**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**======\*\*\*======**

****

BÁO CÁO BTL THUỘC HỌC PHẦN:

AN TOÀN VÀ BẢO MẬT THÔNG TIN

**Đề tài : XÂY DỰNG CÁC GIẢI PHÁP VỀ CHÍNH SÁCH ĐẢM BẢO AN TOÀN, AN TOÀN MẠNG VÀ HẠ TẦNG HỆ THỐNG QUẢN LÍ ĐIỀU HÀNH ĐÀO TẠO TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

Giáo viên hướng dẫn : ThS.TRẦN PHƯƠNG NHUNG

Nhóm thực hiện : Nhóm 14

Lớp : KTPM 2 Khóa : K12

Sinh viên thực hiện :

|  |  |
| --- | --- |
| **Mã sv** | **Họ và tên** |
| 2017604873 | Nguyễn Ngọc Vinh |
| 2017605870 | Lưu Tuấn Vũ |
| 2017604374 | Vũ Đức Vượng |
| 2017604545 | Nguyễn Thành Vy |
| 2017605046 | Nguyễn Thị Yến |

Hà nội, Năm 2020

Mục Lục

[Lời mở đầu 2](#_Toc43844857)

[Phần 1: Tổng quan về hệ thống 3](#_Toc43844858)

[1. Tìm hiểu về hệ thống 3](#_Toc43844859)

[1.1. Mô hình mạng Client – Server 3](#_Toc43844860)

[1.2. Mô hình mạng ngang hàng 3](#_Toc43844861)

[2. Chỉ định các chính sách, quy định, chỉ dẫn cần phải có trong hệ thống, nội dung dự kiến của văn bản 3](#_Toc43844862)

[3. Các văn bản chi tiết cho các chính sách, quy định, chỉ dẫn(Lưu Tuấn Vũ) 3](#_Toc43844863)

[4. Tìm hiểu các giải pháp an toàn mạng cho hệ thống mạng hỗ trợ quá trình hoạt động và điều hành (thiết bị, phần mềm, ...) 4](#_Toc43844864)

[4.1. Những nguy cơ gây nguy hiểm cho an toàn mạng 4](#_Toc43844865)

[4.2. Giải pháp cho phần cứng 4](#_Toc43844866)

[4.3. Giải pháp cho phần mềm 5](#_Toc43844867)

[4.4. Giải pháp an ninh cho lớp trung gian 6](#_Toc43844868)

[4.5. Giải pháp bảo mật hệ thống mạng thông qua firewall 6](#_Toc43844869)

[4.6. Những giải pháp bảo mật mạng khác không thể bỏ qua 7](#_Toc43844870)

[5. Các hạ tầng mạng 7](#_Toc43844871)

[Phần 2: Ứng dụng cài đặt minh họa 9](#_Toc43844872)

[1. ….. 9](#_Toc43844873)

[2. ….. 9](#_Toc43844874)

[3. Cài đặt minh họa các chính sách đảm bảo an toàn cho hệ thống(Lưu Tuấn Vũ) 9](#_Toc43844875)

[3.1. Lớp sử lý MyCrypto 9](#_Toc43844876)

[3.2. Lớp sử lý sự kiện 12](#_Toc43844877)

[3.3. Kết Quả 13](#_Toc43844878)

[4. ……… 14](#_Toc43844879)

[5. ….. 14](#_Toc43844880)

# Lời mở đầu

Với sự phát triển nhanh chóng của mạng internet và đặc biệt là các công nghệ mạng, kèm theo đó là các vấn đề bảo vệ các tài nguyên trên mạng, tránh sự mất mát, xâm nhập là việc cần thiết và cấp bách. Bảo mật mạng có thể hiểu là cách bảo vệ, đảm bảo an toàn cho các thành phần mạng bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng và đảm bảo mọi tài nguyên trên mạng tránh bị đánh cắp thông tin, đồng thời đảm bảo an toàn, an toàn mạng và hạ tầng quản lý của trường

Việc đảm bảo an toàn cho hệ thống cần đặt lên hàng đầu trước khi xây dựng một hệ thống cho mọi người sử dụng. Vậy nên việc sử dụng các thiết bị tường lửa trong hệ thống mạng để đảm bảo an toàn, an toàn mạng là rất cần thiết. Nhằm ngăn chặn các kết nối không mong muốn, giảm nguy cơ mất kiểm soát hệ thống hoặc tấn công và lây nhiễm các chương trình và mã độc hại.

Trong bài báo cáo này chúng em xin được trình bày nghiên cứu về vấn đề: *Xây dựng các giải pháp về chính sách đảm bảo an toàn, an toàn mạng và hạ tầng cho hệ thống quản lý điều hành đào tạo trường đại học Công nghiệp Hà Nội.* Dù đã cố gắng rất nhiều trong quá trình tìm hiểu, nghiên cứu và viết báo cáo, nhưng chắc chắn không thể tránh khỏi những hạn chế và thiếu sót. Chúng em rất mong được những ý kiến đóng góp và chỉ bảo thêm từ thầy cô giáo giúp cho bài tập lớn của nhóm chúng em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn ạ!

# Phần 1: Tổng quan về hệ thống

## Tìm hiểu về hệ thống

### Mô hình mạng Client – Server

* Mô hình mạng Client – Server: một mô hình thông dụng trong mạng máy tính bao gồm 2 thành phần chính là máy chủ server và máy khách client.
* Trong mô hình Client – Server thì Client là các máy tính, các thiết bị điện tử như máy in, máy fax… gửi yêu cầu đến Server và được tiếp nhận yêu cầu, xử lý các yêu cầu đó và trả về kết quả.
* Các hệ thống phù hợp với mô hình mạng này: hệ thống quản lý, …

### Mô hình mạng ngang hàng

* Mô hình mạng ngang hàng: một mạng máy tính mà hoạt động của nó chủ yếu dựa vào khả năng tính toán và băng thông của các máy tham gia chứ không tập trung vào một số nhỏ các máy chủ trung tâm như các mạng truyền thống thông thường.
* Trong mô hình này thì Client là các máy tính, các thiết bị điện tử như máy in, máy fax… gửi yêu cầu đến Server và được tiếp nhận yêu cầu, xử lý các yêu cầu đó và trả về kết quả.

## Chỉ định các chính sách, quy định, chỉ dẫn cần phải có trong hệ thống, nội dung dự kiến của văn bản

* Bảo mật tài khoản và phân quyền: sử dụng cách mã hóa MD5 cho mật khẩu của tài khoản.
* Phạm vi sử dụng cho mỗi loại tài khoản: ví dụ như giáo viên chỉ được quản lý thông tin sinh viên, nhập điểm và xem các chức năng khác trong phạm vi quyền sử dụng của giáo viên.
* Đối tượng sử dụng: đang công tác và hoạt động trong phạm vi của nhà trường như giáo viên, sinh viên, quản lý đào tạo, … Ngoài ra không ai có quyền xâm phạm vào thông tin có trên hệ thống.
* Lưu trữ thông tin: hệ thống cung cấp các dịch vụ dựa theo thông tin từ phía người dùng cung cấp.

## Các văn bản chi tiết cho các chính sách, quy định, chỉ dẫn(Lưu Tuấn Vũ)

* Chính sách, quy định, chỉ dẫn cần phải có:
* Bảo mật tài khoản và phân quyền: sử dụng cách mã hóa MD5 cho mật khẩu của tài khoản.
* Phạm vi sử dụng cho mỗi loại tài khoản: ví dụ như giáo viên chỉ được quản lý thông tin sinh viên, nhập điểm và xem các chức năng khác trong phạm vi quyền sử dụng của giáo viên.
* Đối tượng sử dụng: đang công tác và hoạt động trong phạm vi của nhà trường như giáo viên, sinh viên, quản lý đào tạo, … Ngoài ra không ai có quyền xâm phạm vào thông tin có trên hệ thống.
* Lưu trữ thông tin: hệ thống cung cấp các dịch vụ dựa theo thông tin từ phía người dùng cung cấp.

## Tìm hiểu các giải pháp an toàn mạng cho hệ thống mạng hỗ trợ quá trình hoạt động và điều hành (thiết bị, phần mềm, ...)

### Những nguy cơ gây nguy hiểm cho an toàn mạng

* Tấn công xâm nhập mạng từ bên trong nội bộ
* Đánh cắp dữ liệu
* Chèn mã độc, virus vào trong phần mềm, công cụ
* Mã độc lây nhiễm bắt nguồn từ Plug-in trình duyệt
* Thiết bị IoT (Internet of Things)

### Giải pháp cho phần cứng

* Là giải pháp sử dụng thiết bị phần cứng được tích hợp bộ định tuyến, các quy tắc cho việc lọc gói tin được thiết lập ngay trên bộ định tuyến đó. Tường lửa phần cứng này như một chiếc máy tính thực hiện chức năng lọc gói tin bằng cách chạy một phần mềm đã được cứng hóa trong đó. Tùy vào từng loại tường lửa phần cứng của các hãng khác nhau mà cho phép người quản trị có khả năng cập nhật những quy tắc lọc gói tin khác nhau.
* Sự đầu tư đúng đắn trước khi mua bất kỳ phần mềm hoặc công cụ nào đó phục vụ cho việc bảo mật.
* Nếu cần nâng cấp hệ thống, bạn hãy chọn những nhà cung cấp dịch vụ chuyên nghiệp và đã có kinh nghiệm lâu năm.
* Tăng cường sự bảo mật cho các thiết bị đầu vào và đầu ra. Ví dụ như USB, ổ cứng, ổ đĩa, …
* Tăng thêm lớp bảo mật cho hệ thống tường lửa.
* Mô hình Tường lửa phần cứng

Khi hoạt động, tường lửa sẽ dựa trên các quy tắc được thiết lập trong bộ định tuyến mà kiểm tra thông tin được gắn vào gói tin như địa chỉ nguồn, địa chỉ đích, cổng... Nếu mọi thông tin trong đó của gói tin là hợp lệ nó sẽ được cho qua và nếu không hợp lệ nó sẽ bị bỏ qua. Một số tường lửa phần cứng chuyên dụng như ASA của Cisco, hay NetScreen của Juniper.

- Ưu điểm của Tường lửa phần cứng

+ Là thiết bị riêng biệt chạy trên một hệ điều hành riêng của nhà cung cấp, do đó đảm bảo có khả năng bảo vệ hệ thống chống lại các cuộc tấn công từ bên ngoài.

+ Giúp giám sát và quản lý truyền tải dữ liệu ra và vào máy tính.

+ Tốc độ xử lí rất nhanh vì Tường lửa phần cứng hoạt động ở tầng thấp (tầng mạng trong mô hình mạng hay còn gọi mô hình OSI gồm 7 tầng), sẽ lọc các gói tin ở tầng này dựa trên các địa chỉ mạng gửi đi hay đích đến mà không quan tâm đến việc nó thuộc ứng dụng gì.

- Nhược điểm của Tường lửa phần cứng

+ Không được linh hoạt vì thiết bị được thiết kế theo 1 tiêu chuẩn nhất định nên khả năng thêm chức năng, thêm quy tắc rất hạn chế, có khi không thực hiện được mà chỉ sử dụng những chức năng, quy tắc được lập trình ngay từ đầu.

+ Không thể kiểm tra được nội dung của gói tin.

+ Không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Nghĩa là, không thể chống lại một cuộc tấn công từ một đường truyền riêng, hoặc sự rò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

+ Chi phí cao, để sở hữu một hệ thống Tường lửa phần cứng đảm bảo thì kính phí đầu tư rất lớn, từ khoảng 250.000.000đ trở lên.

### Giải pháp cho phần mềm

- Các phương pháp xác thực hay các phương pháp mã hoá: Phương pháp này đảm bảo cho thông tin truyền trên mạng một cách an toàn nhất. Vì với cách thức làm việc của nó, thông tin thật trên đường truyền được mã hoá dưới dạng mà những kẻ “nhòm trộm” không thể thấy được hoặc nếu thông tin bị sửa đổi thì tại nơi nhận sẽ có cơ chế phát hiện sự sửa đổi đó.

- Phương pháp bức tường lửa hay mạng riêng ảo: Phương pháp này đảm bảo an ninh ở góc độ khác. Bằng cách thiết lập các luật tại một điểm đặc biệt (thường gọi là điểm nghẹt) giữa hệ thống mạng bên trong (mạng cần bảo vệ) với hệ thống mạng bên ngoài (mạng được coi là không an toàn về bảo mật - hay là internet). Hệ thống bức tường lửa hoàn toàn có thể kiểm soát các kết nối trao đổi thông tin giữa hai mạng.

* Mô hình Tường lửa phần mềm

Hiện nay, một số tường lửa mềm thông dụng, như: Zone Alarm, Microsoft ISA Server, Norton Firewall, …

* Ưu điểm của tường lửa phần mềm:

+ Tính linh hoạt cao: Có thể thêm, bớt các quy tắc, các chức năng tùy theo nhu cầu cụ thể của từng đơn vị.

+Tường lửa phần mềm hoạt động ở tầng ứng dụng cao hơn Tường lửa phần cứng. Vì vậy có thể kiểm tra được nội dung của gói tin (thông qua các từ khóa được quy định trong quy tắc đã thiết lập trong tường lửa).

+Chi phí thấp: Giải pháp Tường lửa phần mềm chỉ là các chương trình máy tính được cài đặt trên các Server, do đó chi phí cho giải pháp này sẽ ít hơn so với giải pháp sử dụng Tường lửa phần cứng, phù hợp cho những tổ chức, cơ quan có nguồn kinh phí sử dụng cho ứng dụng công nghệ thông tin ít, hạn chế.

* Nhược điểm của tường lửa phần mềm:

+Không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, không thể chống lại một cuộc tấn công từ một đường truyền riêng, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

+Tường lửa phần mềm cũng không thể chống lại các cuộc tấn công bằng dữ liệu hay khi thực hiện nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, vì phụ thuộc vào tốc độ làm việc, sự xuất hiện liên tục của các virus mới, các cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát như chuyển theo thư điện tử, vượt qua tường lửa vào trong mạng được bảo vệ.

+ Không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Tường lửa phần mềm chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

### Giải pháp an ninh cho lớp trung gian

* Hạn chế sự truy cập trái phép qua Access Control và nâng cao sự bảo mật thông qua strong password, username.
* Ngăn chặn những kết nối trái phép thông qua kết nối vật lý như: port security, VLAN access control list trong thiết bị mạng.
* Hạn chế sự tràn ngập dữ liệu từ khu này đến khu khác, đảm bảo sự lưu thông mạng luôn được duy trì giúp khách hàng dễ dàng truy cập vào hệ thống website.

### Giải pháp bảo mật hệ thống mạng thông qua firewall

* Firewall là lớp bảo mật tuyệt vời đối với mọi hệ thống mạng doanh nghiệp.
* Firewall hay còn gọi là tường lửa sẽ giúp ngăn chặn những nguy cơ tấn công mạng xâm nhập từ bên ngoài hệ thống, ngăn chặn virus.
* Tuy nhiên, những hacker giỏi hoàn toàn có thể vượt qua hệ thống tường lửa của doanh nghiệp bạn một cách dễ dàng. Nhưng việc thực hiện giải pháp bảo mật này sẽ tốt hơn là không thực hiện.

### Những giải pháp bảo mật mạng khác không thể bỏ qua

1. Sử dụng phần mềm diệt virus cho máy trạm end- user

* Đây là thành phần không thể thiếu đối với bất kỳ hệ thống mạng hay hệ thống website nào.

1. Rà quét lỗ hổng thường xuyên

* Bạn cần thực hiện việc rà quét lỗ hổng 1 cách thường xuyên. Thay vì sử dụng phần mềm diệt virus miễn phí, bạn nên đăng ký gói dịch vụ đánh giá an ninh mạng của những công ty lớn thì sẽ tốt hơn.

1. Giải pháp chống mất dữ liệu

* Xác định các dữ liệu quan trọng
* Giám sát truy cập và hoạt động
* Sử dụng mã hóa
* Khóa mạng
* An ninh điểm cuối

1. Xây dựng chính sách an toàn thông tin toàn diện cho doanh nghiệp

Nhiều người cho rằng việc đảm bảo ATTT thuộc về đội ngũ kỹ thuật. Thực tế, điều này phải có sự kết hơp giữa đội ngũ kỹ thuật và những người quản lý. Nếu doanh nghiệp xây dựng một chính sách an ninh toàn diện cho cả người dùng và thiết bị, cho cả hiện tại và tương lai thì sẽ không bao giờ lo lắng trước những nguy cơ tấn công mạng.

1. Xây dựng các lớp bảo mật cho hạ tầng mạng

Quý khách có thể nâng cấp thiết bị, phần mềm, công cụ liên quan tới hệ thống mạng và website. Ví dụ như, nâng cấp phần mềm theo dõi hệ thống mạng, tăng cường bảo mật cho phần mềm quản trị website…

Nhằm tăng cường hiệu suất của hệ thống mạng và tiết kiệm chi phí tối đa, SecurityBox sẽ tư vấn quý khách hàng những giải pháp an ninh thông tin cho cơ sở hạ tầng đáp ứng linh hoạt hoạt động kinh doanh của tổ chức, doanh nghiệp tại thị trường Việt Nam.

## Các hạ tầng mạng

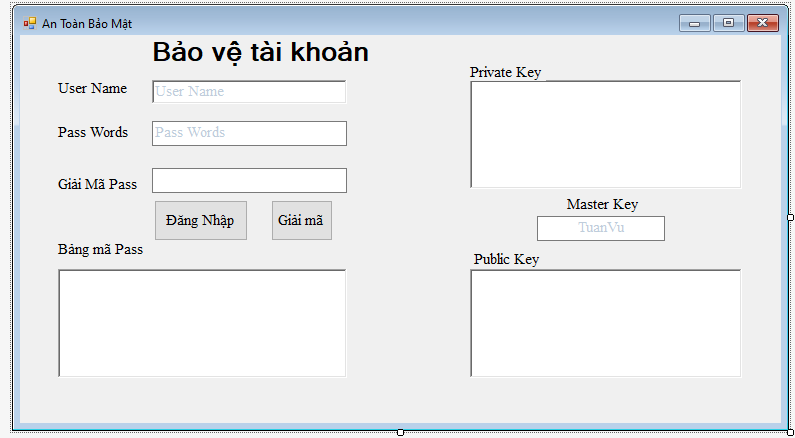
* **Xác định các nguy cơ gây nguy hiểm cho an toàn mạng**
* Tấn công xâm nhập mạng từ bên trong và bên ngoài nội bộ
* Đánh cắp dữ liệu, chèn mã độc, virus vào trong phần mềm, công cụ
* **Giải pháp cho phần cứng**
* Sự đầu tư có chọn lọc trước khi mua bất kỳ phần mềm hoặc công cụ nào đó phục vụ cho việc bảo mật.
* Khi nâng cấp hệ thống, chọn nhà cung cấp dịch vụ có uy tín
* Nâng cấp bảo mật cho các thiết bị đầu vào và đầu ra. Ví dụ như cổng cắm USB, ổ cứng, ổ đĩa, …
* Tăng thêm độ bảo mật cho hệ thống tường lửa.
* **Giải pháp an ninh cho lớp trung gian**
* Hạn chế sự truy cập trái phép qua Access Control và nâng cao sự bảo mật thông qua tài khoàn.
* Ngăn chặn những kết nối trái phép thông qua kết nối vật.
* Hạn chế sự tràn ngập dữ liệu từ khu này đến khu khác, đảm bảo sự lưu thông mạng luôn được duy trì giúp khách hàng dễ dàng truy cập vào hệ thống website.
* **Giải pháp chống mất dữ liệu**
* Thường xuyên sao lưu, bảo trì và nâng cấp máy chủ để hạn chế bị tấn công và nâng cấp trải nghiệm người dùng khi vào giờ cao điểm

# Phần 2: Ứng dụng cài đặt minh họa

## …..

## …..

## Cài đặt minh họa các chính sách đảm bảo an toàn cho hệ thống(Lưu Tuấn Vũ)



Hình 1 : Giao diện mô phỏng

### Lớp sử lý MyCrypto

#### Hàm AssignNewKey

Hàm này tạo 1 khóa mới từ 1 chuỗi ký tự được chuyền vào

public class MyCrypto

{

RSACryptoServiceProvider RSA = null;

public string PrivateKeyXML;

public string PublicOnlyKeyXML;

public void AssignNewKey(string keymaster)

{

const int PROVIDER\_RSA\_FULL = 1;

string CONTAINER\_NAME = keymaster;

CspParameters cspParams;

cspParams = new CspParameters(PROVIDER\_RSA\_FULL);

cspParams.KeyContainerName = CONTAINER\_NAME;

cspParams.Flags = CspProviderFlags.UseMachineKeyStore;

cspParams.ProviderName = "Microsoft Strong Cryptographic Provider";

RSA = new RSACryptoServiceProvider(cspParams);

//Pair of public and private key as XML string.

//Do not share this to other party

PrivateKeyXML = RSA.ToXmlString(true);

//Private key in xml file, this string should be share to other parties

PublicOnlyKeyXML = RSA.ToXmlString(false);

}

* + 1. **Hàm Mã Hóa Encryp**

public byte[] Encrypt(string publicKeyXML, string dataToDycript)

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicKeyXML);

return rsa.Encrypt(ASCIIEncoding.ASCII.GetBytes(dataToDycript), true);

}

public string Encrypt\_string(string publicKeyXML, string dataToDycript)

{

try

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicKeyXML);

string EncryptedResult = System.Convert.ToBase64String(rsa.Encrypt(System.Text.Encoding.Unicode.GetBytes

(dataToDycript), true));

return EncryptedResult;

}

catch

{

return "Mã hóa thất bại";

}

}

* + 1. **Hàm Giải Mã Decrypt**

public string Decrypt(string publicPrivateKeyXML, byte[] encryptedData)

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicPrivateKeyXML);

return ASCIIEncoding.ASCII.GetString(rsa.Decrypt(encryptedData, true));

}

public string Decrypt\_string(string publicPrivateKeyXML, string encryptedData)

{

try

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicPrivateKeyXML);

byte[] toDecryptData = System.Convert.FromBase64String(encryptedData);

return System.Text.Encoding.Unicode.GetString(rsa.Decrypt(toDecryptData, true));

}

catch {

return "Giải mã thất bại"; ;

}

}

* + 1. **Hàm sử lý chuỗi nhị phân**

public static string ByteArrayToHexString(byte[] Bytes)

{

StringBuilder Result = new StringBuilder(Bytes.Length \* 2);

string HexAlphabet = "0123456789ABCDEF";

foreach (byte B in Bytes)

{

Result.Append(HexAlphabet[(int)(B >> 4)]);

Result.Append(HexAlphabet[(int)(B & 0xF)]);

}

return Result.ToString();

}

* + 1. **Hàm sử lý chuỗi thập lục phân**

public static byte[] HexStringToByteArray(string Hex)

{

byte[] Bytes = new byte[Hex.Length / 2];

int[] HexValue = new int[] { 0x00, 0x01, 0x02, 0x03, 0x04, 0x05,

0x06, 0x07, 0x08, 0x09, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,

0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F };

for (int x = 0, i = 0; i < Hex.Length; i += 2, x += 1)

{

Bytes[x] = (byte)(HexValue[Char.ToUpper(Hex[i + 0]) - '0'] << 4 |

HexValue[Char.ToUpper(Hex[i + 1]) - '0']);

}

return Bytes;

}

### Lớp sử lý sự kiện

public partial class FormMain : Form

{

public FormMain()

{

InitializeComponent();

}

MyCrypto ATBM\_RSA = new MyCrypto();

private void Form2\_Load(object sender, EventArgs e)

{

ATBM\_RSA.AssignNewKey(txtMasterKey.Text);

}

private void btnLogin\_Click(object sender, EventArgs e)

{

if (txtUser.Text == "" || txtUser.Text.Length <= 3|| txtUser.Text == "User Name"||

txtPassWords.Text == "" || txtPassWords.Text.Length < 6||

txtPassWords.Text == "Pass Words")

{ txtMasterKey.Text = "Nhập đủ thông tin"; }

else {

txtMasterKey.Text = txtUser.Text.Substring(0, 4);

ATBM\_RSA.AssignNewKey(txtMasterKey.Text);

txtPublicKey.Text = ATBM\_RSA.PublicOnlyKeyXML;

txtPrivateKey.Text = ATBM\_RSA.PrivateKeyXML;

txtBangmaE.Text = ATBM\_RSA.Encrypt\_string(txtPublicKey.Text, txtPassWords.Text);

} }

private void txtGiaima\_Click(object sender, EventArgs e)

{

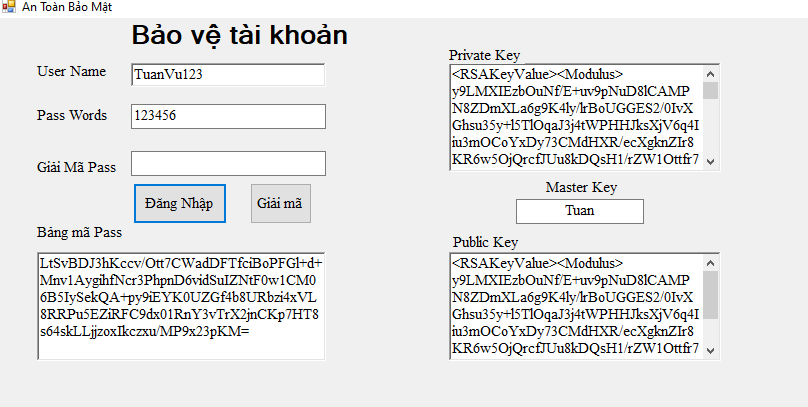
txtBangroD.Text = ATBM\_RSA.Decrypt\_string(txtPrivateKey.Text, txtBangmaE.Text);}

}

### **Kết Quả**

* + 1. **Kết quả khi nhấn “đăng nhập”**

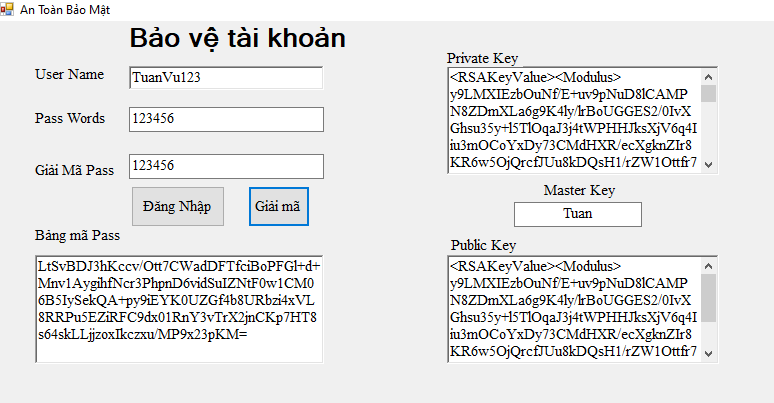
Hệ thống sẽ tự sinh khóa từ chuỗi gồm 4 kí tự đầu của tên tài khoản, Mật khẩu được mã hóa từ khóa được sinh trước khi gủi về Server bằng thuật toán RSA



Hình : kết quả thực hiện 1

* + 1. **Kết quả khi nhấn “giải mã”**

Hệ thống tiến hành giải mã từ bảng mã của Mật khẩu . được mật khẩu và lưu vào CSDL



1. **………**
2. **…..**