TRƯỜNG ĐẠI HỌC TÂY NGUYÊN

**KHOA KHOA HỌC TỰ NHIÊN VÀ CÔNG NGHỆ**



**TIỂU LUẬN**

**HỌC PHẦN : AN TOÀN THÔNG TIN**

**SINH VIÊN : NGYỄN HOÀNG TÁN TRUNG - 18103094**

**CHUYÊN NGÀNH : CÔNG NGHỆ THÔNG TIN**

**KHÓA HỌC : K18**

**Đắk Lắk, tháng 03 năm 2022**

TRƯỜNG ĐẠI HỌC TÂY NGUYÊN

**KHOA KHOA HỌC TỰ NHIÊN VÀ CÔNG NGHỆ**



**TIỂU LUẬN**

**HỌC PHẦN :AN TOÀN THÔNG TIN**

**SINH VIÊN : NGUYỄN HOÀNG TÁN TRUNG - 18103094**

**CHUYÊN NGÀNH : CÔNG NGHỆ THÔNG TIN**

**GIẢNG VIÊN HƯỚNG DẪN : VŨ ANH TUẤN**

**Đắk Lắk, tháng 03 năm 2022**

LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến toàn thể quý thầy cô trong Bộ môn Công nghệ thông tin, Khoa Khoa học Tự nhiên và Công nghệ, Trường Đại học Tây Nguyên đã truyền đạt cho em những kiến thức quý báu trong suốt quá trình học tập. Và đặc biệt là Giảng Viên Hướng Dẫn **Vũ Anh Tuấn** đã tận tình hướng dẫn em trong quá trình hoàn thành đề tài.

Vì kiến thức, khả năng của bản thân còn nhiều hạn hẹp, trong quá trình thực hiện, hoàn thành chuyên đề này em không tránh khỏi những thiếu sót. Chúng rất mong nhận được sự chỉ bảo, đóng góp ý kiến từ quý thầy cô.

Em xin chân thành cảm ơn!

**Đắk Lắk, tháng 03 năm 2022**

**Nguyễn Hoàng Tán Trung**

LỜI NÓI ĐẦU

An toàn thông tin được hiểu là một hành động nhằm phòng ngừa, ngăn chặn hoặc ngăn cản sự truy cập, sử dụng, chia sẻ thông tin, tiết lộ, phát tán, phá hủy hoặc ghi lại những thông tin khi chưa được sự cho phép của chủ sở hữu. An toàn thông tin ngày nay được coi là vấn đề đáng lưu tâm hàng đầu của xã hội. Nó là một vấn đề ảnh hưởng đến các ngành kinh tế, khoa học – kỹ thuật và xã hội.   
Bảo vệ thông tin và các hệ thống thông tin tránh khỏi việc bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép. Hiểu một cách nôm na an toàn thông tin là quá trình phát hiện và ngăn chặn mọi hành vi sử dụng trái phép máy tính máy tính/ điện thoại hoặc thiết bị chứa thông tin. Nó liên quan đến quá trình bảo vệ chống lại những kẻ xâm phạm sử dụng tài nguyên máy tính cá nhân hoặc văn phòng của bạn với mục đích xấu hoặc vì lợi ích riêng bất hợp pháp, hoặc thậm chí do vô tình.

Chính vì vậy mà An toàn thông tin trở thành một thứ đáng quan tâm và hấp dẫn với một thời đại công nghệ số và internet phát triển chóng mặt như hiện nay.

ĐẶT VẤN ĐỀ

Nhân loại đang sống trong những năm đầu thế kỷ 21, thời đại mà thông tin, tri thức trở thành lực lượng sản xuất trực tiếp, thời đại của xã hội thông tin và nền kinh tế tri thức được hình thành trên cơ sở phát triển và ứng dụng rộng rãi công nghệ thông tin và truyền thông. Cuộc cách mạng thông tin đang ảnh hưởng sâu sắc đến mọi lĩnh vực trong đời sống kinh tế - xã hội, đưa con người chuyển nhanh từ xã hội công nghiệp sang xã hội thông tin, từ kinh tế công nghiệp sang kinh tế tri thức, ở đó năng lực cạnh tranh phụ thuộc chủ yếu vào năng lực sáng tạo, thu thập, lưu trữ, xử lý và trao đổi thông tin.

Cùng với sự phát triển bùng nổ của Internet, an toàn thông tin là một vấn đề nóng hổi của xã hội. Nguy cơ mất an toàn thông tin do nhiều nguyên nhân, đối tượng tấn công đa dạng Thiệt hại từ những vụ tấn công mạng là rất lớn, đặc biệt là những thông tin thuộc lĩnh vực kinh tế, an ninh, quốc phòng Do đó, việc tìm hiểu và áp dụng các công nghệ nhằm mã hóa, xác thực dữ liệu để ngăn chặn những truy cập trái phép trở thành nhu cầu cấp bách trong các hoạt động truyền thông.

Theo số liệu thống kê, Việt Nam đứng thứ 2 trong khu vực Đông Nam á về các hoạt động tấn công mạng. Thực tế, nguy cơ mất an ninh an toàn mạng máy tính còn có thể phát sinh ngay từ bên trong. Nguy cơ mất an ninh từ bên trong xảy ra thường lớn hơn nhiều, nguyên nhân chính là do người sử dụng có quyền truy nhập hệ thống nắm được điểm yếu của hệ thống hay vô tình tạo cơ hội cho những đối tượng khác xâm nhập hệ thống.

# NỘI DUNG NGHIÊN CỨU

1. **Đối tượng nghiên cứu**

* Nghiên cứu an toàn thông tin

1. **Phạm vi nghiên cứu**

* Chương trình OpenSLL.exe
* Visual Studio Code C#

1. **Nội dung nghiên cứu**

* Tổng quan về an toàn thông tin
* Khái niệm khóa Private key và Public key
* Sử dụng OpenSLL tạo Private key và Public key
* Thực hiện tính năng đăng nhập khóa Private key trên trên Visual Studio Code C#
* Sử dụng mã hóa MD5 trên Visual Studio Code C# để tạo đăng ký , đăng nhập

# MỤC LỤC

[LỜI CẢM ƠN 3](#_Toc96973368)

[LỜI NÓI ĐẦU 4](#_Toc96973369)

[ĐẶT VẤN ĐỀ 5](#_Toc96973370)

[NỘI DUNG NGHIÊN CỨU 6](#_Toc96973371)

[MỤC LỤC 7](#_Toc96973372)

[CHƯƠNG I : TỔNG QUAN VỀ AN TOÀN THÔNG TIN 9](#_Toc96973373)

[1. Một số khái niệm về An toàn thông tin 9](#_Toc96973374)

[1.1. Đối tượng tấn công 9](#_Toc96973375)

[1.2. Các hình thức tấn công phổ biến 9](#_Toc96973376)

[2. Giải pháp nâng cao an toàn thông tin 9](#_Toc96973377)

[CHƯƠNG II : KHÁI NIỆM PRIVATE KEY VÀ PUBLIC KEY 10](#_Toc96973378)

[1. Khái niệm Private key 10](#_Toc96973379)

[2. Khái niệm Public key 10](#_Toc96973380)

[3. So sánh Private key và Public key 10](#_Toc96973381)

[4. Cách thức Private key và Public key hoạt động 11](#_Toc96973382)

[CHƯƠNG III : SỬ DỤNG OPENSSL TẠO PRIVATE KEY VÀ PUBLIC KEY 12](#_Toc96973383)

[1. Tổng quan về OpenSSL 12](#_Toc96973384)

[1.1. Giới thiệu OpenSSL 12](#_Toc96973385)

[1.2. Công dụng của OpenSSL 12](#_Toc96973386)

[2. Hướng dẫn tải 13](#_Toc96973387)

[3. Tạo Public key và Private Key với Openssl.exe 14](#_Toc96973388)

[CHƯƠNG IV: THỰC HIỆN TÍNH NĂNG ĐĂNG NHẬP KHÓA PRIVATE KEY TRÊN TRÊN VISUAL STUDIO CODE C# 15](#_Toc96973389)

[1. Tổng quan mã hóa RSA 15](#_Toc96973390)

[2. Ứng dụng của RSA 16](#_Toc96973391)

[2.1. RSA Trong bảo mật dữ liệu 16](#_Toc96973392)

[2.2. Ứng dụng của RSA trong công nghệ thông tin 17](#_Toc96973393)

[3. Thực hiện trên VISUAL STUDIO CODE C# 18](#_Toc96973394)

[CHƯƠNG V : SỬ DỤNG MÃ HÓA MD5 TRÊN VISUAL STUDIO CODE C# ĐỂ TẠO ĐĂNG KÝ , ĐĂNG NHẬP 21](#_Toc96973395)

[1. Tổng quan mã hóa MD5 21](#_Toc96973396)

[2. Ứng dụng của MD5 22](#_Toc96973397)

[3. Thực hiện trên VISUAL STUDIO CODE C# 22](#_Toc96973398)

[LINK Trình bày báo cáo: 24](#_Toc96973399)

[KẾT LUẬN 25](#_Toc96973400)

[TÀI LIỆU THAM KHẢO: 26](#_Toc96973401)

# CHƯƠNG I : TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1. **Một số khái niệm về An toàn thông tin**
2. **Đối tượng tấn công**

 Là đối tượng sử dụng kỹ thuật về mạng để dò tìm các lỗ hổng bảo mật trên hệ thống để thực hiện xâm nhập và chiếm đoạt thông tin bất hợp pháp. Các đối tượng tấn công mạng:

* Hacker: Xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của hệ thống.
* Masquerader: Giả mạo thông tin, địa chỉ IP, tên miền, định danh người dùng.
* Eavesdropping: Là đối tượng nghe trộm thông tin trên mạng để lấy cắp thông tin.

1. **Các hình thức tấn công phổ biến**

Scanner: Là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc ở xa.

Password Cracker: Là một chương trình có khả năng giải mã mật khẩu đã được mã hoá hoặc vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.



Hình 1. Các hình thức tấn công

Sniffer: Là các công cụ bắt các thông tin trao đổi trên mạng máy tính.

Trojans: Là một chương trình thực hiện không hợp lệ được cài đặt trên một hệ thống.

1. **Giải pháp nâng cao an toàn thông tin**

Việc đảm bảo an ninh an toàn cho hệ thống dữ liệu ta có ba giải pháp chủ yếu sau:

Giải pháp phần cứng: là giải pháp sử dụng các thiết bị vật lý như các hệ thống máy chuyên dụng, thiết lập trong mô hình mạng Giải pháp phần cứng thông thường đi kèm là hệ thống phần mềm điều khiển tương ứng.

Giải pháp phần mềm: có thể phụ thuộc hay không phụ thuộc vào phần cứng. Như các giải pháp: xác thực, mã hoá dữ liệu, mạng riêng ảo, hệ thống tường lửa…

Giải pháp về con người: Đảm bảo an ninh, an toàn thông tin phụ thuộc nhiều vào yếu tố con người, do vậy cần phải đẩy mạnh công tác đào tạo, chế tài để định hướng người sử dụng trong khai thác, sử dụng thông tin.

# CHƯƠNG II : KHÁI NIỆM PRIVATE KEY VÀ PUBLIC KEY

1. **Khái niệm Private key**

Khóa Private key được sử dụng để mã hóa và giải mã dữ liệu. Khóa này được chia sẻ giữa người gửi và người nhận thông tin bảo mật cần được mã hóa. Khóa Private key còn được gọi là khóa đối xứng vì khóa duy nhất được bên khác sao chép hoặc chia sẻ để giải mã văn bản mật mã. Cơ chế mật mã khóa cá nhân nhanh hơn cơ chế mật mã khóa công khai.

1. **Khái niệm Public key**

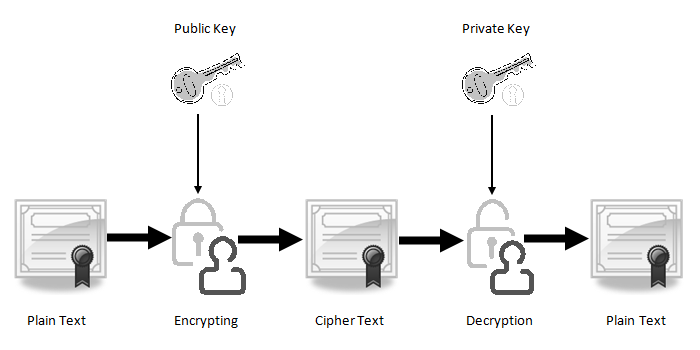
Khóa Public key được sử dụng để mã hóa và khóa Private key được sử dụng để giải mã dữ liệu. Khóa Private key được chia sẻ giữa người gửi và người nhận thông tin nhạy cảm được mã hóa. Khóa Public key được gọi là mật mã không đối xứng.

1. **So sánh Private key và Public key**

|  |  |  |
| --- | --- | --- |
|  | Private key | Public key |
| Tốc độ | Private key nhanh hơn Public key | Chậm hơn Private key |
| Thuật toán | Private Key được sử dụng để vừa mã hóa vừa giải mã dữ liệu và được chia sẻ giữa người gửi và người nhận dữ liệu được mã hóa. | Public key chỉ được sử dụng để mã hóa dữ liệu và để giải mã dữ liệu |
| Bảo mật | Private key được giữ bí mật và không công khai cho bất kỳ ai ngoài người gửi và người nhận. | Public key được sử dụng công khai |
| Thể loại | Private key là **Đối xứng** vì chỉ có một khóa duy nhất được gọi là khóa bí mật. | Cơ chế Public key được gọi là bất đối xứng |
| Chia sẻ | Private key sẽ được chia sẻ giữa hai bên. | Public key có thể được sử dụng bởi bất kỳ ai |
| Mục tiêu | Kiểm tra hiệu suất kiểm tra độ tin cậy, khả năng mở rộng và tốc độ của hệ thống. | Thử tải kiểm tra tính bền vững của hệ thống. |

1. **Cách thức Private key và Public key hoạt động**

Public Key có hai trường hợp sử dụng chính – nhận dạng và bảo mật. Quy trình như được mô tả ngắn gọn như sau:



Hình 2. Cách thức hoạt động của Private key và Public key

* Người gửi biết được public key của người nhận địa chỉ.
* Người gửi sử dụng key này để mã hóa thông tin.
* Người gửi, gửi những thông tin được mã hóa đến người nhận.
* Người nhận sử dụng private key của mình để giải mã thông tin này.

# CHƯƠNG III : SỬ DỤNG OPENSSL TẠO PRIVATE KEY VÀ PUBLIC KEY

1. **Tổng quan về OpenSSL**
2. **Giới thiệu OpenSSL**

OpenSSL là một thư viện phần mềm sử dụng các mã nguồn mở để triển khai các giao thức mạng và mã hoá dữ liệu khác nhau như SSL và TLS. OpenSSL được sử dụng trong trường hợp cần xác định phe truyền thống ở phía đầu bên kia hoặc các ứng dụng bảo mật truyền thông qua mạng máy tính để phòng chống nghe trộm.



Hình 3. phần mềm OpenSSL

OpenSSL đã được ra mắt vào năm 1998 và được cài đặt sẵn trên các hệ điều hành Linux, Windows, macOS hay BSD. Chúng được sử dụng rộng rãi trong nhằm phục vụ đa số các website hiện nay trong các máy chủ web Internet. Hiện nay, theo thống kê, OpenSSL là một phương thức bảo mật được sử dụng nhiều nhất. Tuy nhiên, nếu muốn website được bảo mật tốt nhất, bạn cần gia hạn SSL let’s encrypt.

Khi nhắc tới các chứng chỉ SSL/TLS và cách thức để triển khai chúng, OpenSSL là một công cụ thích hợp hàng đầu. Thư viện gốc của các phần mềm trong OpenSSL được viết bằng ngôn ngữ lập trình C. Bên cạnh đó, OpenSSL cũng có nhiều phần mềm cho phép người dùng sử dụng thư viện với nhiều ngôn ngữ khác nhau. Các phần mềm đều có chức năng mã hoá tổng quát để mã hoá và giải mã dữ liệu. Bạn cũng có thể sử dụng dòng lệnh để yêu cầu, tạo và quản lý các chứng thực số.

1. **Công dụng của OpenSSL**

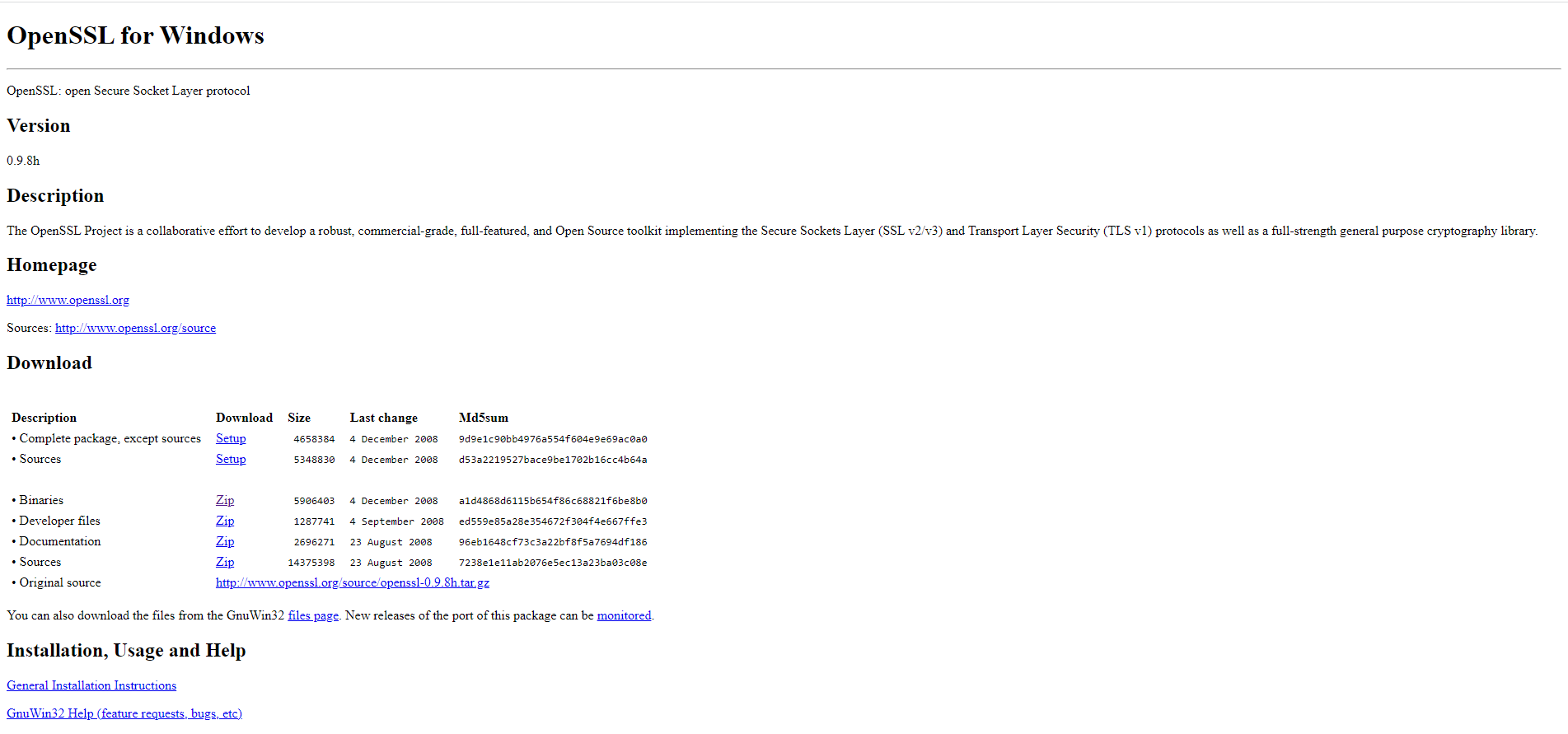
Thư viện phần mềm này có vai trò cực kỳ quan trọng trong công nghệ thông tin. Bạn có thể sử dụng OpenSSL để đăng ký chứng chỉ số hay còn gọi là tạo yêu cầu ký chứng chỉ. Các giao thức SSL cũng được cài đặt trên máy chủ một cách dễ dàng.

Bên cạnh đó, OpenSSL còn hỗ trợ người dùng thực hiện các loại xác minh và chuyển đổi chứng chỉ đang có thành các dạng SSL khác nhau. Các lệnh OpenSSL được sử dụng phổ biến để hỗ trợ quá trình cấu hình hoá trở nên dễ dàng và nhanh chóng hơn. Hiện nay, hầu hết các máy chủ đều không cung cấp giao diện người dùng web nên bạn hoàn toàn có thể quản lý SSL. OpenSSL là giải pháp duy nhất trên một số nền tảng để bạn nhập và cấu hình chứng chỉ.

Tóm lại, nhờ có OpenSSL, bạn có thể tạo ra các tham số chính RSA, DH hay DSA. Người dùng tạo ra các chứng chỉ X.509, CSR, CRL và mã hoá hoặc giải mã chúng bằng mật mã. Hơn thế nữa, các lệnh của OpenSSL được dùng để kiểm tra máy khách, máy chủ SSL/TLS, mã hóa S/MIME và xử lý email đã ký.

1. **Hướng dẫn tải**

B1: Truy cập vào đường dẫn [**http://gnuwin32.sourceforge.net/packages/openssl.htm**](http://gnuwin32.sourceforge.net/packages/openssl.htm)

****

Hình 4. Tải OpenSSL

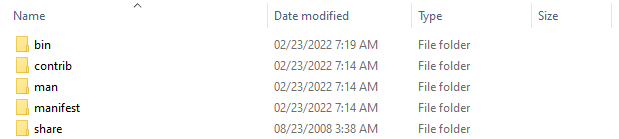
B2: Tại mục Dowload tải xuống Binaries Zip

B3: Sau khi tải về ta được 1 file nén Zip



Hình 5. File nén zip sau khi tải xuống

B4: Giải nén file ta các có thư mục sau:



Hình 6. File sau khi giải nén

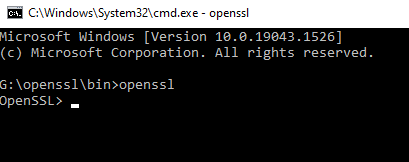
1. **Tạo Public key và Private Key với Openssl.exe**

**Bài hướng dẫn :**

[**http://lunar.lyris.com/help/Content/generating\_public\_and\_private\_keys.html**](http://lunar.lyris.com/help/Content/generating_public_and_private_keys.html)

B1: Mở Command Prompt điều hướng tới thư mục bin trong folder OpenSSL

B2: Sau đó nhập OPENSSL

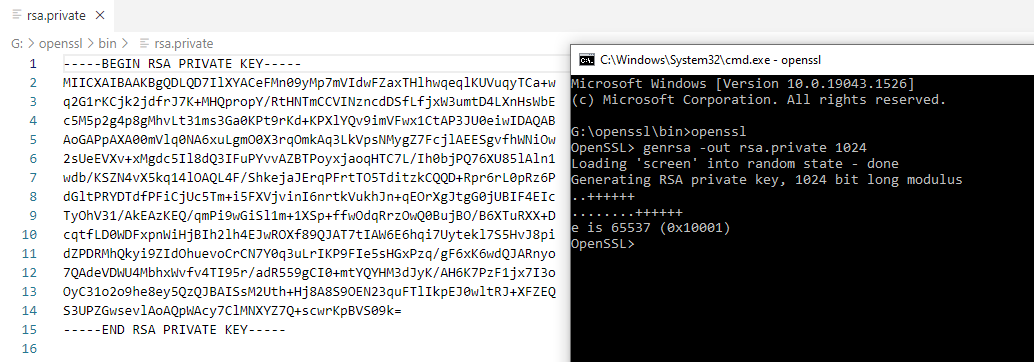
****

Hình 7. Thực hiện trên cmd

B3: Nhập dòng lệnh

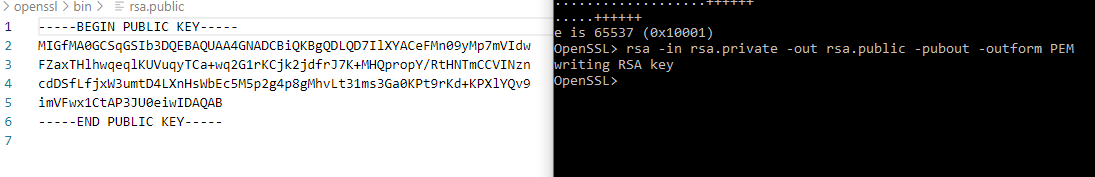
genrsa -out rsa.private 1024

B4: Kết quả



Hình 8. tạo được 1 file Private key

Từ Private key ta sẽ tạo ra được Public key, ta sẽ tạo Public key bằng cách nhập dòng lệnh sau:  
rsa -in rsa.private -out rsa.public -pubout -outform PEM

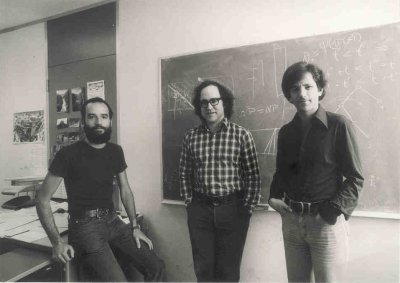


Hình 9. Kết quả thu được

# CHƯƠNG IV: THỰC HIỆN TÍNH NĂNG ĐĂNG NHẬP KHÓA PRIVATE KEY TRÊN TRÊN VISUAL STUDIO CODE C#

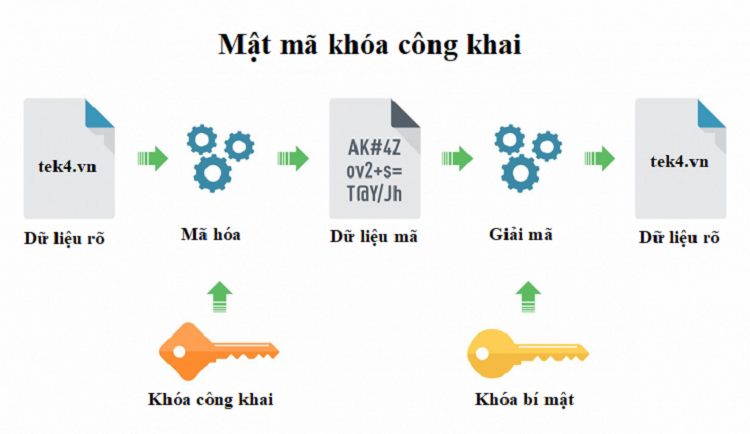
1. **Tổng quan mã hóa RSA**

Thuật toán được Rivest, Shamir và Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.



Hình 10. Ba tác giả của thuật toán mã hóa RSA

Mã hóa RSA chính là một thuật toán hay còn gọi là hệ mã hóa bất đối xứng có pháp vi ứng dụng rộng rãi và phổ biến. đặc biệt người ta sử dụng RSA rất nhiều ở công tác mã hóa, thiết lập chữ ký điện tử, với vai trò là một mã hóa khóa công khai. Bất cứ ai cũng có thể dùng khóa công khai để có thể mã hóa được nguồn dữ liệu muốn gửi đi thế nhưng để giải mã được dữ liệu gửi đi đó thì buộc phải có sự hỗ trợ của Private Key.



Hình 11. Cách thức hoạt động của RSA

Hoạt động gửi và nhận sẽ được can thiệp bởi RSA vì bản thân nó chứa 2 khóa là Public Key và Private để làm 2 nhiệm vụ bất đối xứng và mã hóa và giải mã. Điều này cũng tương tự như cơ chế đóng khóa và mở khóa cửa vậy nhưng tất nhiên RSA sẽ phức tạp hơn rất nhiều bởi nó là một thuật toán. Việc mã hóa để bảo mật thông tin nhưng gây bất lợi cho người nhận khi không thể giải mã được các giá trị thông tin đã được mã hóa, chính vì thế mà cần đến yếu tố khóa bí mật luôn đi kèm với việc mã hóa, và khóa bí mật này cũng chỉ có ở người nhận thông tin đã mã hóa được gửi tới họ thông qua RSA.

Không giống với loại mã hóa có khóa đối xứng, Private của RSA tuyệt đối không truyền được thông tin ra bên ngoài ngay cả khi có thiết bị nghe trộm thì nếu đối tượng xấu không có khóa bị mật cũng sẽ không thể giải mã được thông tin đó. Như vậy rõ ràng với 2 tính năng mã hóa và giải mã tối ưu đến tuyệt đối ở một phương trình bất đối xứng như vậy cho nên giá trị của RSA vô cùng lớn, nó sẽ được sử dụng ở hầu hết mọi trường hợp cần bảo mật thông tin. Giao thức SSL hayTSL, HTTPS cùng với chứng chỉ điện tử đều sử dụng RSA.

1. **Ứng dụng của RSA**
2. **RSA Trong bảo mật dữ liệu**

RSA ra đời với mục đích bảo vệ dữ liệu, do vậy chúng được ứng dụng rất nhiều trong hoạt động hiện đại. Những ứng dụng của RSA trong bảo mật dữ liệu như:

* Chứng thực dữ liệu: chắc hẳn các bạn đã từng gặp tình trạng yêu cầu xác minh bằng cách đưa ra các con số gửi về email hay số điện thoại trước khi đăng nhập. Đây chính là phương pháp bảo mật thông tin, dữ liệu ứng dụng thuật toán RSA để tránh những tình trạng mạo danh, hack tài khoản gây ảnh hưởng cho người dùng và xã hội. Việc chứng thực giúp bảo vệ được tài khoản của bản thân người sử dụng giúp an tâm hơn khi sử dụng các dịch vụ trực tuyến.
* Truyền tải dữ liệu an toàn: hiện nay tình trạng nghe lén, theo dõi hoạt động cũng như lấy cắp dữ liệu cá nhân trên mạng xã hội bị lên án và chỉ trích rất nhiều, bao gồm cả ông lớn Facebook. Không chỉ những trang mạng xã hội, các trang web cũng không tránh khỏi việc lưu lại các hoạt động, hành vi truy cập để phục vụ các mục đích Marketing. Do đó với thuật toán RSA giúp dữ liệu khỏi các cuộc tấn công của kẻ xấu.



Hình 12. RSA và chữ ký số

* Chữ ký số/ chữ ký điện tử: trên các thẻ ATM luôn có phần chữ ký điện tử đã được mã hóa từ chữ ký của khách hàng khi đăng ký tài khoản tại ngân hàng. Có thể nói, trong lĩnh vực ngân hàng, vấn đề bảo mật thông tin của khách hàng cần được đặt lên hàng đầu, chúng quyết định chất lượng của dịch vụ. RSA được ứng dụng để bảo mật dữ liệu khi người dùng thực hiện những giao dịch ngân hàng, đem lại trải nghiệm tốt và giúp khách hàng an tâm hơn.

1. **Ứng dụng của RSA trong công nghệ thông tin**

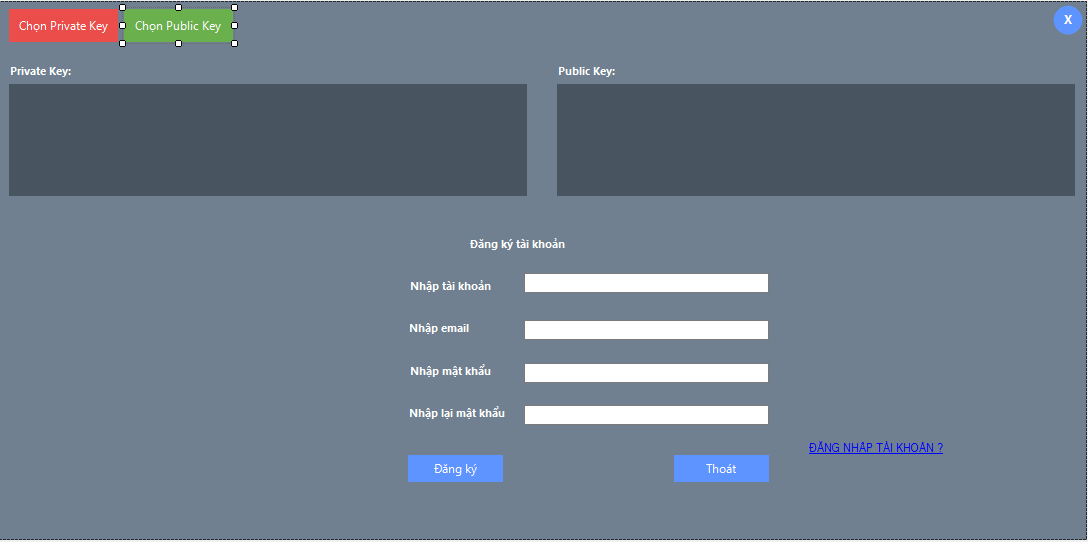
Trong ngôn ngữ lập trình Java, các nhà lập trình viên thường sử dụng những đoạn code chứa RSA để tăng tính bảo mật cho trang web và ứng dụng cũng như đảm bảo an toàn cho người sử dụng.Các đoạn code RSA này có thể hoạt động dưới bất kỳ sự thay đổi nào của môi trường. Ngoài ra, các lập trình viên cũng sử dụng các ngôn ngữ lập trình khác bên cạnh Java có thể tìm hiểu và ứng dụng những tính năng của RSA trong hoạt động làm việc và bảo mật thông tin.



Hình 13. Ứng dụng của RSA trong công nghệ thông tin

Ngày nay việc sử dụng các ứng dụng, trang web trên internet ngày càng gia tăng khiến cho vấn đề bảo mật dữ liệu càng được chú trọng. Những dữ liệu này có thể là những thông tin bí mật cá nhân, thông tin về tài chính,... gây không ít nguy hại cho người sử dụng. Cũng chính vì lý do này mà thuật toán RSA được biết đến và sử dụng nhiều hơn trong tất cả các lĩnh vực đặc biệt là trong ngành ngân hàng.

1. **Thực hiện trên VISUAL STUDIO CODE C#**



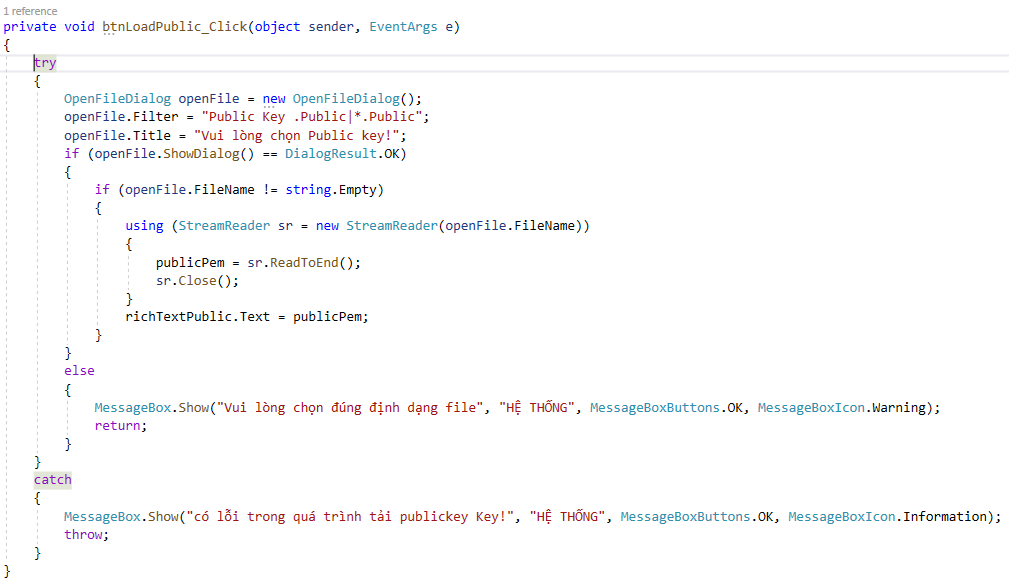
Hình 14. Giao diện đăng ký tài khoản

Mô tả: Nhập file PRIVATE Key vừa tạo ở OPENSSL



Hình 15. Nhập file Private Key

Mô tả: Nhập file PUBLIC Key vừa tạo ở OPENSSL

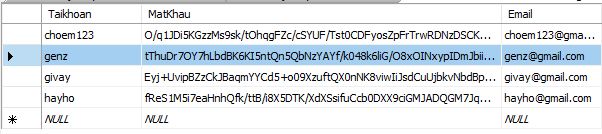


Hình 16. Nhập file Public Key

Mô tả : nhập thông tin tài khoản , mật khẩu , email. Ta sẽ mã hóa mật khẩu rồi đưa vào lưu SQL

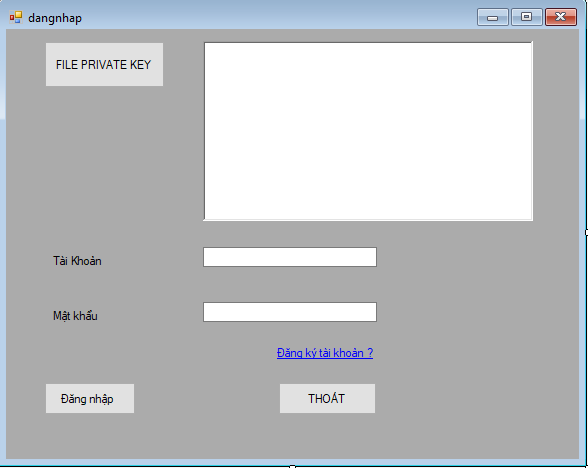


Hình 17. thực hiện lưu tài khoản , mật khẩu vào SQL



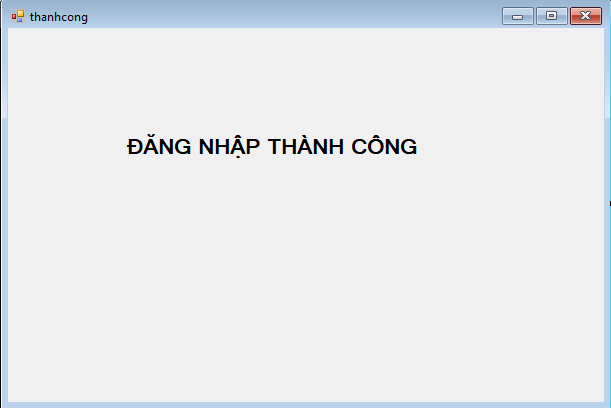
Hình 18. Tài khoản, mật khẩu được lưu vào SQL

Mô tả : ta chọn file PRIVATE key đăng ký tài khoản để đăng nhập



Hình 19. Chọn file Private Key và nhập tài khoản , mật khẩu

Mô tả : đăng nhập thành công sẽ ra trang khác

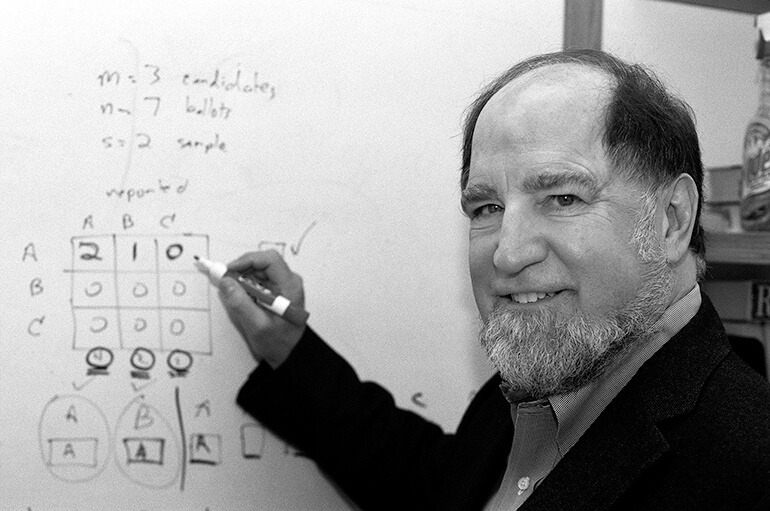


Hình 20. Đăng nhập thành công

# CHƯƠNG V : SỬ DỤNG MÃ HÓA MD5 TRÊN VISUAL STUDIO CODE C# ĐỂ TẠO ĐĂNG KÝ , ĐĂNG NHẬP

1. **Tổng quan mã hóa MD5**

MD5 là một trong ba thuật toán mà Ronald Rivest đã tạo ra. Trong đó MD2 là hàm băm đầu tiên mà Ronald Rivest tạo ra vào năm 1989, được tích hợp trong các máy tính 8-bit. Mặc dù vẫn được sử dụng, nhưng MD2 không được áp dụng cho các ứng dụng yêu cầu độ bảo mật cao, hơn nữa MD2 đã được chứng minh là dễ bị tấn công.



Hình 21. Ronald Rivest người viết mật mã MD5

Sau đó 1 năm, MD4 ra đời vào năm 1990 để thay thế cho MD2. MD4 được tạo ra cho máy tính 32-bit và được đánh giá nhanh hơn rất nhiều so với MD2, nhưng cũng có các lỗ hổng và điểm yếu.

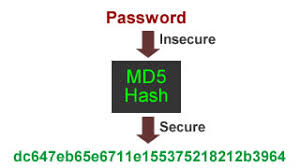
MD5 được phát hành vào năm 1992, và cũng được phát triển cho các máy tính 32-bit. Tuy MD5 không nhanh như MD4, nhưng được đánh giá là an toàn hơn so với các phiên bản MDx được triển khai trước đó.

Mặc dù được đánh giá là an toàn hơn MD2 và MD4, xong MD5 cũng được chứng minh có chứa các lỗ hổng bảo mật, người dùng được khuyến cáo sử dụng một số hàm băm khác như SHA-1 để thay thế.

Theo các nhà nghiên cứu thuộc trường Đại học Carnegie Mellon thuộc Viện Kỹ thuật phần mềm khuyến cáo: "các nhà phát triển phần mềm, nhà cung cấp chứng thực số (CA), chủ sở hữu trang web và người dùng nên hạn chế sử dụng thuật toán MD5. Các nghiên cứu trước đây chứng minh MD5 dễ bị phá vỡ về mặt mã hóa và không còn phù hợp để sử dụng".

1. **Ứng dụng của MD5**

MD5 là phần mềm được ứng dụng chủ yếu là để kiểm tra được mỗi tập tin khi tải về có toàn vẹn như được đưa lên trên mạng hay không. Bạn sẽ kiểm tra bằng cách so sánh mã MD5 của tập tin tải về với mã MD5 được ghi trên trang cung cấp tải tập tin.



Hình 22. Mã hóa MD5

Nếu không trùng khớp nghĩa là quá trình download đã bị lỗi khiến tập file của bạn không tải về được hoặc tải về không đầy đủ. Các tác giả đưa MD5 của tập tin lên nhằm tránh trường hợp bạn tải dữ liệu tại các địa chỉ không tin cậy có thể sẽ bị đính kèm các chương trình nhỏ nguy hại như trojan, keylogger… …Hiện nay MD5 được ứng dụng vào nhiều hệ thống bảo mật khác nhau. Ví dụ như Microsoft File Checksum Integrity Verifier, phần mềm MD5 Hash Generator.

1. **Thực hiện trên VISUAL STUDIO CODE C#**

Mô tả: Thực hiện tính năng đăng ký bằng cách mã hóa mật khẩu rồi lưu trong SQL

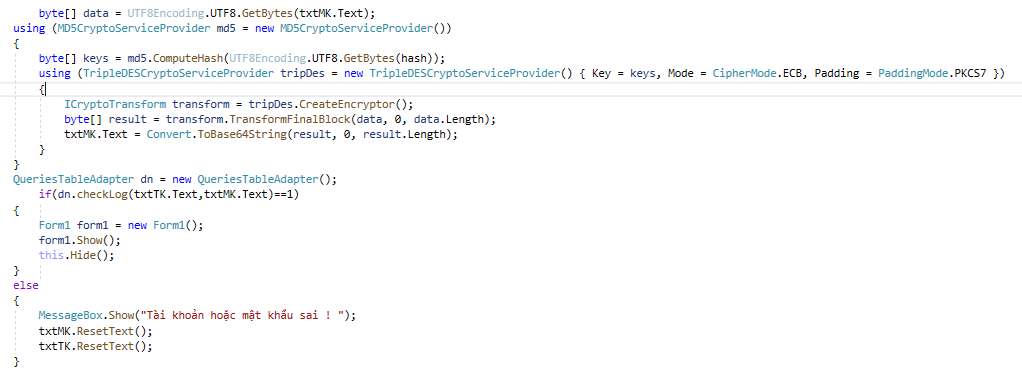


Hình 23. Đăng ký tài khoản



Hình 24. Mật khẩu được mã hóa lưu trong SQL

Mô tả :Thực hiện tính năng đăng nhập bằng cách mã hóa mật khẩu

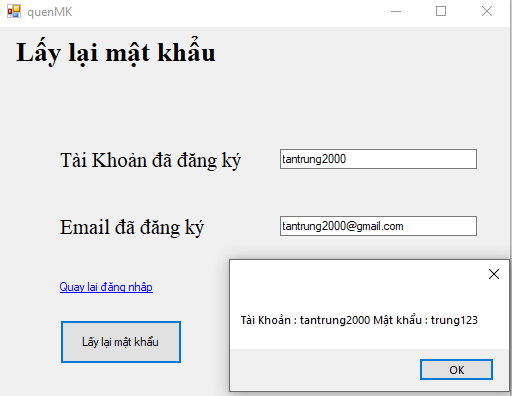


Hình 25. Đăng nhập tài khoản

Mô tả: Thực hiện tính năng quên mật khẩu bằng giải mã



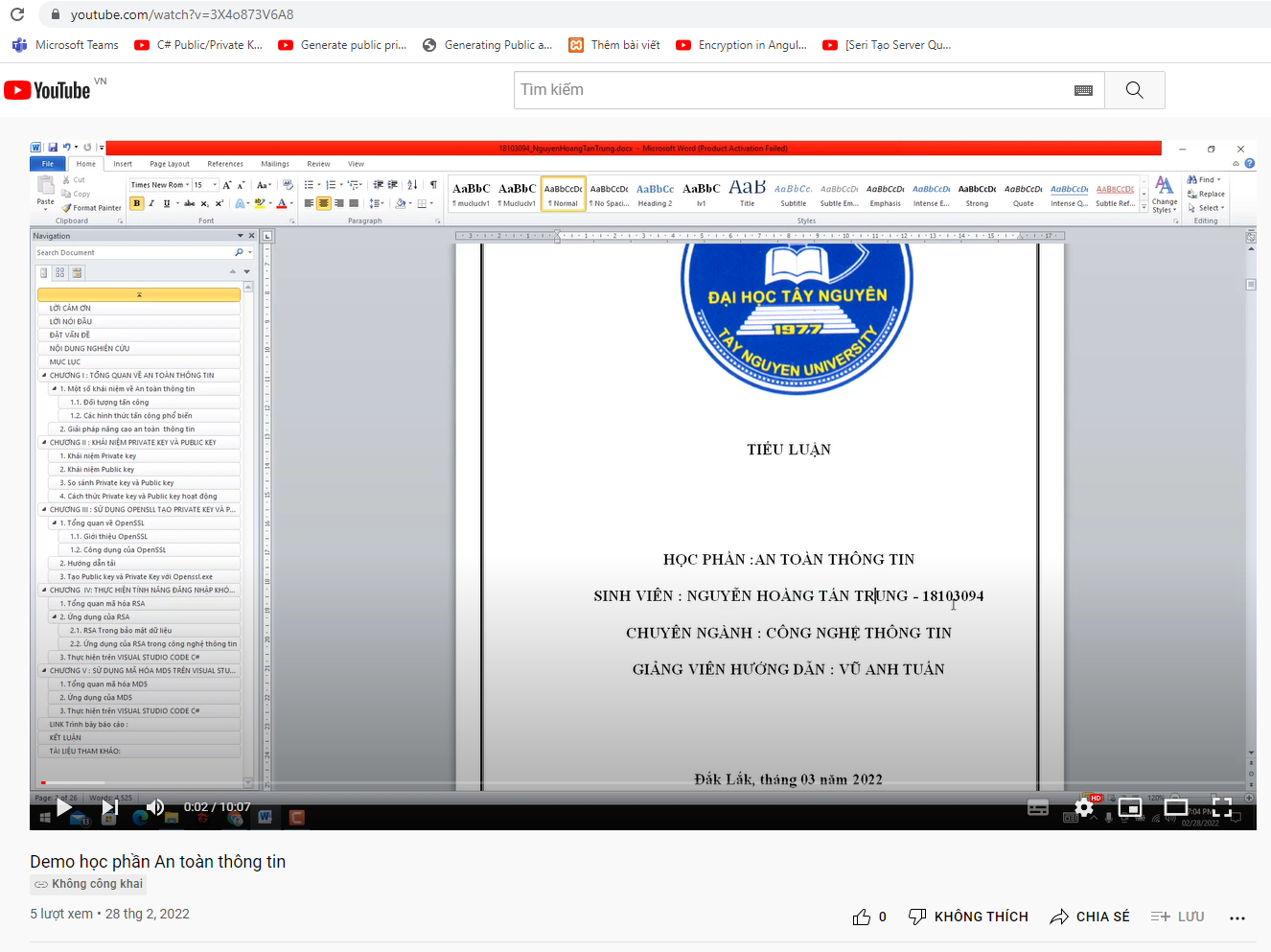
Hình 26. Quên mật khẩu



Hình 27. Kết quả thu được

# LINK Trình bày báo cáo

<https://www.youtube.com/watch?v=3X4o873V6A8>



Hình 28. Thuyết trình demo trên youtube

# KẾT LUẬN

Sự xuất hiện và ảnh hưởng rất lớn của công nghệ sẽ tác động mạnh mẽ đối với con người trong thời đại hiện nay. Công nghệ thông tin đã xuất hiện và chiếm một phần không nhỏ trong đời sống hiện đại, ảnh hưởng đến các ngành và lĩnh vực xã hội. Tuy nhiên, những thay đổi và phát triền Công nghệ thông tin, đặc biệt là sự ra đời của công nghệ 4.0 cũng đồng thời xuất hiện những mặt trái ,mặt tiêu cực trong việc truy cập và sử dụng các dịch vụ liên quan đến công nghệ. Từ đó cho thấy việc của chúng ta cần làm là ngăn chặn những kẻ xấu,hacker thực hiện đánh cắp dữ liệu, tài sản, thông tin cá nhân. Đây là việc vô cùng hệ trọng và cấp bách, vì mối nguy hiểm đối với mỗi tổ chức, cá nhân .Đó là một mối đe dọa tuy vô hình nhưng cực kỳ nguy hiểm, vì nó có khả năng đánh cắp thông tin cực kỳ cao. Chúng ta phải biết cách khôn khéo và tìm cách bảo vệ thông tin trước những phần tử nguy hại tiềm ẩn này.

# TÀI LIỆU THAM KHẢO

**[1]** **https://www.ssl2buy.com/wiki/what-is-a-public-and-private-key-pair**

**[2]** [**https://tailieuthamkhao.org/tieu-luan-mon-an-toan-an-ninh-thong-tin-de-tai-ma-hoa-du-lieu-va-xac-thuc-pgp-pretty-good-privacy-truong-dai-hoc-da-nang-99/**](https://tailieuthamkhao.org/tieu-luan-mon-an-toan-an-ninh-thong-tin-de-tai-ma-hoa-du-lieu-va-xac-thuc-pgp-pretty-good-privacy-truong-dai-hoc-da-nang-99/)

[3] ***Video tham khảo*. (2019). [Video]. YouTube.** [**https://www.youtube.com/watch?v=dSegZHJudLs&t=1943s**](https://www.youtube.com/watch?v=dSegZHJudLs&t=1943s)

**HẾT**