

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO THỰC NGHIỆM**

**HỌC PHẦN:AN NINH MẠNG**

**ĐỀ TÀI:** **CHỮ KÝ SỐ RSA VÀ ỨNG DỤNG TRONG XÁC THỰC TÍNH TOÀN VẸN CỦA DỮ LIỆU**

Giảng viến hướng dẫn : TS. Phạm Văn Hiệp

Lớp : 202412IT6070001

Khóa : K16

Nhóm : 1

Sinh viên thực hiện : Trần Gia Hoàng - 2021605995

Phạm Việt Hưng - 2021603253

Phạm Đức Toản – 2021606942

Trần Xuân Đức - 2022600490

Đỗ Trọng Thích – 2021604318

**Hà Nội – 2024**

# MỤC LỤC

**Contents**

[**MỤC LỤC 2**](#_Toc184336714)

[**DANH MỤC VIẾT TẮT 4**](#_Toc184336715)

[**DANH MỤC HÌNH ẢNH 5**](#_Toc184336716)

[**DANH MỤC BẢNG BIỂU 6**](#_Toc184336717)

[**LỜI CẢM ƠN 7**](#_Toc184336718)

[**LỜI MỞ ĐẦU 8**](#_Toc184336719)

[**CHƯƠNG 1 TỔNG QUAN VỀ ĐỀ TÀI 10**](#_Toc184336720)

[**1.1. Tổng quan về an ninh mạng 10**](#_Toc184336721)

[**1.2. Các kiến thức cơ sở 11**](#_Toc184336722)

[**1.3. Nội dung nghiên cứu 17**](#_Toc184336723)

[**1.3.1. Lý do chọn đề tài 17**](#_Toc184336724)

[**1.3.2. Các nội dung nghiên cứu 18**](#_Toc184336725)

[**1.4. Giới thiệu về RSA 19**](#_Toc184336726)

[**CHƯƠNG 2 KẾT QUẢ NGHIÊN CỨU 21**](#_Toc184336727)

[**2.1. Nghiên cứu, tìm hiểu về mô hình mạng an toàn 21**](#_Toc184336728)

[**2.1.1. Các thành phần chính của mô hình mạng an toàn 21**](#_Toc184336729)

[**2.1.2. Các công nghệ hỗ trợ 21**](#_Toc184336730)

[**2.2. Các mô hình mạng an toàn sử dụng trong doanh nghiệp 21**](#_Toc184336731)

[**2.3. Nghiên cứu mô hình mạng an toàn cho công ty 21**](#_Toc184336732)

[**2.3.1. Cấu trúc cơ bản 21**](#_Toc184336733)

[**2.3.2. Các thành phần chính 21**](#_Toc184336734)

[**2.3.3. Cách thức hoạt động 21**](#_Toc184336735)

[**2.3.4. Ứng dụng 21**](#_Toc184336736)

[**2.4. Thực nghiệm mô hình mạng an toàn cho công ty 21**](#_Toc184336737)

[**2.4.1. Giới thiệu công cụ hỗ trợ mô phỏng: packet tracer 21**](#_Toc184336738)

[**2.4.2. Mục tiêu của hệ thống thực nghiệm 21**](#_Toc184336739)

[**2.4.3. Thiết kế kịch bản chương trình 21**](#_Toc184336740)

[**2.4.4. Giải pháp bảo mật trong hệ thống thực nghiệm 21**](#_Toc184336741)

[**2.4.5. Mô phỏng, triển khai thực nghiệm 21**](#_Toc184336742)

[**CHƯƠNG 3 KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM 22**](#_Toc184336743)

[**3.1. Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài. 22**](#_Toc184336744)

[**3.2. Bài học kinh nghiệm 22**](#_Toc184336745)

[**3.3. Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn 22**](#_Toc184336746)

[**KẾT LUẬN 23**](#_Toc184336747)

[**TÀI LIỆU THAM KHẢO 25**](#_Toc184336748)

# DANH MỤC VIẾT TẮT

# DANH MỤC HÌNH ẢNH

[Hình 1. 1: Sơ đồ biểu diễn thuật toán mã hóa RSA 12](#_Toc184336469)

[Hình 1. 2: Các tác giả 20](#_Toc184336470)

# DANH MỤC BẢNG BIỂU

**LỜI CẢM ƠN**

Lời đầu tiên, chúng em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến các thầy cô trong khoa Công nghệ Thông tin - Trường Đại học Công Nghiệp Hà Nội. Nhờ sự tận tâm và nhiệt huyết của các thầy cô trong suốt quá trình giảng dạy, chúng em đã tiếp thu được những kiến thức quý báu, không chỉ giúp ích cho quá trình học tập mà còn là hành trang quan trọng cho sự nghiệp sau này.

Đặc biệt, chúng em xin gửi lời tri ân sâu sắc đến thầy **Phạm Văn Hiệp**, người đã trực tiếp hướng dẫn, dìu dắt chúng em trong suốt quá trình thực hiện đồ án. Thầy không chỉ cung cấp cho chúng em những kiến thức chuyên môn cần thiết mà còn khơi dậy tinh thần học hỏi, sáng tạo, và khả năng giải quyết vấn đề. Sự hỗ trợ tận tình và những chỉ bảo quý báu của thầy đã giúp chúng em vượt qua nhiều khó khăn, thử thách để hoàn thành đồ án này.

Mặc dù đã nỗ lực hết sức, nhưng do còn hạn chế về kiến thức và kinh nghiệm, chúng em chắc chắn không thể tránh khỏi những thiếu sót. Chúng em rất mong nhận được sự thông cảm và những ý kiến đóng góp quý báu từ các thầy cô và các bạn để chúng em có thể hoàn thiện đồ án này một cách tốt nhất. Chúng em xin trân trọng cảm ơn!

**Nhóm thực hiện**

Trần Gia Hoàng

Phạm Việt Hưng

Phạm Đức Toản

Trần Xuân Đức

Đỗ Trọng Thích

# LỜI MỞ ĐẦU

Trong thời đại công nghệ thông tin phát triển vượt bậc, an ninh mạng đã trở thành một trong những lĩnh vực trọng yếu, quyết định sự an toàn và phát triển của các cá nhân, tổ chức và quốc gia. Trước sự gia tăng không ngừng của các cuộc tấn công mạng, việc xây dựng các mô hình mạng an toàn và ứng dụng các giải pháp bảo mật hiệu quả không chỉ là nhu cầu cấp thiết mà còn là thách thức lớn đối với ngành công nghệ thông tin.

Các mô hình mạng an toàn không chỉ đảm bảo tính bảo mật, toàn vẹn, và khả dụng của dữ liệu mà còn đóng vai trò quan trọng trong việc bảo vệ tài nguyên hệ thống khỏi những mối đe dọa tiềm tàng. Điều này đặc biệt cần thiết đối với các doanh nghiệp, nơi mà hệ thống mạng không chỉ là xương sống của các hoạt động kinh doanh mà còn là mục tiêu chính của các cuộc tấn công mạng.

Với mục tiêu nghiên cứu và tìm hiểu sâu hơn về an ninh mạng, nhóm chúng em đã thực hiện đề tài “Mô hình mạng an toàn và ứng dụng trong doanh nghiệp”. Đề tài tập trung vào việc xây dựng, phân tích và thực nghiệm một mô hình mạng an toàn, đồng thời đề xuất các giải pháp bảo mật hiệu quả, góp phần nâng cao nhận thức và năng lực ứng dụng trong lĩnh vực này.

Báo cáo được chia thành các chương chính như sau:

**Chương 1: Tổng quan về đề tài** – Chương này giới thiệu tổng quan về an ninh mạng, các kiến thức cơ sở liên quan đến an toàn thông tin và tấn công mạng, đồng thời trình bày lý do và nội dung nghiên cứu.

**Chương 2: Kết quả nghiên cứu** – Chương này trình bày các mô hình mạng an toàn, phân tích các thành phần chính và công nghệ hỗ trợ, ứng dụng các mô hình mạng trong doanh nghiệp, đồng thời thực nghiệm mô hình mạng an toàn với các công cụ hỗ trợ như Packet Tracer.

**Chương 3: Kết luận và bài học kinh nghiệm** – Chương này tóm tắt các kiến thức, kỹ năng đã học được, rút ra bài học kinh nghiệm và đánh giá tính khả thi của chủ đề nghiên cứu.

Qua quá trình thực hiện đề tài, chúng em không chỉ hiểu rõ hơn về các mô hình mạng an toàn mà còn nắm vững các giải pháp bảo mật hiện đại, từ đó có thể ứng dụng vào thực tiễn. Chúng em kỳ vọng rằng báo cáo này sẽ mang đến những giá trị hữu ích, góp phần nâng cao hiệu quả bảo mật hệ thống mạng, đặc biệt trong bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng.

# CHƯƠNG 1 TỔNG QUAN VỀ ĐỀ TÀI

## Tổng quan về an ninh mạng

Trong kỷ nguyên số, mọi thứ đều được kết nối, từ chiếc điện thoại thông minh đến các hệ thống công nghiệp. Sự tiện lợi mà công nghệ mang lại đi kèm với những rủi ro tiềm ẩn về an ninh mạng. Các cuộc tấn công mạng ngày càng tinh vi và đa dạng, đe dọa không chỉ các tổ chức lớn mà còn cả cá nhân. Từ những vụ rò rỉ dữ liệu quy mô lớn làm chấn động toàn cầu đến các cuộc tấn công ransomware khiến các hệ thống tê liệt, an ninh mạng đã trở thành một vấn đề cấp bách.

Những kẻ tấn công không ngừng tìm kiếm những lỗ hổng trong hệ thống để đánh cắp dữ liệu, phá hoại hoạt động và tống tiền. Các hình thức tấn công cũng trở nên đa dạng hơn, từ các cuộc tấn công truyền thống như phần mềm độc hại, phishing đến các cuộc tấn công nhắm vào các thiết bị IoT, trí tuệ nhân tạo và blockchain.

Để đối phó với những thách thức này, các tổ chức cần xây dựng một chiến lược an ninh mạng toàn diện, kết hợp các giải pháp công nghệ hiện đại với việc nâng cao nhận thức của người dùng. Việc đầu tư vào các công cụ bảo mật như tường lửa, hệ thống phát hiện xâm nhập, và các giải pháp AI để phát hiện các mối đe dọa mới là vô cùng cần thiết. Bên cạnh đó, việc đào tạo nhân viên về an ninh mạng, xây dựng các quy trình bảo mật chặt chẽ và thường xuyên cập nhật các biện pháp phòng thủ cũng đóng vai trò quan trọng.

Tuy nhiên, an ninh mạng không chỉ là một vấn đề công nghệ. Đó còn là một cuộc chiến giữa trí tuệ của con người. Các hacker luôn tìm kiếm những cách thức mới để tấn công, trong khi các chuyên gia bảo mật phải không ngừng đổi mới để đối phó. Đây là một cuộc đua không có hồi kết, đòi hỏi sự sáng tạo, kiên trì và sự hợp tác giữa các tổ chức, chính phủ và cộng đồng.

Mặc dù đối mặt với nhiều thách thức, an ninh mạng cũng mang đến những cơ hội lớn. Việc phát triển các giải pháp bảo mật hiệu quả không chỉ giúp bảo vệ dữ liệu mà còn tạo ra những sản phẩm, dịch vụ mới, thúc đẩy sự phát triển của ngành công nghiệp bảo mật. Bên cạnh đó, việc nâng cao nhận thức về an ninh mạng cũng giúp mọi người trở thành những người sử dụng internet an toàn hơn.

Tóm lại, an ninh mạng là một vấn đề quan trọng ảnh hưởng đến mọi khía cạnh của cuộc sống số. Để xây dựng một thế giới số an toàn và đáng tin cậy, chúng ta cần chung tay nỗ lực, đầu tư vào công nghệ, nâng cao nhận thức và không ngừng học hỏi để đối phó với những thách thức mới.

## Các kiến thức cơ sở

**1.2.1 Toán học cơ bản**

* **Số nguyên tố**: Hai số nguyên tố lớn được sử dụng để tạo khóa trong RSA.
* **Modulo**: Dùng trong mã hóa và giải mã để xử lý các phép toán với số lớn.
* **Thuật toán Euclid mở rộng**: Tìm nghịch đảo modulo – một bước quan trọng để tính khóa bí mật trong RSA.

**1.2.2 Thuật toán RSA**

*Định lý cơ sở:*

Định lý nhỏ của Fermat: Với p là một số nguyên tố khác 2 thì chia một số a lũy thừa p cho p sẽ có số dư chính bằng a:

Mở rộng ta có:

Với là số nguyên tố cùng nhau với m và nhỏ hơn m

Thuật toán RSA có 2 khóa:

* Khóa công khai (Public Key)
* Khóa bí mật (Private Key)

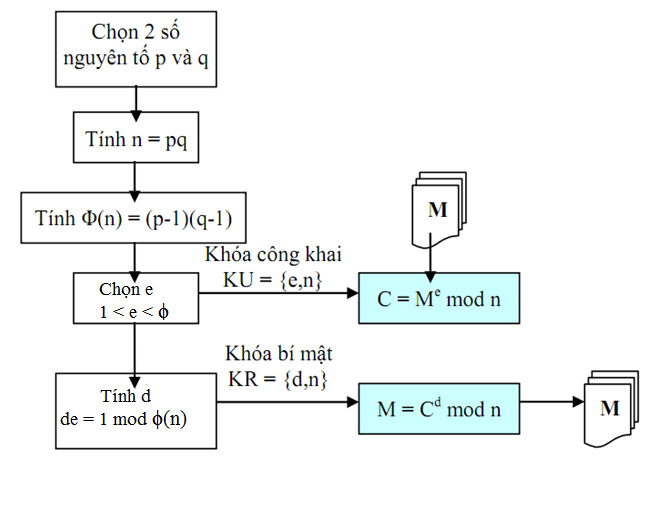
Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã.

Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa.

Khóa bí mật được cá nhân giữ kín và dùng để giải mã

*Ví dụ:* Bod muốn gửi cho Alice một thông tin mật M mà Bod muốn duy nhất Alice có thể đọc được.

|  |  |  |  |
| --- | --- | --- | --- |
| Bod |  | | Alice |
| ( Mã hóa M bằng Public Key của A đc C) | | (Giải mã C bằng Private Key của A đc M ) | |



Hình 1. : Sơ đồ biểu diễn thuật toán mã hóa RSA

1. **Quá trình tạo khóa cho hệ mật mã RSA:**

Giả sử Alice và Bob cần trao đổi thông tin bí mật thông qua một kênh không an toàn (ví dụ như [Internet](http://vi.wikipedia.org/wiki/Internet)). Với thuật toán RSA, Alice đầu tiên cần tạo ra cho mình cặp khóa gồm khóa công khai và khóa bí mật theo 5 bước sau:

1. Chọn 2 số nguyên tố lớn khác nhau p, q thỏa mãn điều kiện
2. Tính tích của nó
3. Tính giá trị hàm Phi Euler của n:
4. Chọn số nguyên d, sao cho và
5. Tính giá trị e thỏa mãn điều kiện:

**Khóa công khai** bao gồm: n và e. **Khóa mật:** d còn p,q và A black background with a black square

Description automatically generated with medium confidencethường là xóa sau khi tính toán khóa.

1. **Quá trình mã hóa**

Giả sử Bob muốn gửi đoạn thông tin M cho Alice. Đầu tiên Bob chuyển M thành một số m < n theo một hàm có thể đảo ngược (từ m có thể xác định lại M) được thỏa thuận trước. Quá trình này được mô tả ở phần Chuyển đổi văn bản rõ.

Lúc này Bob có m và biết n cũng như e do Alice gửi. Bob sẽ tính c là bản mã hóa của m theo công thức:

Hàm trên có thể tính dễ dàng sử dụng phương pháp tính hàm mũ (môđun) bằng phương pháp bình phương. Cuối cùng Bob gửi C cho Alice

1. **Quá trình giải mã**

Alice nhận *c* từ Bob và khóa bí mật *d*. Alice có thể tìm được m từ *c* theo công thức sau:

Biết m, Alice tìm lại M theo phương pháp đã thỏa thuận trước. Quá trình giải mã hoạt động vì ta có:

Do và , theo [Định lý Fermat nhỏ](http://vi.wikipedia.org/w/index.php?title=%C4%90%E1%BB%8Bnh_l%C3%BD_Fermat_nh%E1%BB%8F&action=edit) nên:

Và

Do p và q là hai số nguyên tố cùng nhau, áp dụng định lý phần dư trung hoa, chúng ta có:

Hay

1. **Ví dụ**

Sau đây là một ví dụ với những số cụ thể. Ở đây chúng ta sử dụng những số nhỏ để tiện tính toán còn trong thực tế phải dùng các số có giá trị đủ lớn.

Lấy:

* p = 61 : số nguyên tố thứ nhất (giữ bí mật hoặc hủy sau khi tạo khóa)
* q = 53 : số nguyên tố thứ hai (giữ bí mật hoặc hủy sau khi tạo khóa)
* n = pq = 3233: môđun (công bố công khai)
* e = 17 : số mũ công khai
* d = 2753: số mũ bí mật
* Khóa công khai là cặp (*e*, *n*). Khóa bí mật là *d*. Hàm mã hóa là:

encrypt(*m*) = *me* mod *n* = *m*17 mod 3233

với *m* là [văn bản rõ](http://vi.wikipedia.org/w/index.php?title=V%C4%83n_b%E1%BA%A3n_r%C3%B5&action=edit&redlink=1). Hàm giải mã là:

decrypt(*c*) = *cd* mod *n* = *c*2753 mod 3233

với *c* là [văn bản mã](http://vi.wikipedia.org/w/index.php?title=V%C4%83n_b%E1%BA%A3n_m%C3%A3&action=edit&redlink=1).

* Để mã hóa văn bản có giá trị 123, ta thực hiện phép tính:

Encrypt (123) = 12317 mod 3233 = 855

* Để giải mã văn bản có giá trị 855, ta thực hiện phép tính:

Decrypt (855) = 8552753 mod 3233 = 123

Cả hai phép tính trên đều có thể được thực hiện hiệu quả nhờ giải thuật bình phương và nhân

1. **Chuyển đổi văn bản rõ**

Trước khi thực hiện mã hóa, ta phải thực hiện việc chuyển đổi văn bản rõ (chuyển đổi từ M sang m) sao cho không có giá trị nào của M tạo ra văn bản mã không an toàn.

Nếu không có quá trình này, RSA sẽ gặp phải một số vấn đề sau:

* Nếu m = 0 hoặc m = 1 sẽ tạo ra các bản mã có giá trị là 0 và 1 tương ứng
* Khi mã hóa với số mũ nhỏ (chẳng hạn e = 3) và m cũng có giá trị nhỏ, giá trị me cũng nhận giá trị nhỏ (so với n). Như vậy phép môđun không có tác dụng và có thể dễ dàng tìm được m bằng cách khai căn bậc e của c (bỏ qua môđun).
* RSA là phương pháp mã hóa xác định (không có thành phần ngẫu nhiên) nên kẻ tấn công có thể thực hiện tấn công lựa chọn bản rõ bằng cách tạo ra một bảng tra giữa bản rõ và bản mã. Khi gặp một bản mã, kẻ tấn công sử dụng bảng tra để tìm ra bản rõ tương ứng.

Trên thực tế, ta thường gặp 2 vấn đề đầu khi gửi các bản tin ASCII ngắn với m là nhóm vài ký tự ASCII. Một đoạn tin chỉ có 1 ký tự NULL sẽ được gán giá trị m = 0 và cho ra bản mã là 0 bất kể giá trị của e và N. Tương tự, một ký tự ASCII khác, SOH, có giá trị 1 sẽ luôn cho ra bản mã là 1. Với các hệ thống dùng giá trị e nhỏ thì tất cả ký tự ASCII đều cho kết quả mã hóa không an toàn vì giá trị lớn nhất của m chỉ là 255 và 2553 nhỏ hơn giá trị n chấp nhận được. Những bản mã này sẽ dễ dàng bị phá mã.

Để tránh gặp phải những vấn đề trên, RSA trên thực tế thường bao gồm một hình thức chuyển đổi ngẫu nhiên hóa m trước khi mã hóa. Quá trình chuyển đổi này phải đảm bảo rằng m không rơi vào các giá trị không an toàn. Sau khi chuyển đổi, mỗi bản rõ khi mã hóa sẽ cho ra một trong số khả năng trong tập hợp bản mã. Điều này làm giảm tính khả thi của phương pháp tấn công lựa chọn bản rõ (một bản rõ sẽ có thê tương ứng với nhiều bản mã tùy thuộc vào cách chuyển đổi).

Một số tiêu chuẩn, chẳng hạn như PKCS, đã được thiết kế để chuyển đổi bản rõ trước khi mã hóa bằng RSA. Các phương pháp chuyển đổi này bổ xung thêm bit vào M. Các phương pháp chuyển đổi cần được thiết kế cẩn thận để tránh những dạng tấn công phức tạp tận dụng khả năng biết trước được cấu trúc của bản rõ. Phiên bản ban đầu của PKCS dùng một phương pháp đặc ứng (ad-hoc) mà về sau được biết là không an toàn trước tấn công lựa chọn bản rõ thích ứng (adaptive chosen ciphertext attack). Các phương pháp chuyển đổi hiện đại sử dụng các kỹ thuật như chuyển đổi mã hóa bất đối xứng tối ưu như (Optimal Asymmetric Encryption Padding – OAEP) để chống lại tấn công dạng này. Tiêu chuẩn PKCS còn được bổ xung các tính năng khác để đảm bảo an toàn cho chữ ký RSA (Probabilistic Signature Scheme for RSA-RSA-PSS).

1. **Tạo chữ ký vào văn bản**

Thuật toán RSA còn được dùng để tạo chữ ký số cho văn bản.

Giả sử Alice muốn gửi cho Bob một văn bản có chữ ký của mình. Để làm việc này, Alice tạo ra một ***giá trị băm* (**hash value) của văn bản cần ký và tính giá trị mũ **d mod n** của nó (giống như khi Alice thực hiện giải mã). Giá trị cuối cùng chính là chữ ký điện tử của văn bản đang xét.

Khi Bob nhận được văn bản cùng với chữ ký điện tử, anh ta tính giá trị mũ **e mod n** của chữ ký đồng thời với việc tính giá trị băm của văn bản. Nếu 2 giá trị này như nhau thì Bob biết rằng người tạo ra chữ ký biết khóa bí mật của Alice và văn bản đã không bị thay đổi sau khi ký.

Cần chú ý rằng các phương pháp chuyển đổi bản rõ (như RSA-PSS) giữ vai trò quan trọng đối với quá trình mã hóa cũng như chữ ký điện tử và không được dùng chung cho đồng thời cho cả hai mục đích trên.

**1.2.3 Ngôn ngữ lập trình**

* **Java**: Hỗ trợ nhiều thư viện mã hóa như java.security.
* **C#**: Cung cấp các API mạnh mẽ qua System.Security.Cryptography.

## Nội dung nghiên cứu

### Lý do chọn đề tài

Trong kỷ nguyên số hiện nay, an ninh mạng đóng vai trò cực kỳ quan trọng trong việc bảo vệ thông tin và dữ liệu. Việc đảm bảo tính toàn vẹn và xác thực của dữ liệu là một thách thức lớn, đặc biệt khi dữ liệu được truyền tải và lưu trữ trên các hệ thống mạng mở và dễ bị tấn công. Chữ ký số RSA, một trong những thuật toán mật mã học bất đối xứng phổ biến nhất, cung cấp một giải pháp hiệu quả cho vấn đề này. Đề tài này được chọn vì:

* Tính thời sự và cấp thiết: Với sự gia tăng của các hoạt động tội phạm mạng, việc bảo vệ tính toàn vẹn dữ liệu là một nhu cầu bức thiết. Chữ ký số RSA đóng vai trò quan trọng trong nhiều ứng dụng, từ giao dịch điện tử đến bảo mật hệ điều hành.
* Tính ứng dụng thực tiễn: Chữ ký số RSA được ứng dụng rộng rãi trong thực tế, giúp người dùng có thể hiểu rõ hơn về cơ chế hoạt động và tầm quan trọng của nó trong bảo mật thông tin.

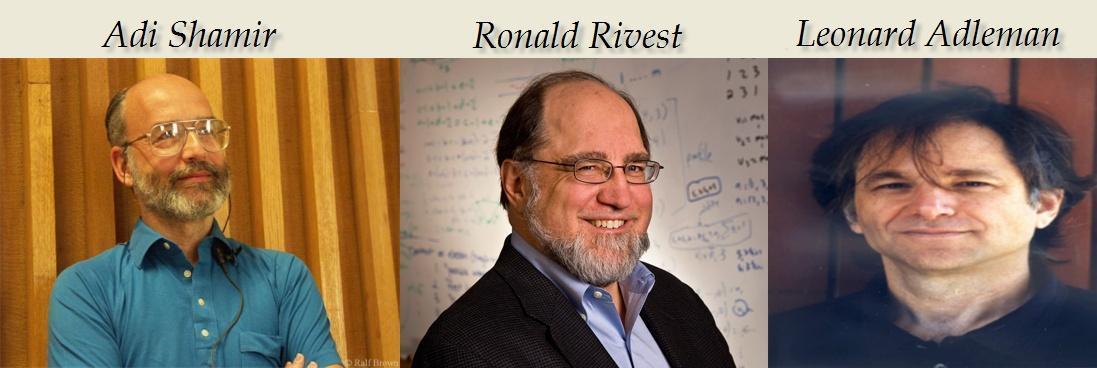
### Các nội dung nghiên cứu

Đề tài sẽ tập trung vào các nội dung chính sau:

* **Giới thiệu về chữ ký số và tầm quan trọng của nó trong bảo mật thông tin:** Phần này sẽ định nghĩa chữ ký số, phân loại các loại chữ ký số, và nhấn mạnh vai trò của chữ ký số trong việc đảm bảo tính toàn vẹn, xác thực và không chối bỏ dữ liệu.
* **Thuật toán chữ ký số RSA:** Phần này sẽ đi sâu vào chi tiết thuật toán RSA, bao gồm:
  + **Nguyên lý hoạt động:** Giải thích cơ chế hoạt động của RSA dựa trên vấn đề khó tính toán phân tích thừa số nguyên tố lớn.
  + **Các bước tạo khóa:** Mô tả chi tiết quá trình tạo cặp khóa công khai và khóa riêng.
  + **Các bước tạo và xác thực chữ ký:** Giải thích chi tiết các bước tạo chữ ký số và quá trình xác thực chữ ký.
  + **Phân tích độ an toàn:** Thảo luận về độ an toàn của thuật toán RSA và các tấn công tiềm tàng.
* **Ứng dụng của chữ ký số RSA trong xác thực tính toàn vẹn dữ liệu:** Phần này sẽ tập trung vào việc minh họa cách thức sử dụng chữ ký số RSA để bảo vệ tính toàn vẹn của dữ liệu, bao gồm:
  + **Xác thực tính toàn vẹn của tập tin:** Mô tả cách sử dụng RSA để kiểm tra xem một tập tin có bị thay đổi hay không.
  + **Bảo mật giao tiếp:** Giải thích cách RSA được sử dụng để bảo mật quá trình truyền dữ liệu giữa các hệ thống.
  + **Ví dụ cụ thể:** Trình bày một số ví dụ minh họa cụ thể về ứng dụng của chữ ký số RSA trong các hệ thống thực tế.
* **So sánh chữ ký số RSA với các thuật toán khác:** So sánh ưu điểm, nhược điểm của RSA so với các thuật toán chữ ký số khác như DSA, ECDSA, v.v. Đánh giá hiệu quả và tính khả thi của RSA trong các ứng dụng khác nhau.
* **Thực trạng và xu hướng phát triển của chữ ký số RSA:** Phân tích thực trạng ứng dụng chữ ký số RSA hiện nay và dự báo xu hướng phát triển trong tương lai. Bao gồm cả việc thảo luận về các thách thức và giải pháp liên quan đến việc đảm bảo an toàn cho chữ ký số RSA.

## Giới thiệu về RSA

Tiêu chuẩn Rivest-Shamir-Adleman (RSA) - Giải thuật mã hóa khóa công khai RSA là một tiêu chuẩn được các tác giả Ronald Rivest, Adi Shamir và Leonard Adleman phát triển tại Học Viện Công nghệ Massachusetts (MIT) vào năm 1977, tên tiêu chuẩn được lấy từ 3 chữ cái đầu của tên 3 tác giả, hiện tiêu chuẩn được các tổ chức Viện Tiêu chuẩn Quốc gia Hoa Kỳ (American National Standards Institute – ANSI), Viện Kỹ nghệ Điện và Điện tử (Institute of Electrical and Electronics Engineers – IEEE) và Phòng thí nghiệm RSA công nhận (RSA Laboratories là một bộ phận của Tập đoàn EMC). Đây là thuật toán đầu tiên phù hợp với việc tạo ra [chữ ký điện tử](http://vi.wikipedia.org/wiki/Ch%E1%BB%AF_k%C3%BD_%C4%91i%E1%BB%87n_t%E1%BB%AD) đồng thời với việc [mã hóa](http://vi.wikipedia.org/wiki/M%C3%A3_h%C3%B3a). Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực [mật mã học](http://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_h%E1%BB%8Dc) trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong [thương mại điện tử](http://vi.wikipedia.org/wiki/Th%C6%B0%C6%A1ng_m%E1%BA%A1i_%C4%91i%E1%BB%87n_t%E1%BB%AD) và được cho là đảm bảo an toàn với điều kiện độ dài [khóa](http://vi.wikipedia.org/wiki/Kh%C3%B3a_%28m%E1%BA%ADt_m%C3%A3%29) đủ lớn.



Hình 1. : Các tác giả

Trước đó vài năm, Clifford Cox, một chuyên gia mã hóa người Anh đã phát triển riêng một biến thể của RSA. Tuy nhiên, Chính phủ Anh xem đây là vấn đề mật và đã không công bố. Khi Rivest, Shamir và Adleman công bố RSA trong ấn phẩm Scientific American tháng 9/1977, Cơ quan an ninh quốc gia Hoa Kỳ (NSA) không đồng ý về việc phổ biến rộng rãi RSA và ra lệnh cấm, tuy nhiên lệnh cấm này không có cơ sở pháp lý.

Thuật toán RSA được MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm [1983](http://vi.wikipedia.org/wiki/1983) (Số đăng ký 4,405,829). Bằng sáng chế này hết hạn vào ngày [21 tháng 9](http://vi.wikipedia.org/wiki/21_th%C3%A1ng_9) năm [2000](http://vi.wikipedia.org/wiki/2000). Tuy nhiên, do thuật toán đã được công bố trước khi có đăng ký bảo hộ nên sự bảo hộ hầu như không có giá trị bên ngoài Hoa Kỳ. Ngoài ra, nếu như công trình của Clifford Cocks đã được công bố trước đó thì bằng sáng chế RSA đã không thể được đăng ký.

Năm 1978, các tác giả đã công bố thuật toán trên Tạp chí của Hiệp hội Kỹ thuật Tính toán Hoa Kỳ (Communications of the Association for Computing Machinery – ACM). Hiện nay, có thể tham khảo đặc tả của RSA trên trang thông tin của Tập đoàn EMC.

# KẾT QUẢ NGHIÊN CỨU

## Nghiên cứu, tìm hiểu về mô hình mạng an toàn

### Các thành phần chính của mô hình mạng an toàn

### Các công nghệ hỗ trợ

## Các mô hình mạng an toàn sử dụng trong doanh nghiệp

## Nghiên cứu mô hình mạng an toàn cho công ty

### Cấu trúc cơ bản

### Các thành phần chính

### Cách thức hoạt động

### Ứng dụng

## Thực nghiệm mô hình mạng an toàn cho công ty

### Giới thiệu công cụ hỗ trợ mô phỏng: packet tracer

### Mục tiêu của hệ thống thực nghiệm

### Thiết kế kịch bản chương trình

### Giải pháp bảo mật trong hệ thống thực nghiệm

### Mô phỏng, triển khai thực nghiệm

# KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM

## Kiến thức kỹ năng đã học được trong quá trình thực hiện đề tài.

## Bài học kinh nghiệm

## Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn

# KẾT LUẬN

Chữ ký số RSA là một trong những giải pháp bảo mật quan trọng giúp đảm bảo tính toàn vẹn và xác thực của dữ liệu trong môi trường mạng. Qua đề tài **“Chữ Ký Số RSA và Ứng Dụng trong Xác Thực Tính Toàn Vẹn của Dữ Liệu”**, chúng em đã nghiên cứu chi tiết về cơ chế hoạt động của thuật toán RSA, từ cách tạo khóa, mã hóa, giải mã, cho đến ứng dụng thực tế trong chữ ký số.

Kết quả nghiên cứu không chỉ làm rõ lý thuyết về chữ ký số và thuật toán RSA mà còn minh họa cụ thể cách ứng dụng chúng để xác thực tính toàn vẹn của dữ liệu. Thông qua các bước thực nghiệm, chúng em đã thiết kế và triển khai thành công một chương trình sử dụng chữ ký số RSA, đồng thời kiểm chứng được khả năng bảo vệ dữ liệu khỏi các hành vi giả mạo hoặc xâm phạm.

Quá trình thực hiện đề tài đã mang lại cho chúng em nhiều kiến thức và kỹ năng quan trọng, bao gồm:

* Hiểu rõ nguyên lý hoạt động và tầm quan trọng của các hệ thống mã hóa khóa công khai, đặc biệt là thuật toán RSA.
* Áp dụng kiến thức về lập trình và an ninh mạng để triển khai một ứng dụng thực tế, từ đó rút ra các bài học kinh nghiệm về cách bảo vệ dữ liệu trong môi trường mạng.
* Tăng cường khả năng phân tích và giải quyết vấn đề trong lĩnh vực an ninh mạng.

Mặc dù đạt được những kết quả tích cực, đề tài vẫn còn một số hạn chế, chẳng hạn như phạm vi ứng dụng chưa mở rộng sang các hệ thống phức tạp hoặc các bài toán thực tế lớn hơn. Trong tương lai, chúng em hy vọng sẽ tiếp tục phát triển và tối ưu hóa các ứng dụng liên quan đến chữ ký số, từ đó nâng cao hiệu quả trong việc đảm bảo an ninh dữ liệu.

Với sự phát triển không ngừng của công nghệ số, chữ ký số nói chung và RSA nói riêng sẽ tiếp tục đóng vai trò quan trọng trong việc bảo vệ thông tin và dữ liệu. Đề tài này không chỉ giúp chúng em hiểu rõ hơn về một công cụ bảo mật hữu ích mà còn góp phần nhỏ vào việc nâng cao nhận thức về an ninh mạng, đặc biệt trong bối cảnh các mối đe dọa mạng ngày càng gia tăng.

# TÀI LIỆU THAM KHẢO