bảo vệ tính toàn vẹn của các tài liệu hợp đồng.

Tăng cường tính bảo mật và tin cậy của thông tin trong quá trình quản lý hợp đồng.

**Tính năng chính:**

Thêm và hiển thị hợp đồng: Cho phép người dùng thêm mới và hiển thị thông tin chi tiết của các hợp đồng nhân viên.

Chữ ký số: Hỗ trợ quá trình ký kết hợp đồng bằng chữ ký số và hiển thị chữ ký số đã tạo.

Xác thực và bảo vệ tính toàn vẹn: Cung cấp chức năng để xác thực tính toàn vẹn của các tài liệu hợp đồng và bảo vệ chúng khỏi sự thay đổi trái phép.

Hiển thị khóa công khai và khóa riêng: Cho phép người dùng xem và quản lý các khóa công khai và khóa riêng được sử dụng trong quá trình ký kết và xác thực.

**Giao diện người dùng:**

Giao diện trực quan và dễ sử dụng, tối ưu hóa cho việc quản lý tài liệu hợp đồng một cách thuận tiện.

Các chức năng và thao tác được tổ chức một cách logic và có thể truy cập dễ dàng từ menu và các nút chức năng.

**Triển khai và tích hợp:**

Ứng dụng có thể triển khai trên nền tảng máy tính cá nhân hoặc máy chủ để đáp ứng nhu cầu của cá nhân hoặc tổ chức.

**Tính mở rộng và cải tiến:**

Dễ dàng mở rộng và cải tiến để đáp ứng các yêu cầu mới và nâng cao khả năng hoạt động của ứng dụng theo thời gian.

Có khả năng tích hợp các tính năng bảo mật và quản lý khóa mới để tăng cường tính an toàn và tin cậy của hệ thống.

Tóm lại, ứng dụng "Quản lý Hợp đồng Ứng dụng chữ ký số" được thiết kế nhằm cung cấp một giải pháp toàn diện và hiệu quả cho quản lý tài liệu hợp đồng nhân viên trong ngành an ninh mạng, đồng thời đảm bảo tính bảo mật và tin cậy của thông tin.

## 3.2 Phân tích các yêu cầu chức năng và phi chức năng

**Yêu cầu chức năng:**

**Thêm Hợp đồng*:*** Người dùng có thể thêm mới thông tin về hợp đồng nhân viên vào hệ thống bằng cách nhập các thông tin như tên hợp đồng, ngày bắt đầu, ngày kết thúc, v.v.

**Hiển thị Hợp đồng:** Hệ thống cung cấp chức năng để hiển thị danh sách các hợp đồng nhân viên đã được thêm vào, bao gồm các thông tin chi tiết như mã hợp đồng, tên hợp đồng, ngày bắt đầu, ngày kết thúc, đường dẫn tới tài liệu hợp đồng, và giá trị băm của tài liệu.

**Ký kết Hợp đồng*:*** Người dùng có thể ký kết các hợp đồng nhân viên bằng cách sử dụng chữ ký số. Hệ thống sẽ tạo ra chữ ký số dựa trên tài liệu hợp đồng đã chọn và khóa riêng của người dùng.

**Xác thực Chữ ký:** Hệ thống cho phép xác thực chữ ký số của các tài liệu hợp đồng để đảm bảo tính toàn vẹn và tin cậy của chúng. Khi người dùng chọn một tài liệu hợp đồng, hệ thống sẽ kiểm tra chữ ký số của tài liệu và hiển thị kết quả xác thực.

**Yêu cầu phi chức năng:**

**Giao diện Người dùng Thân thiện:** Giao diện người dùng phải được thiết kế đơn giản, dễ sử dụng và thân thiện với người dùng để giúp họ tương tác với hệ thống một cách hiệu quả.

**Bảo mật:** Hệ thống phải đảm bảo tính bảo mật của thông tin, bao gồm cả thông tin về hợp đồng và khóa riêng của người dùng. Ngoài ra, quá trình xác thực chữ ký số cũng phải được thực hiện một cách an toàn và đáng tin cậy.

**Tích hợp Dễ dàng:** Hệ thống cần có khả năng tích hợp dễ dàng với các hệ thống quản lý tài liệu hiện có và các công nghệ khác để tối ưu hóa quá trình làm việc của người dùng.

**Hiệu suất và Đáng tin cậy:** Hệ thống cần phải hoạt động một cách hiệu suất và đáng tin cậy, đặc biệt là trong việc tạo và xác thực chữ ký số, để đảm bảo rằng người dùng có thể sử dụng nó một cách liên tục mà không gặp phải sự cố.

## 3.3 Cài đặt

### 3.3.1. Giới thiệu về ngôn ngữ c#

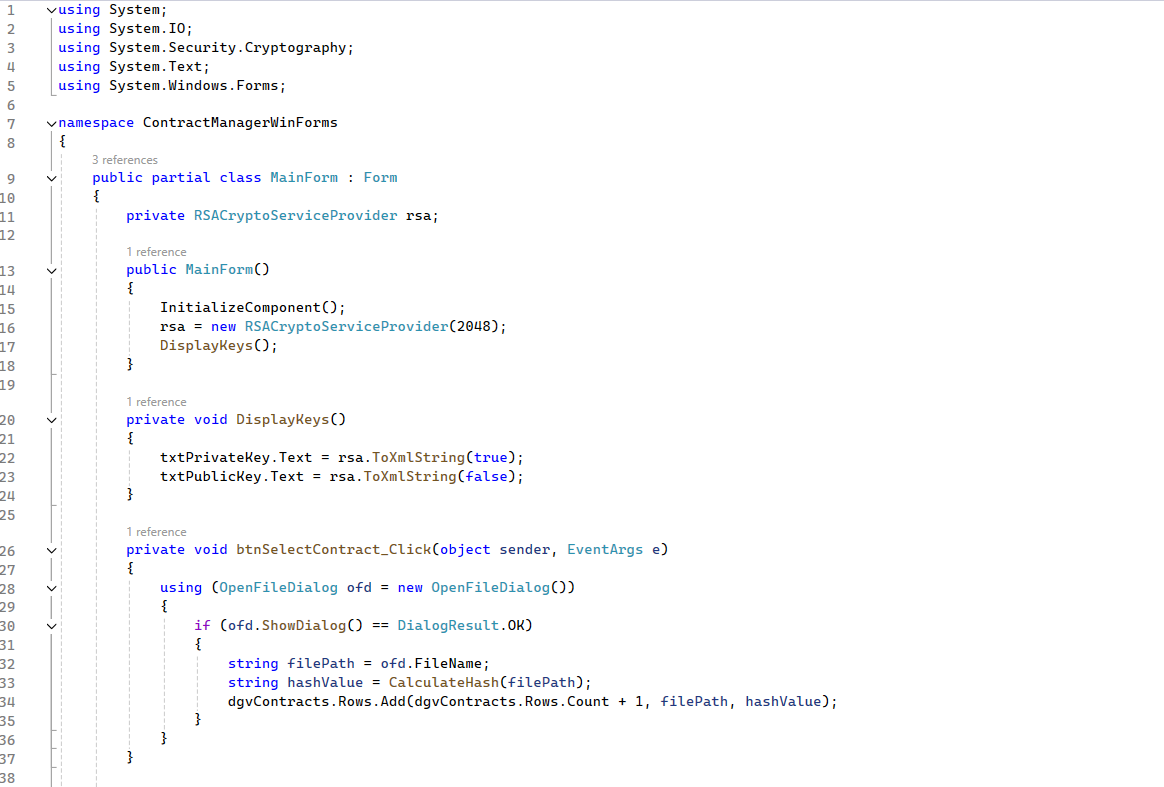
C# (C-Sharp) là một ngôn ngữ lập trình hướng đối tượng được phát triển bởi Microsoft trong khuôn khổ của .NET framework. Được công bố lần đầu tiên vào năm 2000, C# được thiết kế bởi Anders Hejlsberg, người cũng là một trong những người đã phát triển ngôn ngữ Delphi và Turbo Pascal.

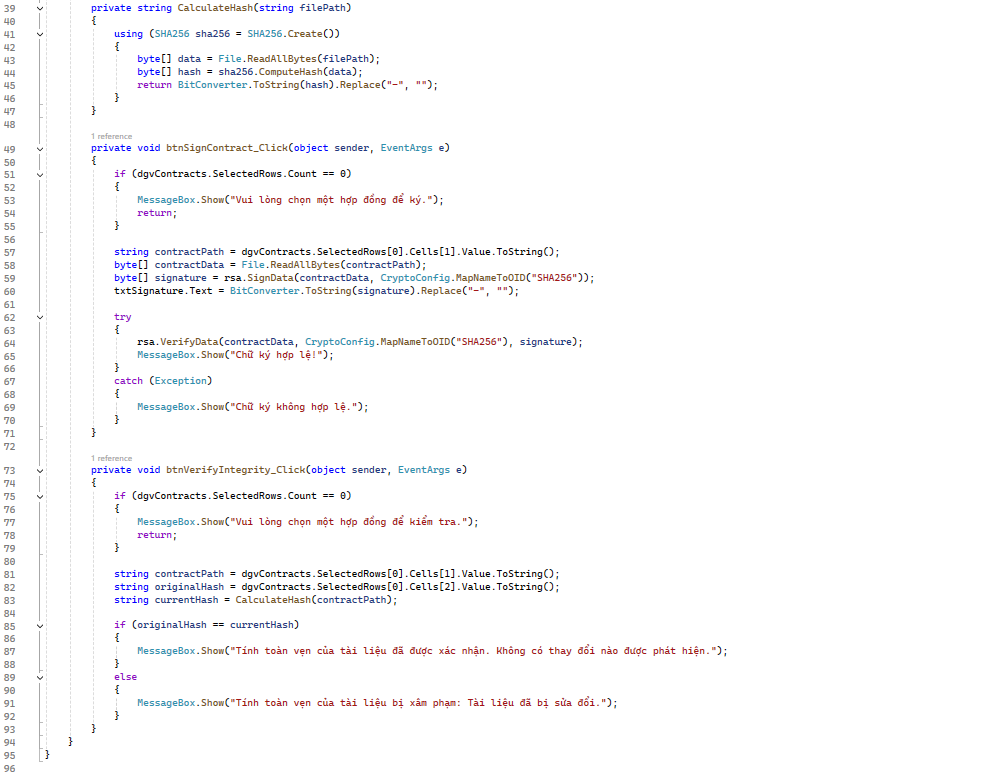
Các đặc điểm chính của C#:

1. **Ngôn ngữ hướng đối tượng (OOP)**: C# hỗ trợ các khái niệm cơ bản của lập trình hướng đối tượng như lớp (class), đối tượng (object), kế thừa (inheritance), đóng gói (encapsulation), đa hình (polymorphism), và trừu tượng (abstraction).
2. **Được quản lý bởi CLR (Common Language Runtime)**: C# chạy trong môi trường quản lý .NET CLR, giúp quản lý bộ nhớ, xử lý ngoại lệ, và bảo mật.
3. **Tính đa nền tảng**: Ban đầu, C# chủ yếu được sử dụng cho các ứng dụng trên nền tảng Windows. Tuy nhiên, với sự phát triển của .NET Core và .NET 5/6/7, C# đã trở thành một ngôn ngữ đa nền tảng, cho phép phát triển ứng dụng trên Windows, Linux, macOS, và nhiều nền tảng khác.
4. **Linh hoạt và mạnh mẽ**: C# có thể được sử dụng để phát triển nhiều loại ứng dụng khác nhau, từ ứng dụng desktop, web, di động, đến các hệ thống nhúng và dịch vụ đám mây.
5. **Tích hợp chặt chẽ với .NET Framework và .NET Core**: C# tận dụng tối đa các thư viện và công cụ của .NET, giúp lập trình viên phát triển nhanh chóng và hiệu quả hơn.
6. **Ngữ pháp rõ ràng và dễ học**: C# có cú pháp tương đối dễ hiểu, gần gũi với các ngôn ngữ lập trình phổ biến như Java và C++, làm cho việc học và sử dụng ngôn ngữ này trở nên dễ dàng hơn đối với các lập trình viên.
7. **Hỗ trợ LINQ (Language Integrated Query)**: C# cung cấp khả năng truy vấn dữ liệu mạnh mẽ trực tiếp trong ngôn ngữ thông qua LINQ, giúp thao tác với các tập dữ liệu một cách hiệu quả và dễ dàng.

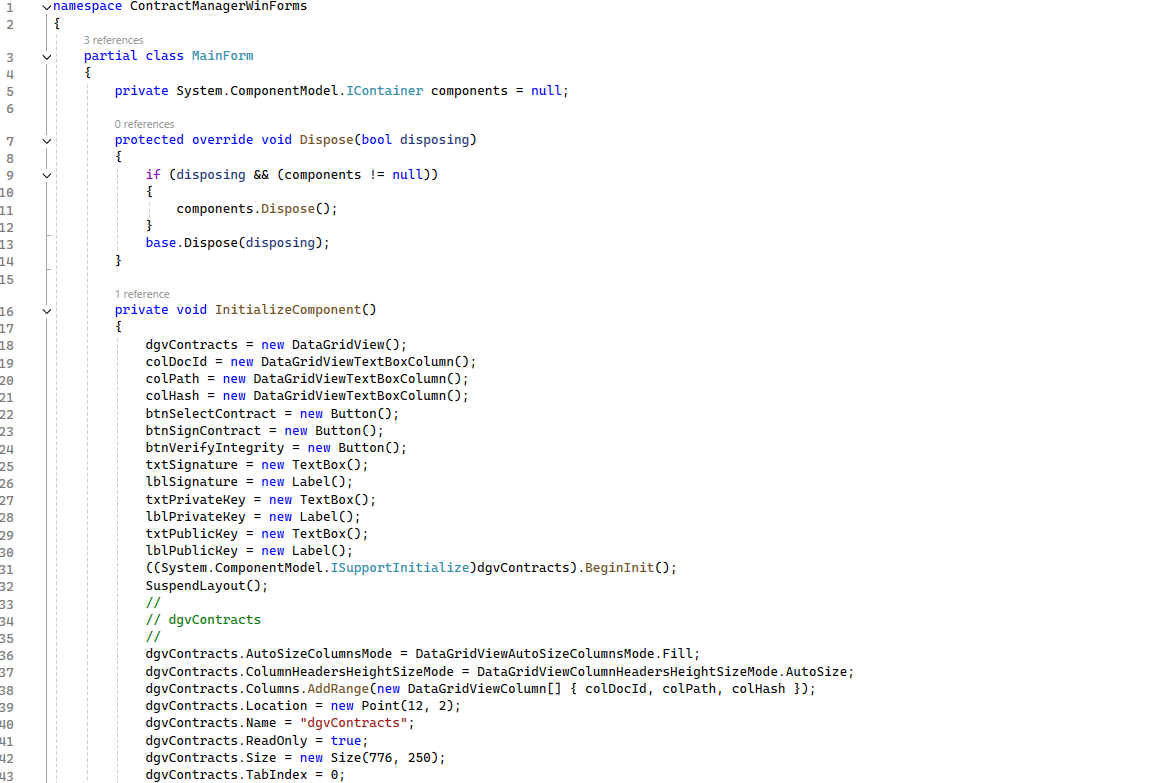
**Code sử dụng ngôn ngữ c# và chạy trên Winform c#:**

MainFrom.cs

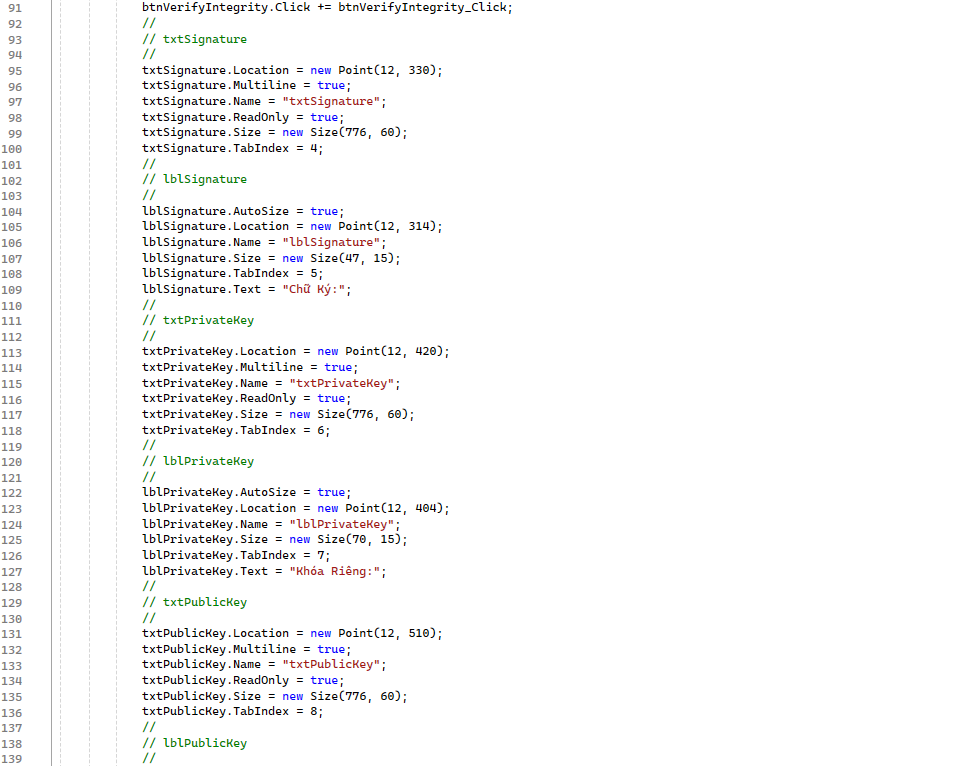




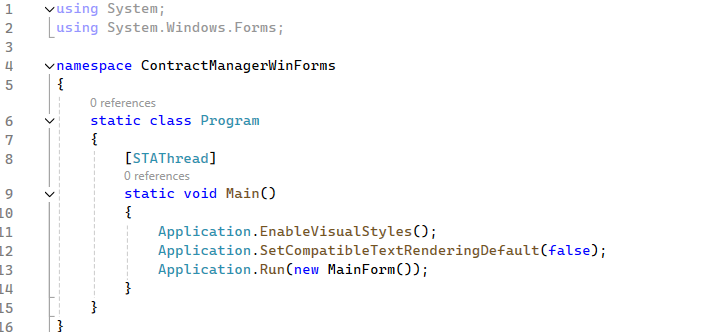
MainForm.designer







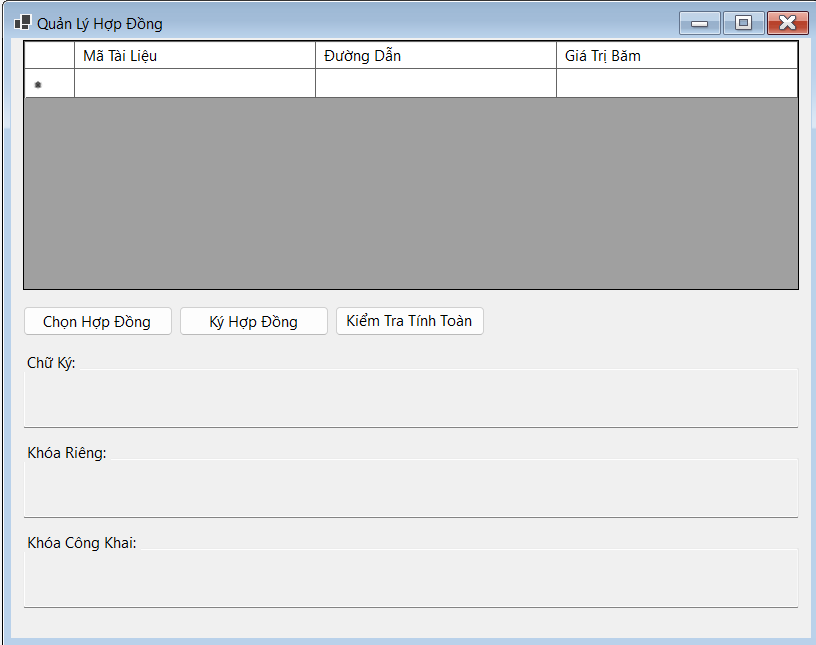




### 3.3.2 Giải thích các hàm trong code:

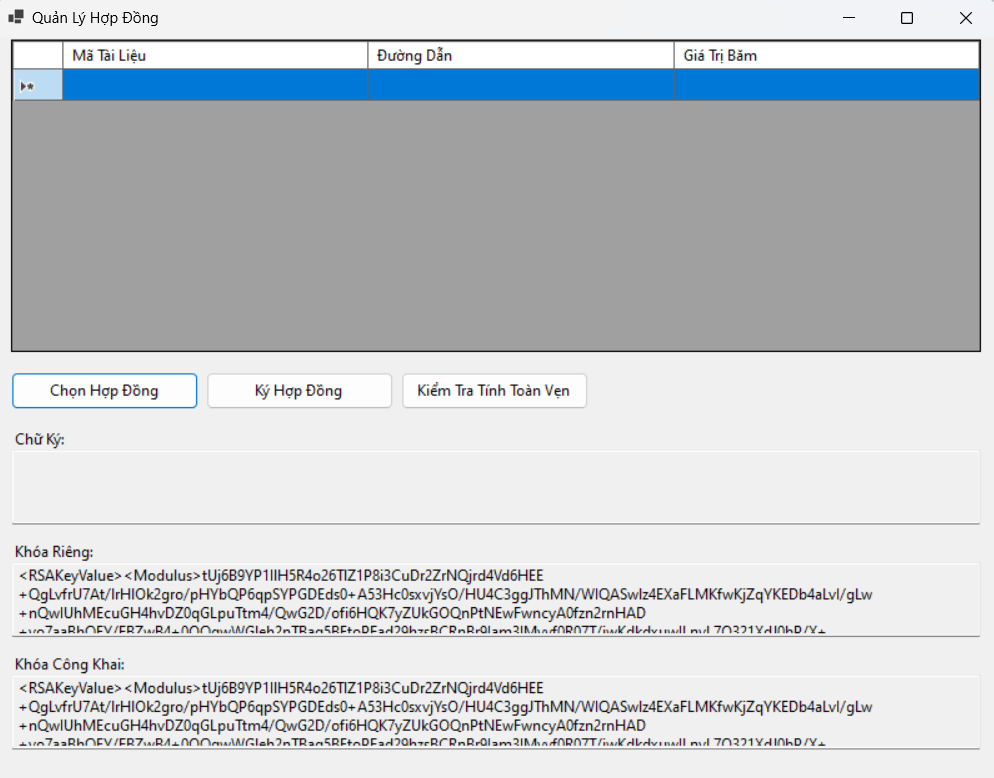
## 3.4 Mô tả giao diện người dùng và các tính năng chính của ứng dụng

### 3.4.1 Giao diện Người dùng:

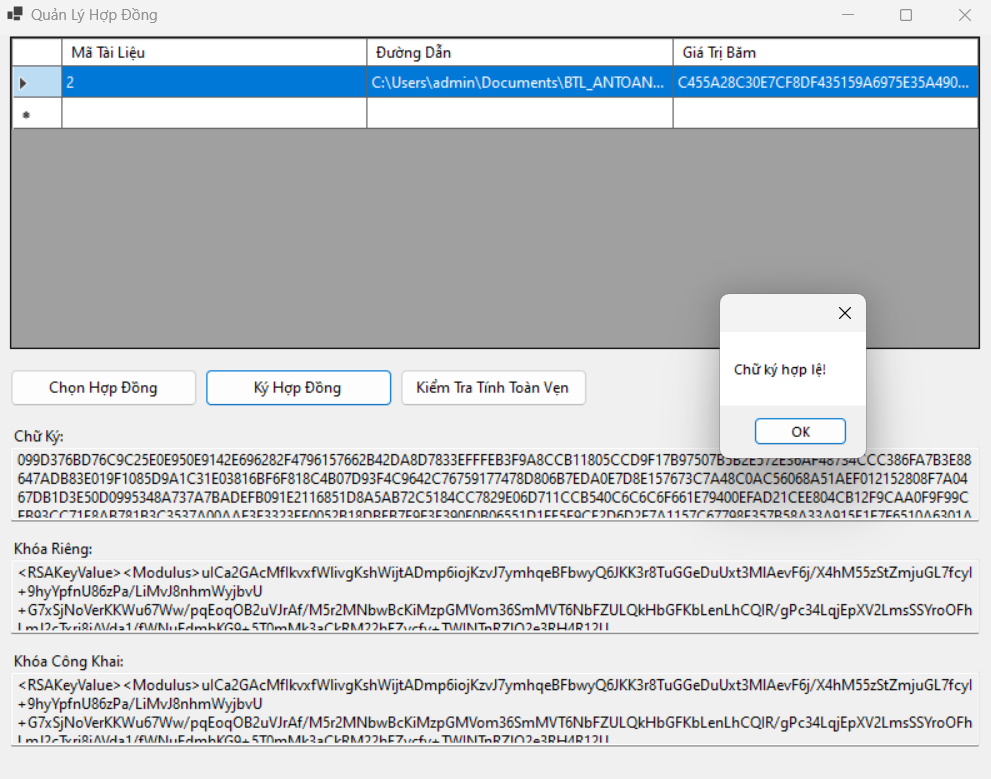


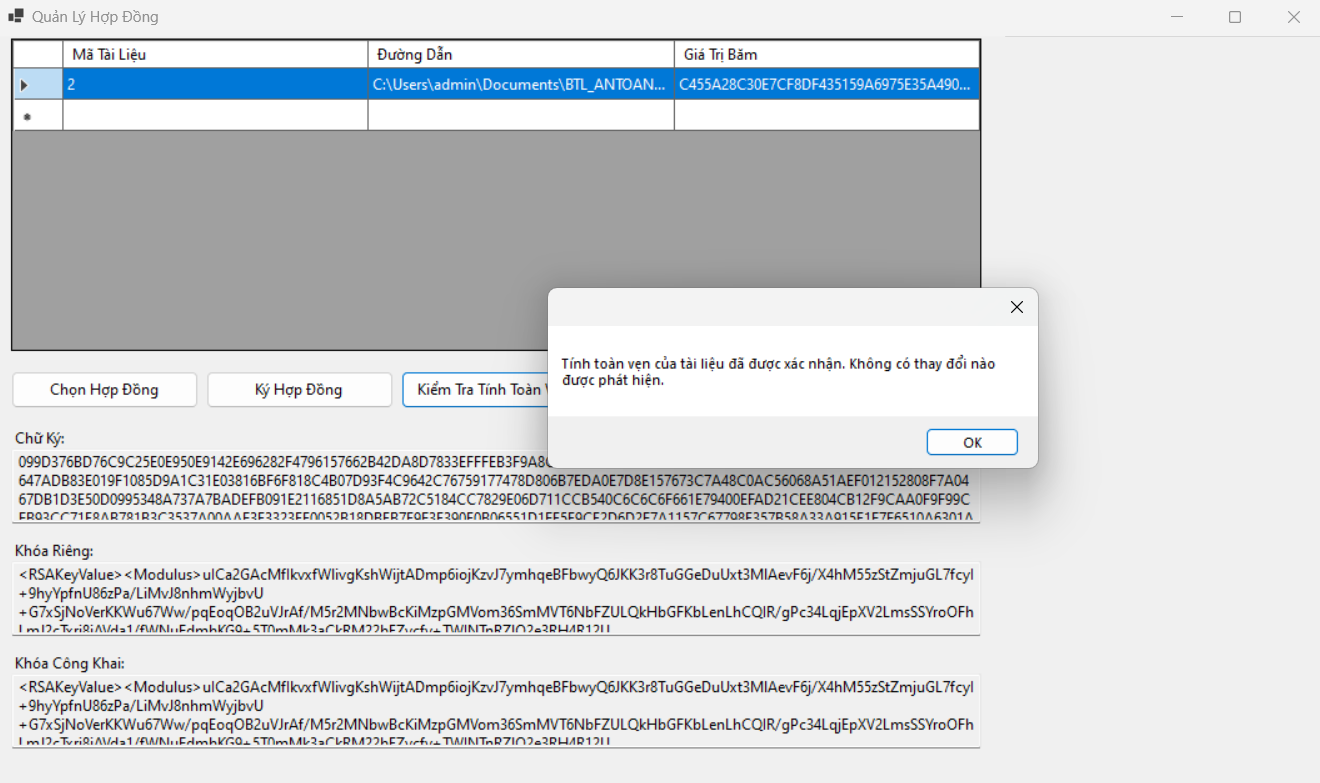
Hình 3.1. Giao diện chương trình

**Nguyên lý hoạt động:**

****

### 





### 3.4.2 Tính năng chính:

Thêm Hợp đồng: Người dùng có thể thêm mới thông tin về hợp đồng nhân viên bằng cách nhập các thông tin cần thiết vào các trường dữ liệu tương ứng.

Hiển thị Chi tiết: Cho phép người dùng xem thông tin chi tiết về một hợp đồng nhân viên cụ thể, bao gồm các thông tin như tên hợp đồng, ngày bắt đầu, ngày kết thúc, đường dẫn tới tài liệu hợp đồng và giá trị băm của tài liệu.

Ký kết Hợp đồng: Hỗ trợ quá trình ký kết hợp đồng bằng chữ ký số. Người dùng có thể chọn một hợp đồng nhân viên từ danh sách và ký kết nó bằng cách sử dụng chữ ký số của mình.

Xác thực Chữ ký: Cho phép người dùng xác thực chữ ký số của các tài liệu hợp đồng để đảm bảo tính toàn vẹn và tin cậy của chúng. Khi một hợp đồng được chọn, hệ thống sẽ kiểm tra chữ ký số của tài liệu và hiển thị kết quả xác thực.

## 3.5 Mối quan hệ giữa chữ ký số và an ninh mạng

Chữ ký số và an ninh mạng có mối quan hệ chặt chẽ với nhau. Chữ ký số là một công cụ quan trọng trong việc bảo đảm tính bảo mật và toàn vẹn của thông tin trong môi trường mạng. Dưới đây là một cái nhìn tổng quan về mối quan hệ này và cách thức triển khai chữ ký số trong an ninh mạng:

Mối quan hệ giữa chữ ký số và an ninh mạng

1. **Bảo mật và Xác thực**: Chữ ký số giúp bảo đảm rằng dữ liệu gửi đi không bị thay đổi trong quá trình truyền tải và xác thực danh tính của người gửi. Nó sử dụng mã hóa để bảo vệ dữ liệu và giúp người nhận kiểm tra tính toàn vẹn của dữ liệu.
2. **Xác thực Danh tính**: Chữ ký số cung cấp một cách thức xác thực danh tính của người dùng hoặc tổ chức, đảm bảo rằng người gửi là ai mà họ nói. Điều này giúp ngăn chặn các cuộc tấn công giả mạo và tăng cường độ tin cậy trong các giao dịch mạng.
3. **Toàn vẹn Dữ liệu**: Chữ ký số bảo đảm rằng dữ liệu không bị thay đổi sau khi nó được ký. Nếu dữ liệu bị thay đổi, chữ ký số sẽ không còn hợp lệ, giúp phát hiện và ngăn chặn các cuộc tấn công làm giả dữ liệu.
4. **Bảo vệ chống lại Tấn công Replay**: Chữ ký số có thể bao gồm thông tin thời gian, giúp ngăn chặn các tấn công replay, trong đó tin nhắn hoặc dữ liệu bị gửi lại nhiều lần để gây hiểu nhầm hoặc lừa đảo.

**Cách thức triển khai:**

- **Lựa chọn Cơ chế Mã hóa**: Đầu tiên, cần lựa chọn cơ chế mã hóa phù hợp cho chữ ký số. Thông thường, các thuật toán mã hóa như RSA, ECDSA, và DSA được sử dụng. Cơ chế mã hóa này sẽ đảm bảo rằng chữ ký số được tạo ra và xác thực chính xác.

- **Tạo và Quản lý Khóa**: Để tạo chữ ký số, bạn cần một cặp khóa: khóa riêng (private key) và khóa công khai (public key). Khóa riêng được dùng để ký dữ liệu, còn khóa công khai được dùng để xác thực chữ ký. Việc quản lý và bảo mật khóa riêng là rất quan trọng vì nếu khóa riêng bị lộ, chữ ký số sẽ không còn bảo mật.

- **Ký Dữ liệu**: Khi dữ liệu cần được ký, hệ thống sẽ tạo ra một hash (băm) của dữ liệu đó và mã hóa hash này bằng khóa riêng. Chữ ký số là bản mã hóa của hash và có thể được đính kèm vào dữ liệu gốc.

- **Xác thực Chữ ký**: Khi nhận dữ liệu, người nhận sử dụng khóa công khai để giải mã chữ ký số và lấy được hash. Sau đó, họ tạo hash từ dữ liệu nhận được và so sánh với hash đã giải mã. Nếu hai giá trị hash khớp nhau, dữ liệu không bị thay đổi và chữ ký là hợp lệ.

- **Tích hợp vào Hệ thống**: Chữ ký số có thể được tích hợp vào các hệ thống mạng như email, giao dịch điện tử, và các ứng dụng web để bảo vệ dữ liệu trong quá trình truyền tải và lưu trữ.

- **Cung cấp và Quản lý Chứng thư số**: Để chữ ký số có hiệu lực, cần có chứng thư số do một cơ quan cấp phát chứng thư số (CA) cấp. CA xác thực danh tính và phát hành chứng thư số cho người dùng hoặc tổ chức. Quản lý và duy trì chứng thư số là một phần quan trọng trong việc đảm bảo tính bảo mật của chữ ký số.

**Triển khai trên máy tính cá nhân:**

Triển khai chữ ký số trên máy tính cá nhân liên quan đến việc thiết lập và quản lý các công cụ và quy trình cần thiết để tạo và xác thực chữ ký số. Dưới đây là các bước cơ bản:

1. Cài đặt Phần mềm Chữ ký Số:
   * Chọn Phần mềm: Chọn phần mềm chữ ký số phù hợp, chẳng hạn như Adobe Acrobat, phần mềm chữ ký số của các nhà cung cấp dịch vụ chứng thư số (CA), hoặc các công cụ mã nguồn mở như OpenSSL.
   * Cài đặt và Cấu hình: Cài đặt phần mềm chữ ký số trên máy tính cá nhân và cấu hình các thiết lập cơ bản, bao gồm việc nhập các thông tin liên quan đến chứng thư số và khóa cá nhân.
2. Tạo và Quản lý Khóa:
   * Tạo Cặp Khóa: Sử dụng phần mềm chữ ký số để tạo một cặp khóa (khóa công khai và khóa riêng). Khóa riêng được dùng để ký dữ liệu, trong khi khóa công khai được dùng để xác thực chữ ký.
   * Bảo mật Khóa: Bảo vệ khóa riêng bằng cách lưu trữ nó trong một môi trường an toàn, chẳng hạn như một thiết bị phần cứng bảo mật (HSM) hoặc một phần mềm quản lý khóa an toàn.
3. Nhận và Cài đặt Chứng thư số:
   * Nhận Chứng thư số: Mua hoặc nhận chứng thư số từ một cơ quan cấp phát chứng thư số (CA). Chứng thư số xác nhận danh tính của bạn và liên kết với khóa công khai của bạn.
   * Cài đặt Chứng thư số: Cài đặt chứng thư số vào phần mềm chữ ký số hoặc trình duyệt web để bắt đầu sử dụng chữ ký số.
4. Ký Dữ liệu:
   * Ký Tài liệu: Mở tài liệu cần ký trong phần mềm chữ ký số, chọn tùy chọn ký, và sử dụng khóa riêng để tạo chữ ký số cho tài liệu. Chữ ký số sẽ được đính kèm vào tài liệu hoặc tạo ra một tệp chữ ký kèm theo tài liệu.
5. Xác thực Chữ ký:
   * Kiểm tra Chữ ký: Khi nhận tài liệu đã ký, sử dụng phần mềm chữ ký số để kiểm tra tính hợp lệ của chữ ký. Phần mềm sẽ sử dụng khóa công khai để giải mã chữ ký và so sánh hash dữ liệu để đảm bảo tính toàn vẹn.

**Cấu trúc mã nguồn:**

Cấu trúc mã nguồn của một hệ thống chữ ký số có thể bao gồm các thành phần chính sau:

1. Thư viện Mã hóa:
   * Chứa các thuật toán mã hóa và giải mã, chẳng hạn như RSA, ECDSA, hoặc DSA.
   * Ví dụ: openssl trong C/C++ hoặc thư viện pycryptodome trong Python.
2. Quản lý Khóa:
   * Cung cấp chức năng để tạo, lưu trữ và bảo vệ các khóa cá nhân và khóa công khai.
   * Ví dụ: Quản lý khóa trong các tệp khóa hoặc cơ sở dữ liệu.
3. Tạo và Xác thực Chữ ký:
   * Tạo Chữ ký: Chứa các chức năng để băm dữ liệu và ký hash bằng khóa riêng.
   * Xác thực Chữ ký: Chứa các chức năng để giải mã chữ ký, băm dữ liệu và so sánh với hash được giải mã.
4. Giao diện Người dùng:
   * Giao diện Ký: Cho phép người dùng chọn tài liệu để ký và nhập thông tin chứng thư số.
   * Giao diện Xác thực: Cho phép người dùng kiểm tra và xác thực chữ ký trên tài liệu nhận được.
5. Quản lý Chứng thư số:
   * Tích hợp CA: Giao tiếp với các cơ quan cấp phát chứng thư số để nhận và quản lý chứng thư số.
   * Kiểm tra Chứng thư: Xác thực chứng thư số để đảm bảo tính hợp lệ của nó.

Trong mã nguồn trên:

* Tạo cặp khóa: Tạo khóa riêng và khóa công khai.
* Ký dữ liệu: Tạo hash của dữ liệu và ký hash bằng khóa riêng.
* Xác thực chữ ký: Sử dụng khóa công khai để xác thực chữ ký.

# CHƯƠNG 4. KẾT LUẬN

## 4.1 Kết quả đạt được

Hiểu rõ về cách hoạt động của các thuật toán chữ ký số như RSA, Băm SHA-256 và một số thuật toán khác.

Nắm vững các nguyên lý toán học và lý thuyết trong việc triển khai các thuật toán này.

Phát triển các ứng dụng mẫu sử dụng các thuật toán chữ ký số cho các mục đích thử nghiệm và minh họa.

Thử nghiệm các chức năng mã hóa và xác thực chữ ký số trong các ứng dụng này.

Tìm hiểu về cách sử dụng ngôn ngữ lập trình c# để triển khai các thuật toán chữ ký số.

Hiểu biết về cách sử dụng các thuật toán chữ ký số để đảm bảo tính toàn vẹn và bảo mật cho thông tin.

Có khả năng đánh giá các vấn đề bảo mật liên quan và đề xuất các biện pháp cải thiện.

Độ an toàn:

**Phân tích:** RSA là một thuật toán mật mã công khai phổ biến và được công nhận là an toàn. Việc sử dụng RSA trong việc tạo chữ ký điện tử giúp đảm bảo tính bảo mật cho quản lý tài liệu hợp đồng nhân viên.

**Đánh giá:** Việc sử dụng RSA là một lựa chọn đáng tin cậy để bảo vệ dữ liệu trên hợp đồng nhân viên.

Hiệu suất:

**Phân tích:** RSA có thể làm tăng đáng kể thời gian xử lý, đặc biệt là khi sử dụng các khóa dài. Điều này có thể ảnh hưởng đến hiệu suất của hệ thống.

**Đánh giá:** Cần đánh giá hiệu suất của việc sử dụng RSA trong ứng dụng quản lý hopwkj đồng nhân viên để đảm bảo rằng thời gian xử lý vẫn đảm bảo hiệu quả và không gây ảnh hưởng đến trải nghiệm người dùng.

Quản lý khóa:

**Phân tích:** Việc quản lý khóa là một thách thức đối với việc triển khai RSA trong một hệ thống lớn. Quản lý khóa không chỉ đảm bảo tính bảo mật mà còn cần phải hiệu quả và linh hoạt.

**Đánh giá*:*** Cần đảm bảo rằng việc quản lý khóa được thực hiện một cách an toàn và hiệu quả để tránh rủi ro về bảo mật và mất mát dữ liệu

Tích hợp:

**Phân tích:** Tích hợp RSA vào hệ thống chữ ký điện tử trên trên hợp đồng nhân viên cần phải được thực hiện một cách cẩn thận để tránh gây ra sự cố hoặc ảnh hưởng đến các chức năng khác của hệ thống.

**Đánh giá:** Cần đánh giá tính khả thi của việc tích hợp RSA để đảm bảo rằng quá trình triển khai diễn ra mà không gặp vấn đề nào.

Kiểm thử:

**Phân tích:** Quá trình kiểm thử là quan trọng để đảm bảo rằng hệ thống hoạt động đúng như kỳ vọng và không có lỗ hổng bảo mật.

**Đánh giá:** Cần thực hiện kiểm thử kỹ lưỡng để đảm bảo tính chính xác và an toàn của hệ thống trước khi triển khai.

Tính thực tế:

**Phân tích*:*** Đánh giá xem việc triển khai RSA có phù hợp với yêu cầu và ngữ cảnh cụ thể của việc quản lý hpwj đồng nhân viên.

**Đánh giá:** Việc đảm bảo tính thực tế của triển khai RSA là quan trọng để đảm bảo rằng nó đáp ứng được nhu cầu và mong muốn của các công ty tronh viện quản lý hợp đồng nhân viên.

## 4.2 Hướng phát triển

Tiếp tục phát triển và thử nghiệm các ứng dụng thực tiễn sử dụng các thuật toán chữ ký số trong các tình huống thực tế.

Việc mở rộng tính năng giúp ứng dụng trở nên đa dạng và đáp ứng nhiều nhu cầu hơn của người dùng.

Đảm bảo ứng dụng hoạt động ổn định và đáp ứng các yêu cầu bảo mật cụ thể.

Nghiên cứu và áp dụng các công nghệ mới trong lĩnh vực an toàn bảo mật để cải thiện và mở rộng các giải pháp chữ ký số.

Tìm hiểu về các công nghệ mới như blockchain và áp dụng chúng vào các ứng dụng chữ ký số.

Tiếp tục nghiên cứu và cập nhật kiến thức về các tiêu chuẩn và các cải tiến mới trong lĩnh vực chữ ký số.

Chia sẻ kiến thức và kinh nghiệm với cộng đồng lập trình và an toàn bảo mật thông qua việc viết bài blog, tham gia diễn đàn và đóng góp vào các dự án mã nguồn mở liên quan.

# TÀI LIỆU THAM KHẢO

[1] Tan, Z., Jia, K., & Yan, L. (2019). Research on Contract Management of Construction Enterprises Based on Blockchain Technology. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 835-839). IEEE.

[2] Barboza, F. G., de Carvalho, M. M., & do Prado Leite, J. C. S. (2020). A framework for electronic contract management based on blockchain smart contracts. Enterprise Information Systems, 1-31.

[3] Hlaing, A. N. (2018). The Security of Digital Signature. International Journal of Advanced Computer Science and Applications, 9(10), 452-458.

[4] Allen, J., & Moulton, S. (2019). Signature Technology for the Web. W3C Recommendation, 4.

[5] Liu, B., Huang, H., Li, M., & Zhang, T. (2018). Blockchain-based electronic signature for electronic contract. In 2018 IEEE International Conference on Mechatronics and Automation (ICMA) (pp. 2083-2088). IEEE.

[6] Benito, M., Simal, I., & Molina, J. M. (2019). A System for Digital Signature and Verification of Documents Using Blockchain and RFID. In International Conference on Smart Communications in Network Technologies (pp. 95-103). Springer, Cham.