**ĐẠI HỌC UEH**

**TRƯỜNG CÔNG NGHỆ VÀ THIẾT KẾ**

KHOA CÔNG NGHỆ THÔNG TIN KINH DOANH

BỘ MÔN AN NINH THÔNG TIN



**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**ỨNG DỤNG CHỮ KÝ SỐ TRONG KÊ KHAI NHẬP HỌC**

**GVHD: TS.GVC Nguyễn Quốc Hùng**

Nhóm thực hiện: Nhóm 3

Đoàn Trần Bá Đạt( Nhóm trưởng)

Nguyễn Ngọc Bảo

Lồ Sìn Dậu

Nguyễn Hoàn Thiện

Nguyễn Thị Bích Kiều

**TP. Hồ Chí Minh, 11/2022**

**MỤC LỤC**

[**DANH MỤC HÌNH ẢNH.**](#_heading=h.30j0zll) **5**

[**DANH MỤC BẢNG BIỂU.**](#_heading=h.1fob9te) **6**

[**DANH MỤC TỪ VIẾT TẮT.**](#_heading=h.3znysh7) **7**

[**Từ viết tắt**](#_heading=h.2sul01925m84) **7**

[**Từ đầy đủ**](#_heading=h.w0rqy1zcl5d6) **7**

[**Ý nghĩa**](#_heading=h.l5678a94ztp4) **7**

[**Lời mở đầu.**](#_heading=h.2et92p0) **8**

[**BẢNG PHÂN CÔNG CÁC THÀNH VIÊN**](#_heading=h.tyjcwt) **9**

[**Chương 1: GIỚI THIỆU VỀ AN NINH THÔNG TIN**](#_heading=h.3dy6vkm) **10**

[1.1 Tổng quan khái niệm và mục tiêu ANTT là gì?](#_heading=h.e2xmudetlllt) 10

[1.2.1 Tổng quan về các mối đe dọa](#_heading=h.luvwkmszs3n8) 10

[1.2.2.1 Các tác nhân đe dọa](#_heading=h.rkaclnp84krz) 11

[**Chương 2: CƠ SỞ LÝ THUYẾT LIÊN QUAN ĐẾN CÁC PHƯƠNG PHÁP SỬ DỤNG**](#_heading=h.2s8eyo1) **18**

[2.1 Vấn đề chữ ký số](#_heading=h.ocasqg7j6j2f) 18

[2.1.1 Khái niệm và giới thiệu chữ ký số](#_heading=h.9s2x6mftxo96) 18

[2.1.2 Công nghệ chữ ký số](#_heading=h.oysqeqozqnld) 18

[2.1.2.1 Sơ đồ tạo chữ ký số](#_heading=h.e68xpnft4qef) 18

[2.1.2.2 Sơ đồ thẩm định chữ ký số](#_heading=h.xen3v3uzcw5z) 19

[2.1.3 Phân loại chữ ký số](#_heading=h.tqgfj8lbbyw) 20

[2.1.3.1 Phân loại chữ ký theo đặc trưng kiểm tra chữ ký](#_heading=h.9k5u8syiuyqx) 20

[2.1.3.2 Phân loại chữ ký theo mức an toàn](#_heading=h.sxtvom2x34z8) 20

[2.1.3.3 Phân loại chữ ký theo ứng dụng đặc trưng](#_heading=h.vmv2srup9p0j) 20

[2.2. Các kiểu tấn công chữ ký số](#_heading=h.40q7sf2bwba6) 21

[2.2.1. Tấn công chữ ký RSA](#_heading=h.nwcmzurpomuw) 21

[2.2.1.1 Giới thiệu hệ mật RSA](#_heading=h.uahvgbsrdy5b) 21

[2.2.1.2 Mức độ an toàn của hệ mật RSA](#_heading=h.vbrhvimrda9z) 21

[2.2.1.3 Các dạng tấn công đối với hệ mật RSA](#_heading=h.rkgh4gc0dmsa) 21

[a. Dạng 1: Tìm cách xác định khóa bí mật](#_heading=h.hbhr8mcc3qwi) 21

[a.1. Kẻ tấn công chỉ biết khóa công khai của người đăng ký](#_heading=h.gqivic3bcir9) 21

[a.2. Kẻ tấn công biết được (N):](#_heading=h.94uub7yoj0i5) 21

[a.3 Sử dụng giá trị “modulo n” nhỏ](#_heading=h.4pajpv7k14nz) 22

[a.4. Dùng các tham số (p-1) và (q-1) có các ước nguyên tố nhỏ](#_heading=h.80fdl5w0fubv) 22

[b. Dạng 2: Giả mạo chữ ký ( Không tính trực tiếp khóa bí mật)](#_heading=h.uf2245rwe43b) 22

[b.1. Ký trước, mã hóa sau](#_heading=h.885qxucb1nmb) 22

[b.2. Mã hóa trước, ký sau:](#_heading=h.o56i1l7ncbl) 22

[**Chương 3: ỨNG DỤNG CÁC PHƯƠNG PHÁP VÀO   
BÀI TOÁN CỤ THỂ**](#_heading=h.17dp8vu) **23**

[3.1. Thiết kế chương trình](#_heading=h.66ilairx8a45) 23

[3.1.1. Công cụ và ngôn ngữ lập trình](#_heading=h.fo5p3yp3t2zy) 23

[3.1.2. Ứng dụng chữ ký số trên hệ mật RSA vào bài toán kê khai hồ sơ nhập học](#_heading=h.q6183uqv1wwr) 23

[3.1.2.1. Đặt vấn đề](#_heading=h.500qao5xxbwu) 23

[3.1.2.2. Bài toán hệ mã RSA](#_heading=h.yuc578tq3ozn) 23

[a. Thuật toán sinh tham số và khóa](#_heading=h.drwqz1tve94d) 23

[b. Thuật toán ký](#_heading=h.3xv505nitdng) 24

[c. Thuật toán kiểm tra chữ ký](#_heading=h.xxh8wtbf5igd) 24

[3.1.2.3. Hiệu quả đạt được](#_heading=h.jvu3wg3e96fc) 24

[3.2. Xây dựng chương trình](#_heading=h.86j6jr4jh1uc) 25

[3.2.1. Thiết kế giao diện cho hệ mật RSA](#_heading=h.gaccihna4m44) 25

[3.2.1.1 Wireframe demo hệ mật RSA](#_heading=h.p33k4ll4r93) 25

[a. Form Login:](#_heading=h.64fnhcxcihfy) 25

[b. Form Sign:](#_heading=h.iyfp0eace37) 26

[c. Form Verify:](#_heading=h.lyliwp40x2w3) 27

[3.2.1.2 Giao diện demo hệ mật RSA](#_heading=h.cf85zbvzykaf) 28

[a. Giao diện Login:](#_heading=h.9j3j05mm9ekr) 28

[b. Giao diện Sign:](#_heading=h.quv15lttuect) 28

[c. Giao diện Verify:](#_heading=h.fialzum6dto2) 29

[3.2.1.3 Giao diện hệ mật RSA khi chạy chương trình](#_heading=h.ct39p950908) 29

[a. Student](#_heading=h.ep2ctixcmyfr) 29

[b. Admin](#_heading=h.jd3s2vel4rkt) 30

[3.3. Các hàm, thủ tục chính của chương trình](#_heading=h.jfkqde2qdjns) 30

[3.3.1 Code mã hóa RSA](#_heading=h.rwcq6aws7lee) 30

[3.3.1.1 Tạo khóa](#_heading=h.fpy3o2szfy0l) 30

[3.3.1.2 Mã hóa](#_heading=h.k550iwks9rf4) 31

[3.3.1.3 Giải mã](#_heading=h.d85con5b7rhq) 31

[**Chương 4: ĐÁNH GIÁ KẾT QUẢ**](#_heading=h.qndw47fj2fj6) **32**

[**KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**](#_heading=h.lnxbz9) **33**

[Kết luận](#_heading=h.t1kr9imhgyfd) 33

[Hướng phát triển](#_heading=h.6cd21p730sh2) 33

[**TÀI LIỆU THAM KHẢO**](#_heading=h.35nkun2) **34**

# **DANH MỤC HÌNH ẢNH.**

***Hình 1.1*** *Mô hình CIA 10*

***Hình 1.2.2.2*** *Sơ đồ các tác động đe dọa 12*

***Hình 1.5.1*** *Mô hình mã hóa đối xứng 16*

***Hình 1.5.2*** *Mô hình mã hóa công khai 17*

***Hình 2.1.2.1:*** *Sơ đồ tạo chữ ký số 19*

***Hình 2.1.2.2:*** *Sơ đồ thẩm định chữ ký số 20*

***Hình 3.2.1.1.a:*** *Wireframe demo form login 25*

***Hình 3.2.1.1.b:*** *Wireframe demo form sign 26*

***Hình 3.2.1.1.c:*** *Wireframe demo form verify 27*

***Hình 3.2.1.2.a:*** *Giao diện demo form login 28*

***Hình 3.2.1.2.b:*** *Giao diện demo form sign 28*

***Hình 3.2.1.2.c:*** *Giao diện demo form verify 29*

***Hình 3.2.1.3.a:*** *Giao diện Student 29*

***Hình 3.2.1.3.a:*** *Giao diện Admin 30*

***Hình 3.3.1.a:*** *Code Tạo khóa 30*

***Hình 3.3.1.b:*** *Code Mã hóa 31*

***Hình 3.3.1.c:*** *Code Giải mã 31*

# **DANH MỤC BẢNG BIỂU.**

***Bảng 1.4*** *Bảng liệt kê các biện pháp đảm bảo ANTT 15*

***Bảng 3.1.2.2.a***  *Bảng tạo khóa hệ mã RSA 24*

***Bảng 3.1.2.2.b***  *Bảng mã hóa hệ mã RSA 24*

***Bảng 3.1.2.3.c***  *Bảng giải mã hệ mã RSA 24*

# **DANH MỤC TỪ VIẾT TẮT.**

| **TT** | **Từ viết tắt** | **Từ đầy đủ** | **Ý nghĩa** |
| --- | --- | --- | --- |
| 1 | ANTT | An ninh thông tin | An ninh thông tin |
| 2 | CIA | Central Intelligence Agency | Cơ quan tình báo Hoa Kỳ |
| 3 | IDS | Intrusion Detection System | Hệ thống phát hiện xâm nhập |
| 4 | IPS | Intrusion Prevention System | Hệ thống phòng chống xâm nhập |
| 5 | VPN | Virtual Private Network | Mạng riêng ảo |
| 6 | DoS | Denial of Service | Từ chối dịch vụ |
| 7 | DES | Data Encryption Standard | Tiêu chuẩn mã hóa dữ liệu |
| 8 | AES | Advanced Encryption Standard | Tiêu chuẩn mã hóa nâng cao |
| 9 | DSA | Digital Signature Algorithm | Giải thuật ký số |
| 10 | RSA | Rivest-Shamir Adleman | Ron Rivest, Adi Shamir và Leonard Adleman |
| 11 | SSH | Secure Socket Shell | Giao thức mạng giúp kết nối mạng một cách bảo mật |
| 12 | PGP | Pretty Good Privacy | Giao thức mã hóa dữ liệu |
| 13 | S/MIME | Secure/Multipurpose Internet Mail Extensions | Giao thức bảo mật email |
| 14 | SSL/TLS | Secure Sockets Layer/  Transport Layer Security | Lớp socket bảo mật |
| 15 | GPG | GNU Privacy Guard Public Keyring | Khóa giải mã tập tin GNU Privacy Guard (GnuPG) |
| 16 | ZRTP | Ziemmermann | Giao thức thỏa thuận khóa mật mã |
| 17 | CERT | Certificate Authority | Cơ quan cấp chứng chỉ kỹ thuật số |

# **Lời mở đầu.**

Để hoàn thành đồ án báo cáo lần này, tôi xin tỏ lòng biết ơn sâu sắc đến giảng viên hướng dẫn TS. Nguyễn Quốc Hùng, người đã định hướng và hướng dẫn nhóm tôi trong suốt quá trình lên sườn bài đến quá trình làm nội dung đồ án.

Xin trân thành cảm ơn đến quý thầy, cô khoa Công nghệ thông tin kinh doanh trường Công nghệ và thiết kế - Đại học UEH đã tận tình truyền đạt kiến thức trong thời gian học tập vừa qua. Với vốn kiến thức được thu thập và tiếp thu trong quá trình học tập không chỉ là nền tảng trong quá trình làm đồ án mà còn là hành trang quý báu để các chúng tôi ứng dụng và phát huy trong học tập và công việc sắp tới.

Chúng tôi cũng thầm biết ơn đến các thành viên trong nhóm đã nhiệt tình hỗ trợ lẫn nhau trong quá trình làm đồ án. Lời cuối cùng, nhóm tôi xin kính chúc quý thầy, cô giáo dồi dào sức khỏe và thành công trong nhiệm vụ cao quý!

# **BẢNG PHÂN CÔNG CÁC THÀNH VIÊN**

| **TT** | **Họ và tên** | **Công việc phụ trách** | **Mức độ hoàn thành** |
| --- | --- | --- | --- |
|  | Đoàn Trần Bá Đạt *(Trưởng nhóm)* | Ký văn bản, làm slide thuyết trình, chương 1 báo cáo | 100% |
|  | Lồ Sìn Dậu | Thiết kế giao diện, quay video demo, đổ dữ liệu vào danh sách sinh viên, chương 4 báo cáo | 100% |
|  | Nguyễn Ngọc Bảo | Thiết kế cơ sở dữ liệu, đóng gói chương trình thành file setup, lưu dữ liệu sinh viên, chương 3 báo cáo | 100% |
| 4. | Nguyễn Hoàn Thiện | Xác thực văn bản, chương cuối báo cáo | 100% |
| 5 | Nguyễn Thị Bích Kiều | Tạo khóa bí mật, khóa công khai, chương 2 báo cáo, vẽ wireframe chương trình | 100% |

# Chương 1: GIỚI THIỆU VỀ AN NINH THÔNG TIN

## Tổng quan khái niệm và mục tiêu ANTT là gì?

An ninh thông tin (Information Security hoặc "InfoSec") là một thuật ngữ khác của "bảo mật dữ liệu". An ninh thông tin là một lĩnh vực rộng lớn bao gồm nhiều lĩnh vực như: bảo mật vật lý, bảo mật điểm cuối, mã hóa dữ liệu (“Data Encryption”) và bảo mật mạng. Trọng tâm là tính bảo mật, tính toàn vẹn và tính sẵn sàng của dữ liệu (thường được gọi là "CIA"). Mọi yếu tố của chương trình an toàn thông tin phải được thiết kế để thực hiện một hoặc nhiều nguyên tắc này.

***Hình 1.1*** *Mô hình CIA*

*- Tính bí mật (Confidentiality)*: Các biện pháp bảo mật được thiết kế để ngăn chặn việc tiết lộ thông tin trái phép. Mục đích của các nguyên tắc bảo mật là giữ bí mật thông tin cá nhân và đảm bảo rằng thông tin cá nhân chỉ hiển thị và có thể truy cập được đối với những cá nhân sở hữu hoặc cá nhân, tổ chức được cấp quyền truy cập.

- *Tính toàn vẹn (Integrity):* Tính nhất quán bao gồm bảo vệ chống lại những thay đổi trái phép (bổ sung, xóa, thay đổi, v.v.) đối với dữ liệu. Nguyên tắc toàn vẹn đảm bảo rằng dữ liệu là chính xác và đáng tin cậy và không bị sửa đổi sai cách, dù vô tình hay ác ý.

- *Tính sẵn sàng (Availability)*: Tính khả dụng là sự bảo vệ khả năng của hệ thống để làm cho hệ thống phần mềm và dữ liệu luôn sẵn sàng khi người dùng cần (hoặc tại một thời điểm xác định). Mục đích của tính sẵn có là cung cấp cơ sở hạ tầng công nghệ (“High availability solutions”) , các ứng dụng và dữ liệu khi chúng cần thiết cho một quy trình tổ chức hoặc cho khách hàng của tổ chức.

* 1. **Các mối đe dọa đối với hệ thống**

### Tổng quan về các mối đe dọa

Các hệ thống thông tin liên tục đối mặt với các mối đe dọa khác nhau gây ra các loại thiệt hại khác nhau, dẫn đến thiệt hại kinh tế đáng kể. Thiệt hại đối với an ninh thông tin có thể từ tổn thất nhỏ đến phá hủy hoàn toàn hệ thống thông tin. Các tác động, hậu quả của mối đe dọa rất khác nhau. Song, một số ảnh hưởng chính là đến bảo mật và tính toàn vẹn của dữ liệu, trong khi một số ảnh hưởng đến tính khả dụng của hệ thống.

Lỗ hổng bảo mật chủ yếu là một lỗ hổng trong hệ thống có thể bị kẻ tấn công khai thác để gây tác động bất lợi. Nếu một hệ thống dễ bị đe dọa, thì các mối đe dọa thường có thể thể hiện thông qua một tác nhân đe dọa sử dụng các kỹ thuật cụ thể xâm nhập trái phép để gây ra các tác động không mong muốn đối với hệ thống. Nguy cơ thiệt hại tài chính đáng kể cho tổ chức.

* + 1. **Nguyên nhân các mối đe dọa**

Có nhiều lý do dẫn đến các mối đe dọa thường thấy: Cấp quyền người dùng hoặc cho phép truy cập trái phép vào hệ thống. Bản thân hệ điều hành cũng có thể có các lỗ hổng, chẳng hạn như Windows XP, Windows NT, UNIX, hệ điều hành của thiết bị bộ định tuyến, modem hoặc các ứng dụng thường được sử dụng như bộ xử lý văn bản và hệ thống cũng như hệ thống cơ sở dữ liệu. Do bản thân hệ thống có vấn đề và kiến thức chuyên môn của người quản lý còn chưa tốt, dịch vụ cung cấp chưa được hiểu rõ, ý thức bảo mật của người dùng chưa cao. Yếu tố con người cũng được coi là lỗ hổng bảo mật.

- *Các mối đe dọa nội bộ:* Xảy ra khi cá nhân có quyền truy cập vào mạng thông qua tài khoản trên máy chủ hoặc quyền truy cập vật lý. Mối đe dọa hình thành bên trong nội bộ tổ chức do kết quả của hành vi của nhân sự hoặc sự thất bại trong quy trình tổ chức

- *Các mối đe dọa bên ngoài:* Phát sinh từ một hoặc nhiều cá nhân làm việc bên ngoài tổ chức và không có quyền truy cập vào hệ thống máy tính và mạng nội bộ của tổ chức của bạn. Mối đe dọa bên ngoài cơ bản nhất đối với hệ thống máy tính và dữ liệu thường trú là thiên tai: bão, hỏa hoạn, lũ lụt và động đất. Các cuộc tấn công bên ngoài phổ biến khác thường thông qua hệ thống mạng được kết nối (có dây và không dây), xâm nhập vật lý hoặc mạng đối tác.

Mục tiêu tấn công cụ thể được xác định, gây ra kết quả không mong muốn hoặc mong muốn. Các mối đe dọa không mong muốn gồm các cuộc tấn công bên trong hoặc bên ngoài do người thuộc tổ chức hoặc bên ngoài tổ chức gây ra để làm tổn hại và phá vỡ tổ chức như: virus, sâu, ngựa Trojan. Các cuộc tấn công mong muốn được cố ý sắp đặt xảy ra do các chính sách và kiểm soát bảo mật kém cho phép các lỗ hổng và lỗi xảy ra, có thể bị gây ra bởi những nhân viên thiếu hiểu biết hoặc nhân viên có chuyên môn cố ý với mục đích không làm tổn hại đến hệ thống.

#### Các tác nhân đe dọa

*Con người:* Thường là các mối đe dọa chủ yếu gây ra bởi hành động của con người như người trong tổ chức, tin tặc mang mã gây hại hoặc rủi ro bên trong hệ thống.

*Môi trường:*Mối đe dọa không từ chính môi trường sống, thường từ các mối đe dọa thiên tai như: động đất, lũ lụt, hỏa hoạn, sét,.. trong đó gây thiệt hại nghiêm trọng nhất vẫn là: lũ lụt, sóng thần, hỏa hoạn . Ngoài ra, một số mối đe dọa khác có thể kể đến như: chiến tranh và các cuộc tấn công khủng bố,..

*Công nghệ:* gây ra bởi tác động lý học và hóa học trên vật liệu. Tác động lý học lên: tòa nhà hoặc bất kỳ khu vực đã được chỉ định trước như: trộm cắp hoặc làm hư hỏng phần cứng và phần mềm. Bên cạnh đó, quá trình hóa học trực tiếp lên công nghệ phần cứng và phần mềm, điển hình là sử dụng nguồn điện làm hệ thống gián điệp.

* + - 1. *Các tác động đe dọa*

***Hình 1.2.2.2*** *Sơ đồ các tác động đe dọa*

*Phá hủy thông tin*: Làm gián đoạn hoạt động của hệ thống bằng cách cố ý phá hủy một thành phần nào đó thuộc hệ thống.

*Giả mạo thông tin*: Thêm, sửa, xóa làm thay đổi bộ nhớ hệ thống như ổ đĩa, thành phần lưu trữ dữ liệu đích, ví dụ: cấy Trojan làm tăng tệp trên đĩa cứng, virus xâm nhập tấn công tệp sẽ thay đổi tệp đích. Giả mạo thông tin gây ra do: giả mạo, mã độc, làm sai lệch,...

*Tiết lộ thông tin*:Thông tin bị phổ biến cho các cá nhân không có quyền truy cập hoặc sử dụng thông tin đó. Hành động này làm tiết lộ trái phép thông tin: Tiếp xúc, đánh chặn, suy luận, xâm nhập.

*Nâng cao đặc quyền*: Sử dụng công cụ hoặc lợi dụng điểm yếu trong hệ thống; chiếm dụng và được phép truy cập vào hệ thống đích. Điển hình, có thể kể đến như: đoán mật khẩu, kết quả là quyền của người bị chiếm dụng bị đe dọa.

*Trộm cắp dịch vụ*: Việc sử dụng, chiếm dụng trái phép mà không có sự đồng ý của quản trị, hành vi này tuy không làm giảm chất lượng dịch vụ của người dùng khác, tuy nhiên để lại một số hậu quả như: dịch vụ, chức năng, dữ liệu, phần mềm bị đánh cắp, sử dụng sai phần cứng, sai dữ liệu

*Sử dụng bất hợp pháp*: Lợi dụng chức năng thông thường của một hệ thống để thực hiện hành vi tấn công có chủ đích, sai lệch với mục đích chính của chức năng đó. Ví dụ: lợi dùng kết nối mạng để tấn công một hệ thống mạng khác, sử dụng các lỗ hổng để xâm nhập thực hiện với mục đích tấn công

* 1. **Các lỗ hổng trên hệ thống mạng**
     1. **Tổng quan về lỗ hổng mạng**

Ngày nay, các tổ chức trên toàn cầu tiến hành hoạt động kinh doanh trong một môi trường kết nối và thông tin phong phú. Cơ sở hạ tầng mạng toàn cầu như Internet đã dẫn đến việc liên lạc kinh doanh tức thời, trong khi tính khả dụng và khả năng chi trả của bộ nhớ lưu trữ cho phép sử dụng cơ sở dữ liệu khối lượng lớn. Những cơ sở hạ tầng công nghệ này được biết đến không chỉ mang lại cơ hội kinh doanh mới mà còn cả những lỗ hổng mới và phức tạp. Những lỗ hổng như vậy bao gồm một phạm vi rộng từ các chủ đề kỹ thuật đến quản lý. Việc bảo vệ việc khai thác các lỗ hổng này được phức tạp hóa bởi sự gia tăng đáng báo động của tỷ lệ các hoạt động tội phạm mạng. Việc quản lý sự kết hợp của các lỗ hổng phức tạp và các hoạt động tội phạm mạng đòi hỏi các phương pháp quản lý sáng tạo.

* + 1. **Đánh giá và xử lý lỗ hổng**

- *Lỗ hổng loại A*: Lỗ hổng khiến hệ thống dễ bị người ngoài truy cập trái phép.

- *Lỗ hổng loại B*: Lỗ hổng này cho phép người dùng có thêm quyền truy cập hệ thống mà không cần xác minh, dẫn đến lộ thông tin..

- *Lỗ hổng loại C*: Cho phép tấn công DoS (Từ chối dịch vụ), ảnh hưởng đến chất lượng dịch vụ, thời gian ngừng hoạt động, gián đoạn hệ thống, nhưng không làm hỏng dữ liệu hoặc giành quyền truy cập vào hệ thống.

* + 1. **Một số biện pháp đảm bảo ANTT trên hệ thống mạng**

- *Kiểm soát truy cập Bolster***:** Tăng cường các biện pháp kiểm soát truy cập bằng cách sử dụng hệ thống mật khẩu mạnh. Nên có sự kết hợp giữa chữ hoa và chữ thường, số và các ký tự đặc biệt. Ngoài ra, hãy luôn đặt lại tất cả các mật khẩu mặc định.

- *Cập nhật tất cả phần mềm*: Khi một phiên bản phần mềm mới được phát hành, phiên bản đó thường bao gồm các bản sửa lỗi cho các lỗ hổng bảo mật.

- *Chuẩn hóa phần mềm*: Đảm bảo rằng người dùng không thể cài đặt phần mềm vào hệ thống khi chưa được phê duyệt. Không biết phần mềm nào trên mạng của bạn là một lỗ hổng bảo mật rất lớn. Đảm bảo rằng tất cả các máy tính đều sử dụng như nhau: Hệ điều hành, Trình duyệt, Media Player,...

- *Sử dụng các biện pháp bảo vệ mạng*:

+ Cài đặt tường lửa

+ Đảm bảo kiểm soát quyền truy cập thích hợp

+ Sử dụng IDS / IPS để theo dõi lũ gói tiềm ẩn

+ Sử dụng phân đoạn mạng

+ Sử dụng mạng riêng ảo (VPN)

+ Tiến hành bảo trì thích hợp

- *Đào tạo nhân viên*: Đôi khi các mối liên hệ bên ngoài thành công vì một mối đe dọa từ bên trong. Liên kết yếu nhất trong việc bảo vệ dữ liệu có thể là nhân viên. Cần đảm bảo của bạn hiểu về an ninh mạng, các bạn cần xác định liên hệ với ai để tránh vi phạm an ninh.

* 1. **Biện pháp đảm bảo ANTT**

| **CÁC BIỆN PHÁP PHÒNG NGỪA CHUNG** | |
| --- | --- |
| **Chính phủ** | * Tăng cường công tác đảm bảo thực hiện Luật an ninh mang trong tình hình mới. * Phối hợp với các cơ quan chức năng thực thi pháp luật và các CERT. * Áp dụng các phương pháp điều tra, kỹ thuật CNTT kết hợp với thực tế xã hội để tăng cường an ninh mạng, đảm bảo sự chặt chẽ trong xử lý vi phạm Luật an ninh mạng. |
| **Các tổ chức và thể chế** | * Cải thiện bảo mật CNTT bằng các phương pháp mới như vòng kiểm soát chất lượng. * Xác định các tài nguyên, mối đe dọa và lỗ hổng bảo mật của hệ thống ICT để có các khoản đầu tư thích hợp liên quan đến việc bảo vệ không gian mạng. |
| **Dịch vụ Internet**  **Nhà cung cấp dịch vụ lưu trữ** | * Lưu giữ dữ liệu về các hoạt động trực tuyến của khách hàng trong một khoảng thời gian cụ thể. * Thông qua việc thực hiện pháp luật tương ứng khi áp dụng bảo vệ dữ liệu bắt buộc ở tất cả các quốc gia. * Bảo vệ ISP khỏi trách nhiệm pháp lý của bên trung gian, có thể cung cấp sáng kiến thích hợp cho từng hành động. |
| **Cơ quan thực thi pháp luật** | * Đánh giá rủi ro bảo mật và các biện pháp khắc phục tương ứng. * Đánh giá các mối đe dọa tiềm ẩn, tìm kiếm đề phòng cho các hành vi giảm thiểu. * Sử dụng các nguồn nhân lực chuyên môn để nâng cao hiệu quả công việc. |
| **Academia** | * Tư vấn và hỗ trợ pháp lý hiệu quả cho các nhà lập pháp trong nước và quốc tế về các chủ đề như hình sự hóa, bảo vệ hiến pháp và luật pháp,... * Ứng dụng CNTT trong nghiên cứu tạo ra các tiêu chuẩn và giải pháp kỹ thuật dành cho các tổ chức công tư, cơ quan hành pháp, và người dùng phổ thông. * Cung cấp, hỗ trợ kỹ thuật cho các cơ quan hành pháp quốc gia, quốc tế, tư pháp hình sự, các tập đoàn doanh nghiệp kinh doanh và người dùng cá nhân. |
| **Người dùng** | * Sử dụng tất cả các bản hệ thống, bản sửa lỗi bảo mật và các bản cập nhật đã xuất bản. * Cài đặt phần mềm chống virus, tìm kiếm, kiểm tra phần mềm gián điệp, tường lửa với hiệu suất rà soát thường xuyên trên hệ thống. * Sao lưu, mã hóa thông tin cá nhân. |

***Bảng 1.4*** *Bảng liệt kê các biện pháp đảm bảo ANTT*

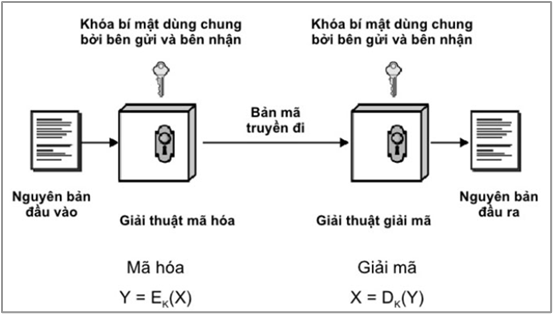
* 1. **Vấn đề mã hóa dữ liệu**

Do việc sử dụng rộng rãi và chia sẻ dữ liệu trên Internet, cần phải bảo vệ dữ liệu khỏi bị hack, nhiễu và can thiệp. Mật mã học đã thu hút nhiều nhà nghiên cứu. Nó được sử dụng để bảo vệ thông tin trong quá trình truyền giữa những người dùng. Nó làm thay đổi nội dung của dữ liệu được truyền sang dạng không thể đọc được, một khi người nhận nhận được, nó sẽ được chuyển đổi trở lại dạng ban đầu. Mã hóa kết quả dữ liệu sang một định dạng không thể đọc được gọi là dữ liệu mật mã. Đảo ngược mật mã này dữ liệu sang dữ liệu gốc gọi là quá trình giải mã.

Cryptography có một tập hợp các mục tiêu bảo mật để đảm bảo tính riêng tư của dữ liệu. Các mục tiêu này là bảo mật, xác thực, toàn vẹn dữ liệu, không từ chối và kiểm soát truy cập. Mật mã được sử dụng rộng rãi để bảo mật dữ liệu trong điện toán đám mây. Nó được phân loại thành mã hóa khóa Đối xứng (khóa riêng) và Không đối xứng (khóa công khai). Ví dụ về thuật toán đối xứng là DES, 3DES, AES, Blowfish bên cạnh đó DSA (Thuật toán chữ ký số), Đường cong Elliptic, Diffie-Hellman (trao đổi khóa) và RSA là những ví dụ về thuật toán Không đối xứng. Mật mã khóa công khai hoặc khóa không đối xứng được sử dụng rộng rãi trong việc thực hiện bảo mật dữ liệu trên hệ thống thông tin và truyền thông.

Trong Khóa đối xứng, mã hóa chỉ sử dụng một khóa để mã hóa và giải mã dữ liệu giữa người gửi và người nhận, được gọi là khóa bí mật. Mặt khác, mã hóa khóa không đối xứng sử dụng khóa công khai để mã hóa và khóa khác để giải mã nó còn được gọi là khóa riêng. Tuy nhiên, mã hóa khóa công khai không hiệu quả lắm đối với các thiết bị di động nhỏ, do đó nó dựa trên các hàm toán học và cần nhiều tính toán hơn. Các thuật toán mã hóa đối xứng nhanh hơn gần 1000 lần so với các thuật toán không đối xứng vì chúng yêu cầu ít năng lực xử lý hơn cho các tính toán. Có nhiều tiêu chuẩn giao thức được sử dụng trong thuật toán không đối xứng như SSH, PGP, S / MIME, SSL / TLS và GPG, ZRTP, Internet Key Exchange và SILC.

* + 1. **Mã hóa khóa đối xứng**

***Hình 1.5.1*** *Mô hình mã hóa đối xứng*

Với mật mã khóa bí mật, cả hai bên liên lạc, A và B, sử dụng cùng một khóa để mã hóa và giải mã các thông điệp. Trước khi bất kỳ dữ liệu mã hóa nào có thể được gửi qua mạng, cả A và B đều phải có khóa và phải đồng ý về thuật toán mật mã mà họ sẽ sử dụng để mã hóa và giải mã.

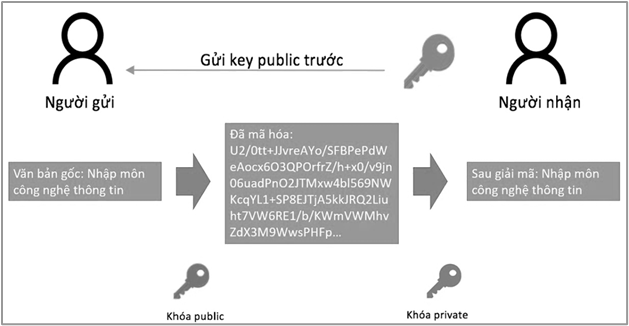
Một trong những vấn đề lớn đối với mật mã khóa bí mật là vấn đề hậu cần về cách lấy khóa từ bên này sang bên kia mà không cho phép kẻ tấn công truy cập. Nếu A và B đang bảo mật dữ liệu của họ bằng mật mã khóa bí mật và nếu C có quyền truy cập vào khóa của họ, thì C có thể hiểu bất kỳ tin nhắn bí mật nào mà anh ta chặn được giữa A và B. C không chỉ có thể giải mã tin nhắn của A và B mà còn có thể giả vờ rằng mình là A và gửi dữ liệu đã mã hóa cho B. B sẽ không biết rằng tin nhắn đến từ C, không phải A.

Sau khi vấn đề phân phối khóa bí mật được giải quyết, mật mã khóa bí mật có thể là một công cụ có giá trị. Các thuật toán cung cấp khả năng bảo mật tuyệt vời và mã hóa dữ liệu tương đối nhanh chóng. Phần lớn dữ liệu nhạy cảm được gửi trong phiên TLS được gửi bằng mật mã khóa bí mật.

Mật mã khóa bí mật còn được gọi là mật mã đối xứng vì cùng một khóa được sử dụng để vừa mã hóa vừa giải mã dữ liệu. Các thuật toán mật mã khóa bí mật nổi tiếng bao gồm Tiêu chuẩn mã hóa nâng cao (AES), Tiêu chuẩn mã hóa dữ liệu ba (3DES) và Rivest Cipher 4 (RC4).

* + 1. **Mã hóa khóa công khai**

Mật mã khóa công khai giải quyết vấn đề hậu cần của việc phân phối khóa bằng cách sử dụng cả khóa công khai và khóa cá nhân. Khóa công khai có thể được gửi công khai thông qua mạng trong khi khóa cá nhân được giữ kín bởi một trong các bên giao tiếp. Khóa công khai và khóa riêng là sự đảo ngược mật mã của nhau; khóa nào mã hóa thì khóa còn lại sẽ giải mã.

***Hình 1.5.2*** *Mô hình mã hóa công khai*

Giả sử rằng B muốn gửi một thông điệp bí mật cho A bằng mật mã khóa công khai. A có cả khóa công khai và khóa riêng tư, vì vậy cô ấy giữ khóa cá nhân của mình ở một nơi an toàn và gửi khóa công khai của mình cho B. B mã hóa thông điệp bí mật cho A bằng khóa công khai của A. A sau đó có thể giải mã tin nhắn bằng khóa riêng của mình.

Nếu A mã hóa một tin nhắn bằng khóa riêng của cô ấy và gửi tin nhắn đã mã hóa cho B, thì B có thể xác định rằng dữ liệu anh ta nhận được đến từ A; nếu B có thể giải mã dữ liệu bằng khóa công khai của A, thì tin nhắn đó phải được A sử dụng cùng với cô ấy. Mã hóa khóa riêng, chỉ A mới có thể sở hữu khóa riêng của A. Vấn đề là bất kỳ ai khác có thể đọc tin nhắn. Vì khóa công khai của A là khóa công khai. Mặc dù sơ đồ này không cho phép giao tiếp dữ liệu an toàn, nhưng nó cung cấp cơ sở cho chữ ký điện tử. Chữ ký số là một trong những thành phần của chứng chỉ khóa công khai và được sử dụng để xác thực máy khách hoặc máy chủ trong TLS. Xem chứng chỉ khóa công khai và chữ ký số. Mật mã khóa công khai còn được gọi là mật mã không đối xứng vì các khóa khác nhau được sử dụng để mã hóa và giải mã dữ liệu.

Thuật toán mật mã khóa công khai Mật mã nổi tiếng thường được sử dụng trong TLS là thuật toán Rivest Shamir Adleman (RSA). Một thuật toán khóa công khai khác được sử dụng với TLS được thiết kế đặc biệt để trao đổi khóa bí mật là thuật toán Diffie-Hellman (DH). Mật mã khóa công khai yêu cầu tính toán nhiều, làm cho nó rất chậm. Do đó, nó thường chỉ được sử dụng để mã hóa các phần dữ liệu nhỏ, chẳng hạn như khóa bí mật, thay vì cho phần lớn các giao tiếp dữ liệu được mã hóa.

# **Chương 2: CƠ SỞ LÝ THUYẾT LIÊN QUAN ĐẾN CÁC PHƯƠNG PHÁP SỬ DỤNG**

## 2.1 Vấn đề chữ ký số

### 2.1.1 Khái niệm và giới thiệu chữ ký số

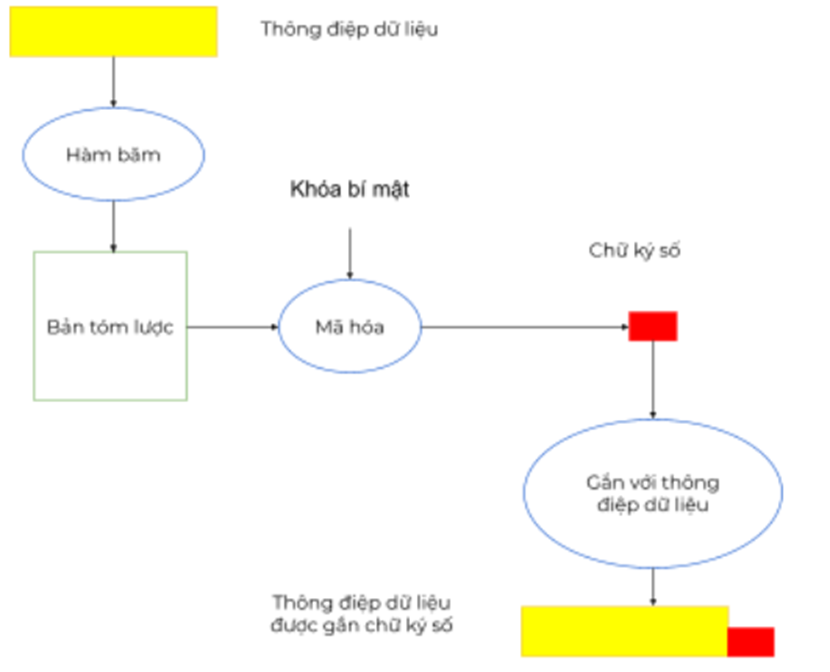
Chữ ký số *(“Nguyễn, Văn Liệu. Tìm hiểu chữ ký số và ứng dụng của nó. Diss. Đại học Quốc gia Hà Nội, 2009.”)* là một dạng chữ ký điện tử. Nó được dùng như một chữ ký thay cho các con dấu của tổ chức, cá nhân. Nó được tạo ra bằng cách mã hóa một thông điệp dữ liệu với hệ thống mật mã bất đối xứng. Chữ ký số có tính bảo mật cao nên sẽ giải quyết được các vấn đề mạo danh đánh cắp thông tin trên không gian mạng.

Chữ ký số cung cấp cho ta bằng chứng về nguồn gốc, danh tính và trạng thái của tài liệu điện tử, thông điệp dữ liệu kỹ thuật số, giao dịch. Chữ ký số cũng giúp cho người ký xác nhận các giao dịch, thông tin, báo cáo,...

### 2.1.2 Công nghệ chữ ký số

#### 2.1.2.1 Sơ đồ tạo chữ ký số

Xem xét dung lượng của thông điệp dữ liệu. Đối với thông điệp dữ liệu có dung lượng lớn, chúng ta sẽ sử dụng hàm băm để băm dữ liệu để thu được một bản tóm lược có dung lượng nhỏ gọn hơn, phù hợp hơn, thuận tiện hơn cho quá trình ký số. Bản tóm lược là một đoạn bit đảm bảo tính một chiều và duy nhất. Bản tóm lược được mã hóa bởi khóa bí mật của người gửi, và được gắn vào sau thông điệp dữ liệu, sau đó gửi đi ( Bản tóm lược được mã hóa chính là chữ ký.



***Hình 2.1.2.1:*** *Sơ đồ tạo chữ ký số*

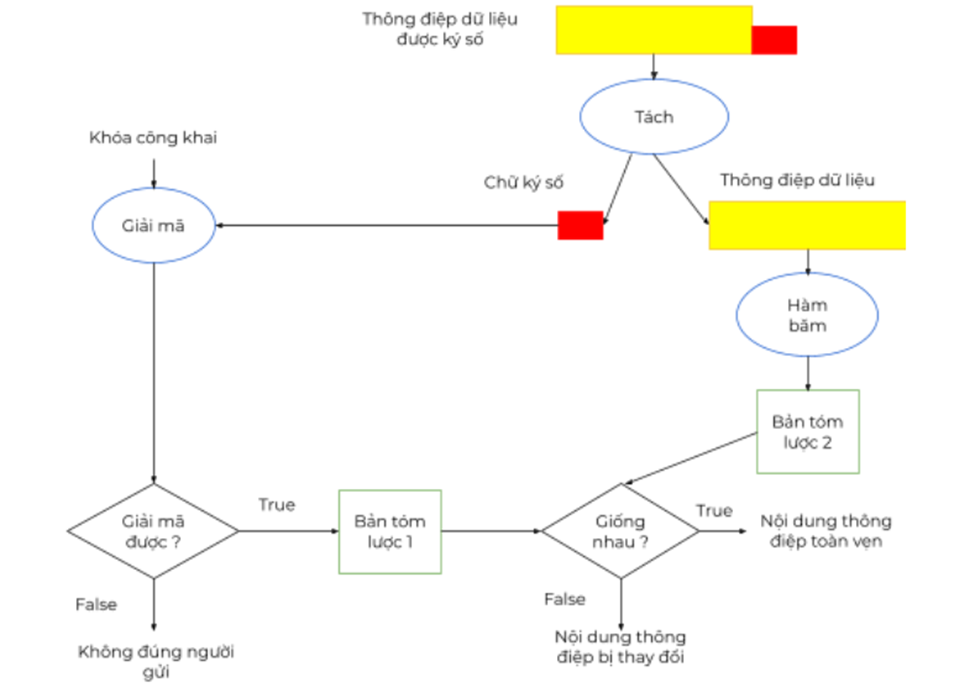
#### 2.1.2.2 Sơ đồ thẩm định chữ ký số

Sau khi nhận được bản tin. Chúng ta sẽ tách ra làm 2 phần là Chữ ký số và thông điệp dữ liệu.

Dùng khóa công khai để giải mã chữ ký số. Nếu giải mã không thành công thì có thể do không đúng người gửi hoặc có vấn đề gian lận. Nếu giải mã thành công, chúng ta sẽ thu được bản tóm lược.

Dùng hàm băm để băm thông điệp dữ liệu, thu được Bản tóm lược 2.

Nếu 2 bản tóm lược ta thu được trong quá trình giải mã giống nhau thì thông điệp được bảo toàn toàn vẹn và đúng người gửi. Ngược lại nếu có khác nhau nội dung đã bị thay đổi trong quá trình gửi đi, tính xác thực và toàn vẹn không được đảm bảo.



***Hình 2.1.2.2:*** *Sơ đồ thẩm định chữ ký số*

### 2.1.3 Phân loại chữ ký số

#### 2.1.3.1 Phân loại chữ ký theo đặc trưng kiểm tra chữ ký

* Chữ ký khôi phục thông điệp: Người dùng chỉ cần gửi chữ ký. Người nhận có thể khôi phục lại thông điệp dựa trên chữ ký này
* Chữ ký kèm thông điệp: Người dùng gửi thông điệp đã được ký chữ ký số. Người nhận sẽ không có được thông điệp gốc.

#### 2.1.3.2 Phân loại chữ ký theo mức an toàn

* Chữ ký không thể phủ nhận: Là bằng chứng chống chối bỏ trách nhiệm trên nội dung đã ký. Để tránh việc sử dụng nhiều lần chữ ký, tốt nhất người gửi nên trực tiếp tham gia kiểm tra chữ ký.
* Chữ ký một lần: Là chỉ ký chỉ dùng 1 lần trên 1 tài liệu.

#### 2.1.3.3 Phân loại chữ ký theo ứng dụng đặc trưng

* Chữ ký mù (Blind Signature): nội dung của một thông điệp được ngụy trang (làm mờ) trước khi nó được ký
* Chữ ký “nhóm” (Group Signature): cho phép một thành viên của nhóm ký một tin nhắn ẩn danh thay mặt cho nhóm
* Chữ ký “bội” (Multi Signature): cho phép một nhóm người dùng ký một tài liệu duy nhất
* Chữ ký “mù nhóm” (Blind Group Signature): tương tự như chữ ký nhóm và được ngụy trang (làm mờ) trước khi nó được ký
* Chữ ký “mù bội” (Blind Multi Signature): tương tự như chữ ký bội và được ngụy trang (làm mờ) trước khi nó được ký.

## 2.2. Các kiểu tấn công chữ ký số

### 2.2.1. Tấn công chữ ký RSA

#### 2.2.1.1 Giới thiệu hệ mật RSA

RSA (Rivest-Shamir Adleman) được phát triển năm 1977 và công bố vào năm 1978. RSA là một hệ mật mã khối, trong đó bản gốc và bản mã là số nguyên thuộc đoạn (0, n − 1) với n < 21024 .Là thuật toán đầu tiên thích hợp việc tạo ra chữ ký số và mã hóa. Việc khám phá ra mật mã RSA được xếp hạng trong số những bước đột phá quan trọng nhất trong mật mã. RSA chứa hai khóa: Khóa công khai và khóa bí mật. Khóa công khai được dùng để mã hóa nên bất kỳ ai cũng có thể mã hóa được thông điệp dữ liệu gửi đi nhưng chỉ có người có khóa bí mật mới giải mã được.

#### 2.2.1.2 Mức độ an toàn của hệ mật RSA

Độ an toàn của hệ mật RSA dựa trên 2 bài toán: bài toán phân tích ra thừa số nguyên tố các số nguyên lớn và bài toán RSA. Bài toán RSA là bài toán tính căn bậc e môđun n (với n là hợp số): tìm số m sao cho , trong đó (e, n) chính là khóa công khai và c là bản mã. Hiện tại nó vẫn được coi là bài toán khó, do chưa có thuật toán thích hợp cho nó và cũng chưa có một công bố nào khẳng định hệ mật RSA bị phá vỡ trong các ứng dụng thực tế bằng việc giải bài toán này khi các tham số của nó được chọn hợp lý.

#### 2.2.1.3 Các dạng tấn công đối với hệ mật RSA

##### *a. Dạng 1: Tìm cách xác định khóa bí mật*

##### a.1. Kẻ tấn công chỉ biết khóa công khai của người đăng ký

Kẻ tấn công sẽ dựa vào giá trị n biết được, tìm cách tính ra 2 số nguyên tố p,q → tính ra → tính ra khóa bí mật

Cách phòng tránh: Chọn cặp số nguyên tố p,q lớn. Gây khó cho việc phân tích để tìm n trong thời gian thực, p và q thường các số khoảng 100 chữ số

##### a.2. Kẻ tấn công biết được (N):

Tính ra q, p theo hệ phương trình

→ p, q là nghiệm của của phương trình :

→ Tính ra khóa bí mật d :

→ Kẻ tấn công giả mạo được chữ ký của người dùng

Các phòng tránh: chọn p,q có giá lớn → lớn → khó khăn trong việc tìm ra khóa bị mật

##### a.3 Sử dụng giá trị “modulo n” nhỏ

Theo sơ đồ chữ ký số RSA với văn bản x và chữ ký y, ta có:

với ( )

Kẻ tấn công tính ra khóa bí mật theo công thức:

Vì các giá trị x, y, n công khai, nên nếu giá trị “modulo n” nhỏ thì kẻ tấn công có thể sử dụng các thuật toán để giải được bài toán logarit rời rạc trên vành Zn , sau đó tìm ra khóa bí mật

Các phòng tránh: chọn các tham số tham số p, q lớn để gây khó khăn cho việc giải được bài toán logarit nêu trên.

##### a.4. Dùng các tham số (p-1) và (q-1) có các ước nguyên tố nhỏ

Khi tạo chữ ký, nếu ta chọn các tham số tham số p, q khiến p-1 hoặc q-1 có các ước nguyên tố nhỏ, thì việc tạo chữ ký mất an toàn. Khi p-1 hoặc q-1 có các ước nguyên tố nhỏ thì ta có thể dùng thuật toán của Pollar đưa ra vào năm 1974 để phân tích n thành thừa số nguyên tố một cách dễ dàng

Cách phòng tránh: chọn các tham số tham số p, q sao cho p-1 hoặc q-1 có các ước nguyên tố lớn.

##### b. Dạng 2: Giả mạo chữ ký ( Không tính trực tiếp khóa bí mật)

##### b.1. Ký trước, mã hóa sau

* H có tài liệu x và đã ký chữ ký y, sau đó mã hóa thành z, rồi gửi cho K. Trong lúc gửi đi thì T lấy cắp được, T tìm cách giải mã ra z để lấy được chữ ký y → thay chữ ký y bằng chữ ký giả y’ → gửi đến K
* Cách phòng tránh: số lập mã và giải mã có giá trị lớn

##### b.2. Mã hóa trước, ký sau:

* H có tài liệu x và chữ ký y. Mã hóa x trước thành z sau đó ký chữ ký y, rồi gửi cho K. Trong lúc gửi đi thì T lấy cắp được, T tấn công bằng cách thay chữ ký y bằng chữ ký giả y’ rồi gửi cho K. Cách tấn công này sẽ làm quá trình truyền tin chậm đi.
* Các phòng tránh: Chúng ta sẽ ký trước, sau đó mới mã hóa tài liệu, số lập mã và giải mã có giá trị lớn.

### 

# **Chương 3: ỨNG DỤNG CÁC PHƯƠNG PHÁP VÀO BÀI TOÁN CỤ THỂ**

## 3.1. Thiết kế chương trình

### 3.1.1. Công cụ và ngôn ngữ lập trình

Công cụ: Visual Studio 2019

Ngôn ngữ lập trình: C#

### 3.1.2. Ứng dụng chữ ký số trên hệ mật RSA vào bài toán kê khai hồ sơ nhập học

#### 3.1.2.1. Đặt vấn đề

Hiện nay, xã hội đang hướng đến chuyển đổi số trong hầu hết các lĩnh vực trong đời sống, bao gồm Thương mại điện tử, hoạt động doanh nghiệp, … và giáo dục cũng không phải là ngoại lệ. Ngày càng có nhiều giải pháp công nghệ nhằm giải quyết các bài toán liên quan đến giáo dục, đảm bảo an toàn, bào mật thông tin, quyên lợi cho học sinh, sinh viên. Thủ tục giấy tờ truyền thống đang dần được thay thế bởi công nghệ. Một trong những bài toán mà nền giáo dục đang đối mặt hiện nay là bài toán về việc kê khai hồ sơ nhập học của học sinh, sinh viên. Việc ứng dụng chữ ký số khi kê khai hồ sơ nhập học sẽ giúp các trường học tiết kiệm thời gian, tiền bạc và nâng cao hiệu quả quản lí của trường

#### 3.1.2.2. Bài toán hệ mã RSA

##### a. Thuật toán sinh tham số và khóa

Chú thích: p, q là các số nguyên tố

| Tạo khóa | Ví dụ |
| --- | --- |
| Chọn 2 số p , q | p = 17 , q = 11 |
| Tính n: n=p x q | n = 17\*11 = 187 |
| Tính Ф(n) :Ф(n) = (p-1) x (q-1) | Ф(n) = 16\*10 = 160 |
| Chọn một số ngẫu nhiên e có giá trị trong khoảng: 1< e< Ф(n) và thỏa mãn điều kiện: gcd(e, Ф(n) )= 1 | Tìm được e = 7 thỏa gcd(e,n) = 1 |
| Tính d: d= e^(-1 ) (mod Ф(n)) | d = 7^(-1 ) mod 160 = 23 |
| Khóa công khai: e | e = 7 |
| Khóa riêng tư: d | d = 23 |

***Bảng 3.1.2.2.a***  *Bảng tạo khóa hệ mã RSA*

##### b. Thuật toán ký

Chú thích:

* M : là bản thông điệp cần đc mã hóa
* C : bản mã khi được mã hóa
* e : khóa công khai

| Mã hóa theo khóa công khai | Ví dụ |
| --- | --- |
| Bản gốc: M (M < n) | M = 88 |
| Tính : C = | C = 88^7 mod 187 = 11 |

***Bảng 3.1.2.2.b***  *Bảng mã hóa hệ mã RSA*

##### c. Thuật toán kiểm tra chữ ký

Chú thích d : khóa riêng

| Giải mã bằng khóa riêng | Ví dụ |
| --- | --- |
| Bản mã: C | C = 11 |
| M = | M = 11^23 mod 187 = 88 |

***Bảng 3.1.2.3.c***  *Bảng giải mã hệ mã RSA*

#### 3.1.2.3. Hiệu quả đạt được

Mức độ an toàn của thông tin được nâng cao, đáp ứng được các vấn đề được đặt ra:

- Chống tấn công làm lộ khóa mật

- Chống tấn công giả mạo chữ ký

- Bảo mật thông tin của sinh viên

- Tiết kiệm thời gian, tiền bạc

## 3.2. Xây dựng chương trình

Công cụ thiết kế giao diện: Figma

Khi có luồng flow, bắt tay vào việc thiết kế giao diện trước tiên ta cần vẽ wireframe phác thảo giao diện. Phần thiết kế giao diện cho demo các hệ mật có hai phần chính gồm:

- Wireframe

- Bản giao diện chính thức

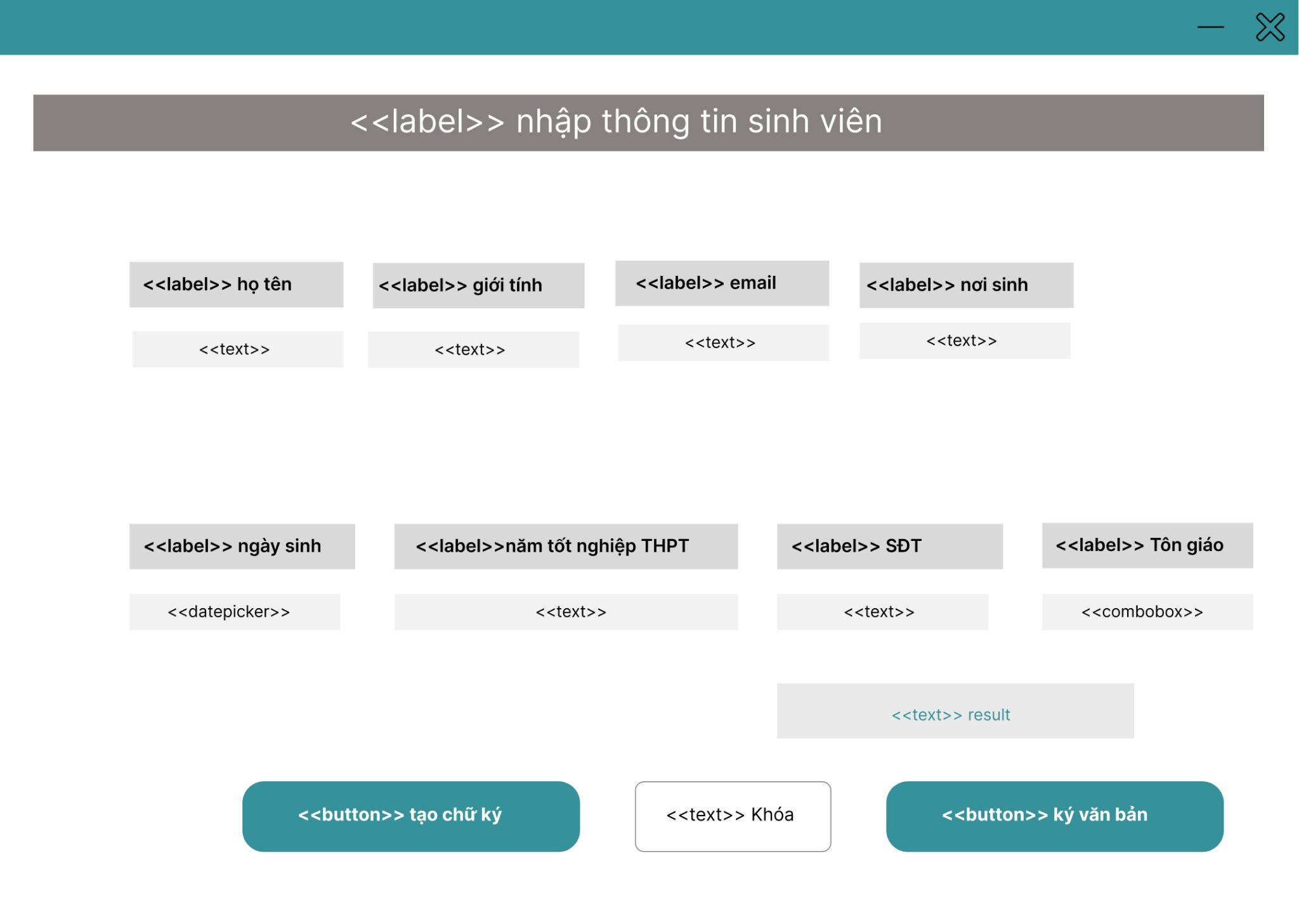
### 3.2.1. Thiết kế giao diện cho hệ mật RSA

#### 3.2.1.1 Wireframe demo hệ mật RSA

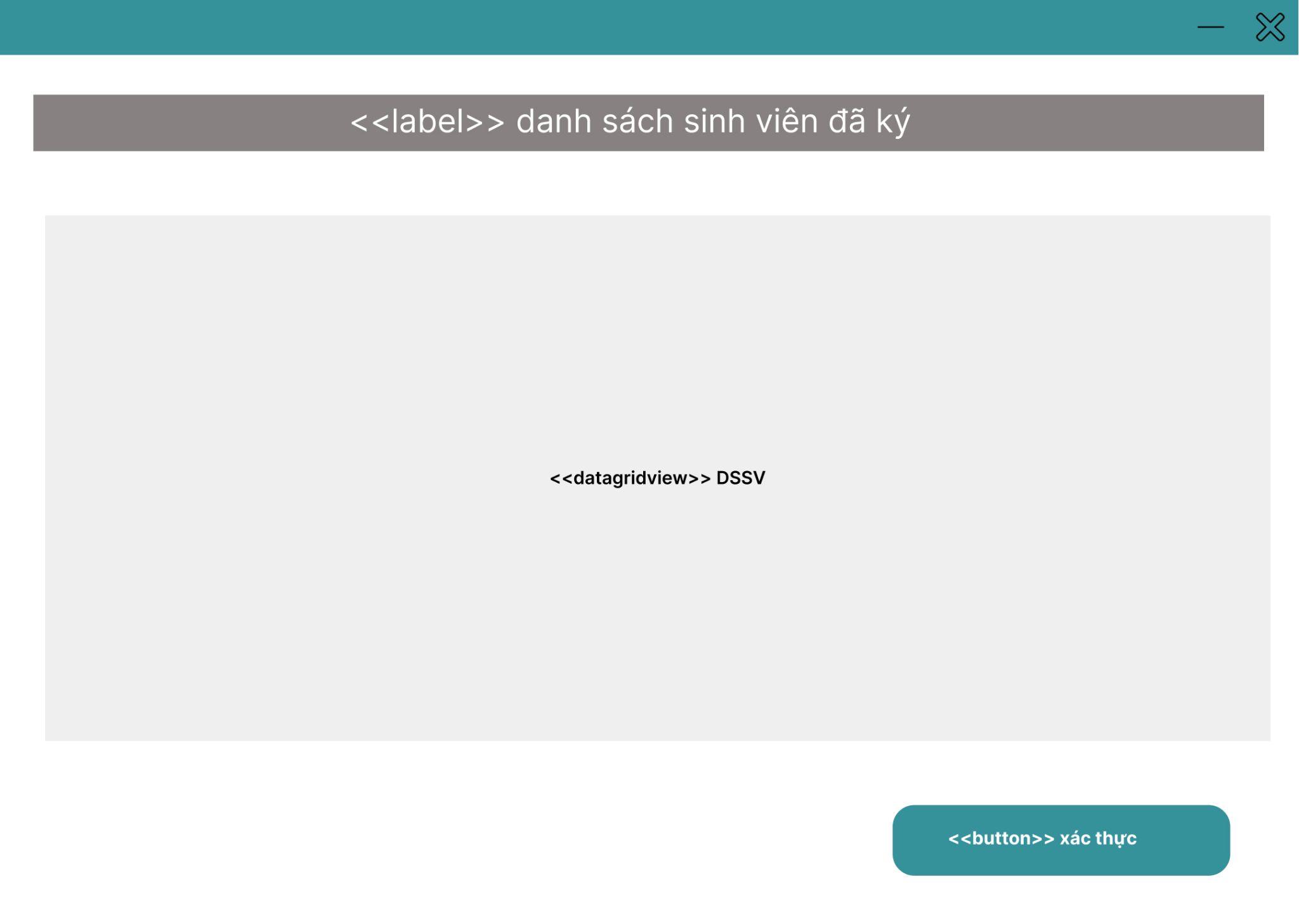
##### Form Login:

***Hình 3.2.1.1.a:*** *Wireframe demo form login*

##### Form Sign:

***Hình 3.2.1.1.b:*** *Wireframe demo form sign*

##### Form Verify:

***Hình 3.2.1.1.c:*** *Wireframe demo form verify*

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

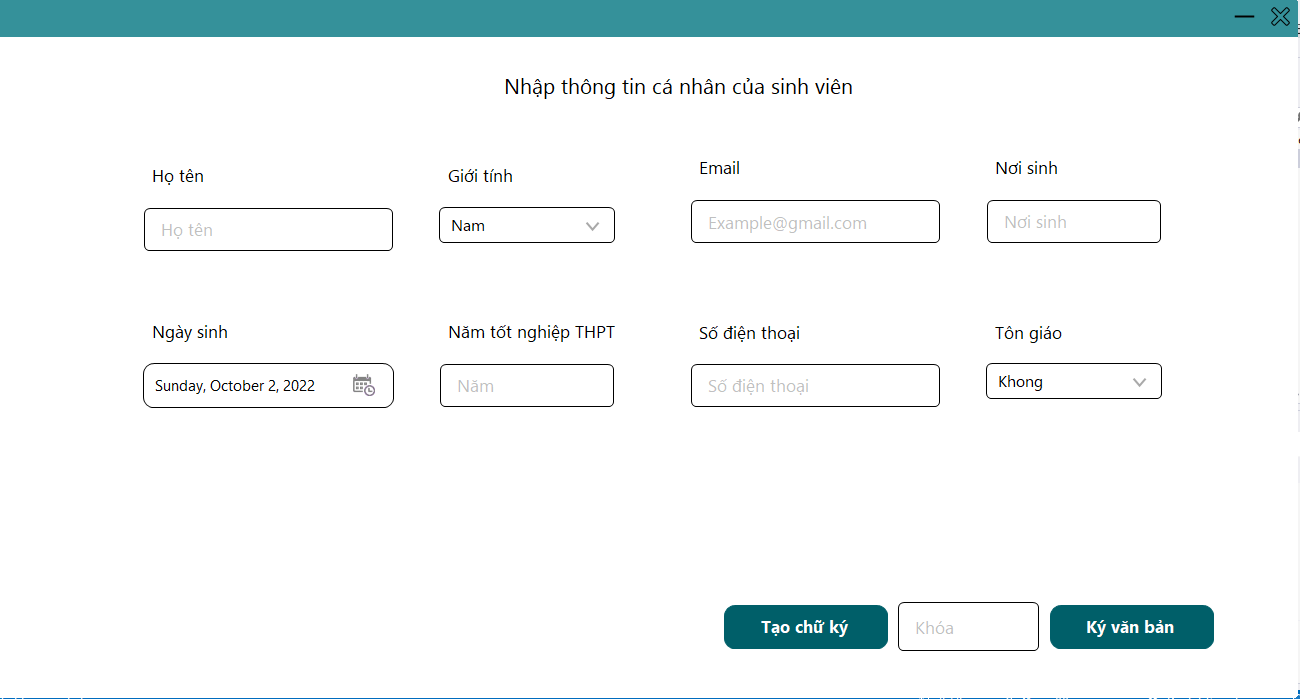
#### 

#### 3.2.1.2 Giao diện demo hệ mật RSA

##### Giao diện Login:

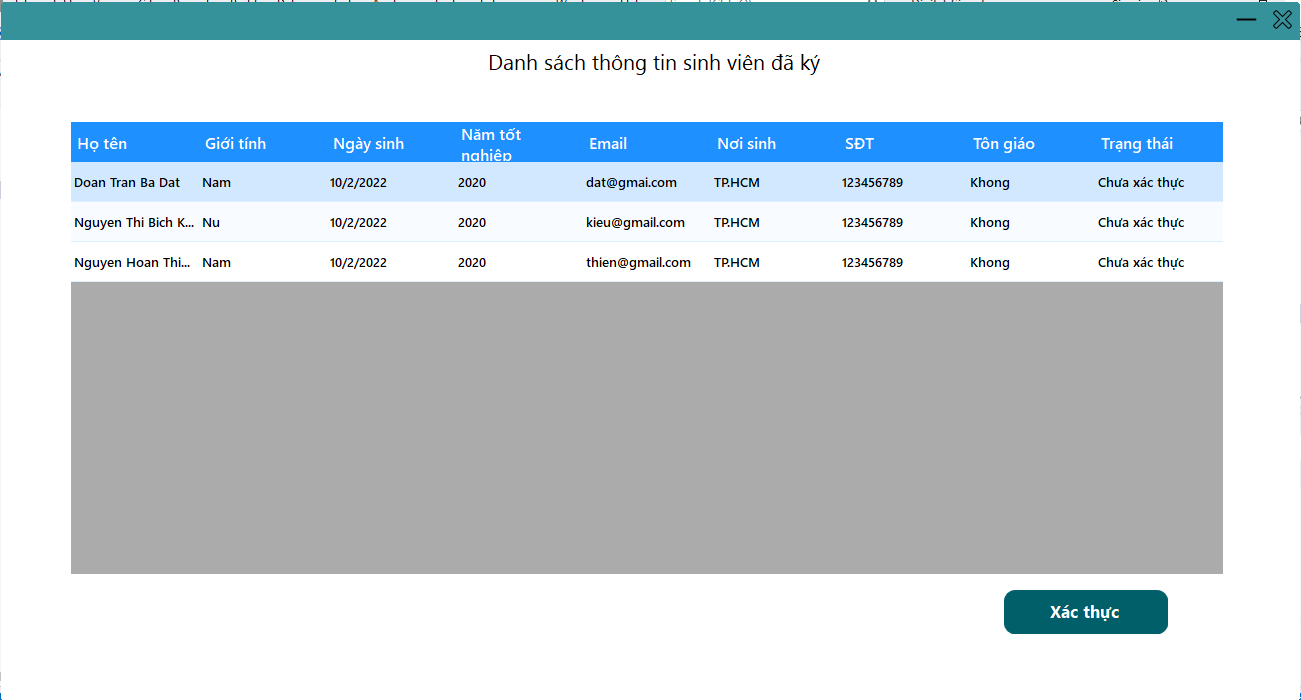
***Hình 3.2.1.2.a:*** *Giao diện demo form login*

##### Giao diện Sign:



***Hình 3.2.1.2.b:*** *Giao diện demo form sign*

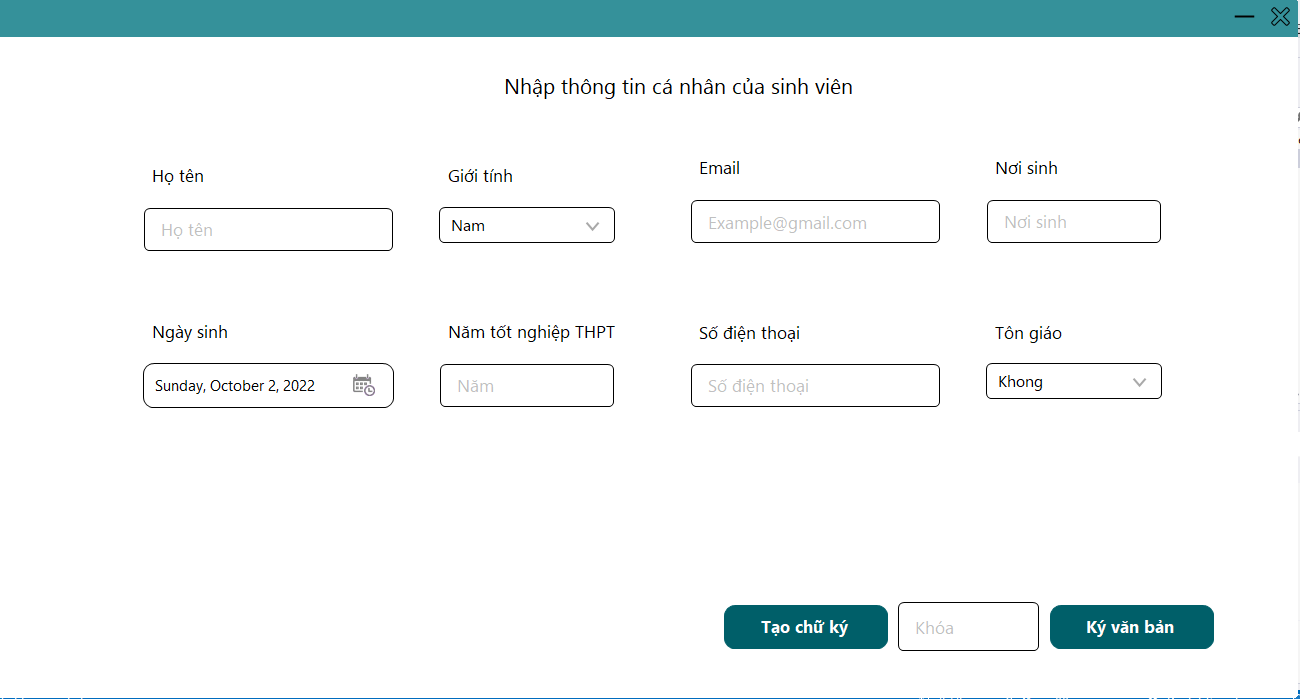
##### Giao diện Verify:

******

***Hình 3.2.1.2.c:*** *Giao diện demo form verify*

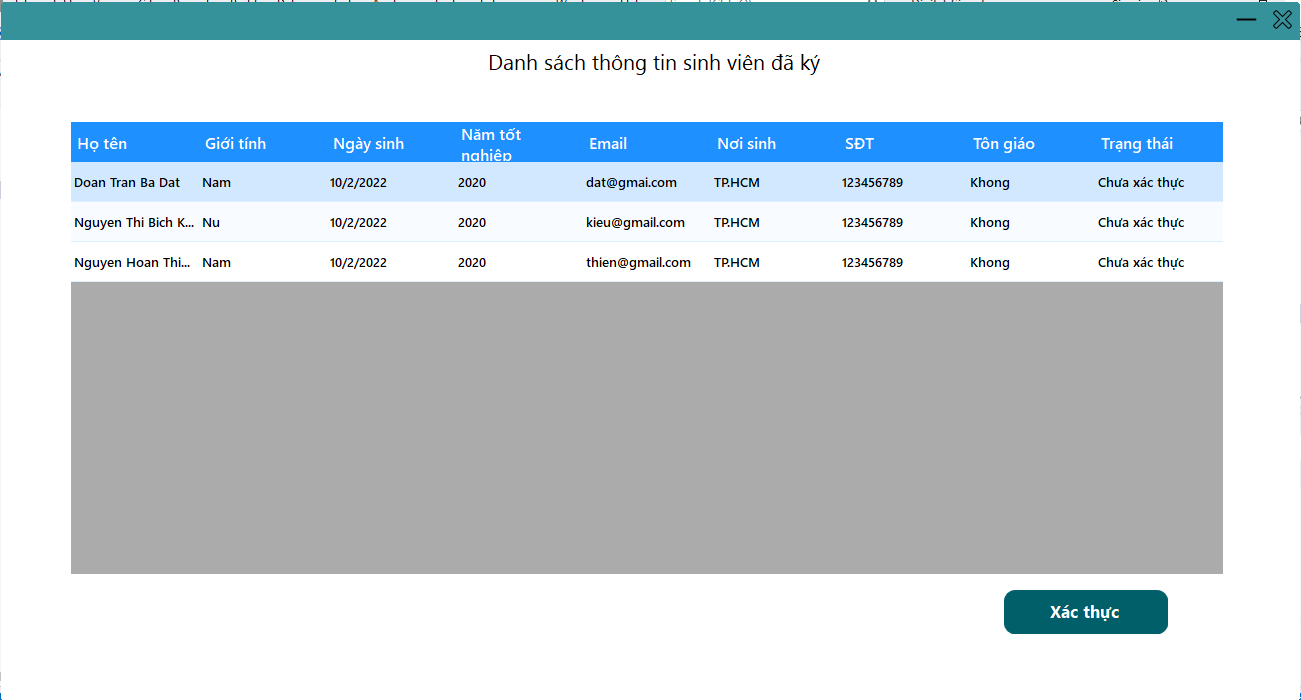
#### 3.2.1.3 Giao diện hệ mật RSA khi chạy chương trình

##### Student



***Hình 3.2.1.3.a:*** *Giao diện Student*

##### Admin

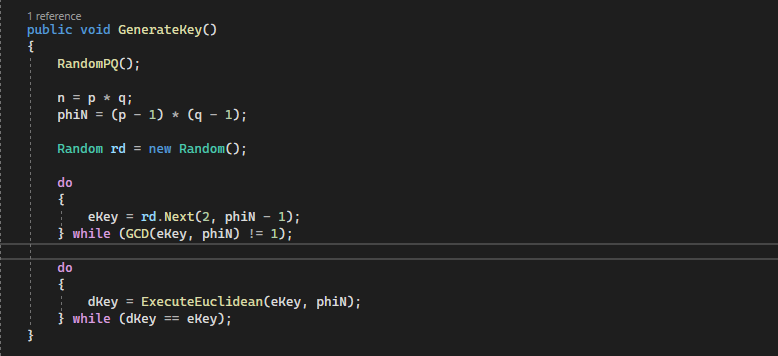
******

***Hình 3.2.1.3.b:*** *Giao diện Admin*

## 3.3. Các hàm, thủ tục chính của chương trình

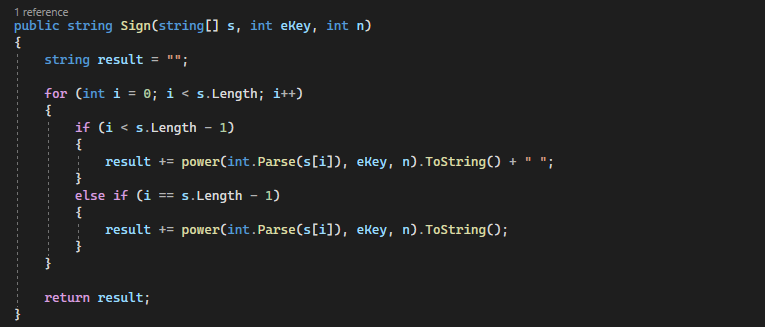
### 3.3.1 Code mã hóa RSA

#### 3.3.1.1 Tạo khóa



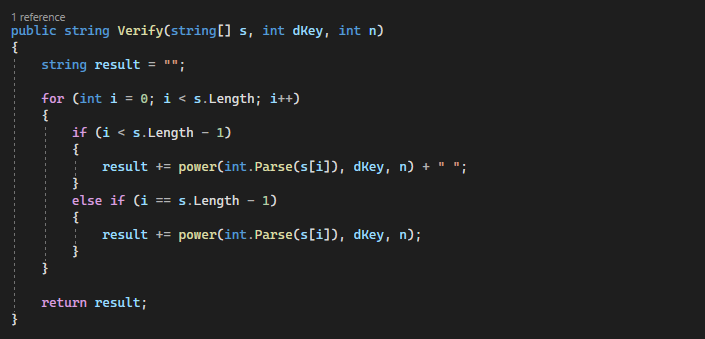
***Hình 3.3.1.a:*** *Code Tạo khóa*

#### 3.3.1.2 Mã hóa



***Hình 3.3.1.b:*** *Code Mã hóa*

#### 3.3.1.3 Giải mã



***Hình 3.3.1.c:*** *Code Giải mã*

# 

# **Chương 4: ĐÁNH GIÁ KẾT QUẢ**

Hiểu và biết ứng dụng phương pháp Mã hóa công khai RSA vào bài toán chữ ký số qua các nội dung:

1. **Giới thiệu về An ninh thông tin**

* Tổng quan khái niệm và mục tiêu An ninh thông tin
* Các mối đe dọa đối với hệ thống
* Các lỗ hổng trên hệ thống mạng
* Biện pháp đảm bảo An ninh thông tin
* Các vấn đề mã hóa dữ liệu gồm mã hóa công khai và mã hóa bất đối xứng

1. **Cơ sở lý thuyết liên quan đến các phương pháp sử dụng**

* Vấn đề chữ ký số
* Kiểu tấn công chữ ký số ( RSA )

1. **Ứng dụng các phương pháp và bài toán cụ thể**

* Thiết kế chương trình
* Xây dựng chương trình
* Các hàm thủ tục chính của chương trình

1. **Xây dựng bản demo cơ bản về hệ mật RSA thông qua bài toán chữ ký số.**

# **KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

## Kết luận

Nghiên cứu và tìm hiểu về tổng quan An ninh thông tin sau đó liên hệ về các mối đe dọa và các lỗ hổng đối với hệ thống, tìm hiểu về nguyên nhân và tìm cách xử lý, giải pháp cho các đe dọa ,lỗ hổng và đảm bảo an ninh trên hệ thống mạng.

Tìm hiểu về vấn đề mã hóa dữ liệu gồm hai vấn đề : Mã hóa khóa đối xứng và mã hóa khóa công khai.

Nghiên cứu và ứng dụng sâu vào Mã hóa khóa công khai, đặc biệt là hệ mật mã: RSA.

Trình bày demo thuật toán RSA trên Winform. Có thể mã hóa và giải mã căn bản.

## Hướng phát triển

Có thể sử dụng vào trong một số ứng dụng để thực hiện những công việc mã hóa cơ bản

Phát triển giao diện đẹp mắt và thân thiện với người dùng hơn.

Tham khảo và liên hệ nhiều hơn với tài liệu nước ngoài.

Áp dụng nhiều hệ mật để ứng dụng vào bài toán chữ ký số một cách hiệu quả và hợp lý.

# **TÀI LIỆU THAM KHẢO**

1. Nguyễn, Hùng Quốc. “*Giáo trình An ninh thông tin*.” Khoa công nghệ thông tin kinh doanh - Trường Công nghệ và thiết kế - Đại học UEH.

2. “*High availability solutions.*” https://www.imperva.com/learn/availability/high-availability/.

3. Ian F. Blake và Theo Garefalakis. *Về độ phức tạp của các bài toán logarit rời rạc* và diffie-hellman.J. *Phức tạp., 20 (2-3): 148–170, 2004.*

4. “Lê, Thị Thu Trang. *Nghiên cứu một số loại tấn công chữ ký số*. Diss. Đại học Dân lập Hải Phòng, 2009.”

5. “Milanov, Evgeny. "*The RSA algorithm." RSA laboratories (2009): 1-11.*”

6. “*Data Encryption.*” https://www.imperva.com/learn/data-security/data-encryption/.

7. “Nguyễn, Văn Liệu. *Tìm hiểu chữ ký số và ứng dụng của nó*. Diss. Đại học Quốc gia Hà Nội, 2009.”