**TRƯỜNG ĐẠI HỌC LÂM NGHIỆP**

**KHOA KINH TẾ VÀ QUẢN TRỊ KINH DOANH**

**========&&&=======**



**BÁO CÁO ĐỀ TÀI BẢO MẬT ĐƯỜNG TRUYỀN MÁY ATM**

**Môn: An toàn bảo mật thông tin**

|  |  |
| --- | --- |
| **Thành viên:** | **Bùi Thị Mai** |
|  | **Hán Lan Hoài** |

**Hà Nội, 2023**

MỤC LỤC

[**Lời mở đầu** 3](#_Toc137601535)

[**Chương 1: Tổng quan vấn đề nghiên cứu** 4](#_Toc137601536)

[**1.Tình hình sử dụng máy atm và những việc làm của thế giới trước vấn đề bảo mật máy atm** 4](#_Toc137601537)

[**2. Một số những vấn đề khó khăn** 5](#_Toc137601538)

[**Chương 2: Nội dung thực hiện** 6](#_Toc137601539)

[***Phương án 1*: Sử dụng thuật toán AES** 6](#_Toc137601540)

[***Phương án 2*: Sử dụng thuật toán DES** 8](#_Toc137601541)

[***Phương án 3*: Sử dụng thuật toán RSA** 10](#_Toc137601542)

[**Chương 3: Kết quả thực hiện** 11](#_Toc137601543)

[**Chương 4: Kết luận, kiến nghị** 13](#_Toc137601544)

[***Tài liệu tham khảo*** 14](#_Toc137601545)

# **Lời mở đầu**

Hiện nay khắp mọi nơi trên các thành phố hay địa phương sự xuất hiện của cây ATM đã quá quen thuộc với người dân, cây ATM là loại máy giao dịch rút tiền tự động, đó là một thiết bị ngân hàng giao dịch tự động, với những tiện ích đó nên cây ATM rất được sự quan tâm để phát triển hệ thống ngày một tốt hơn, với hoạt động của cây ATM theo quy định thì phải thực hiện việc báo cáo tình hình hoạt động ATM của tổ chức cung ứng dịch vụ thanh toán

Máy rút tiền tự động hay máy giao dịch tự động (còn được gọi là ATM, viết tắt của Automated Teller Machine hoặc Automatic Teller Machine trong tiếng Anh) là một thiết bị ngân hàng giao dịch tự động với khách hàng, thực hiện việc nhận dạng khách hàng thông qua thẻ ATM (thẻ ghi nợ, thẻ tín dụng) hay các thiết bị tương thích, và giúp khách hàng kiểm tra tài khoản, rút tiền mặt, chuyển khoản, thanh toán tiền hàng hóa dịch vụ. Các ngân hàng thường đặt số lượng lớn cây ATM khắp nơi để nâng cao dịch vụ, tăng cường cơ hội thị trường và giảm chi phí lao động. ATM cho phép khách hàng truy cập và thực hiện các giao dịch ngân hàng mọi lúc. Bên cạnh sự thuận tiện đó cũng có những rủi ro an ninh tiềm ẩn.

Vấn đề đặt ra là làm thế nào để đảm bảo an toàn tuyệt đối cho hệ thống và cả người dùng, chống lại mọi sự gian lận, ăn cắp tài khoản… của người dùng.

Với vấn đề trên em chọn đề tài là “bảo mật đường truyền máy atm” nhằm mục đích nâng cao độ an toàn và tính bảo mật đường truyền của máy atm.

Ngoài lời mở đầu, tài liệu tham khảo, luận văn gồm có 4 chương:

Chương 1: Tổng quan vấn đề nghiên cứu

Chương 2: Nội dung thực hiện

Chương 3: Kết quả thực hiện

Chương 4: Kết luận, kiến nghị

Tuy nhiên, do trình độ hạn chế và các tài liệu tham khảo lại không nhiều do đó trong báo cáo đồ án của em chắc chắn còn nhiều khiếm khuyết, em rất mong được sự chỉ bảo của thầy để đồ án của em được hoàn thiện hơn. Em xin chân thành cảm ơn!

# 

# **Chương 1: Tổng quan vấn đề nghiên cứu**

1. **Tình hình sử dụng máy atm và những việc làm của thế giới trước vấn đề bảo mật máy atm**

ATM ngày nay là thiết bị để ngân hàng giao dịch tự động với chủ thẻ, thực hiện thông qua các loại thẻ ATM như thẻ ghi nợ, thẻ ghi có (thẻ tín dụng), và các loại thẻ khác, giúp chủ thẻ kiểm tra tài khoản, rút tiền mặt, chuyển khoản thanh toán hàng hóa, dịch vụ.

Thanh toán tiền qua hệ thống ATM đã phổ biến trên toàn thế giới và ở Việt  
Nam hệ thống ATM dần trở nên quen thuộc với mọi người dân.  
Năm 1993, thị trường thẻ Việt Nam mới xuất hiện những sản phẩm thẻ đầu  
tiên do Vietcombank phát hành, đến năm 1996 thì thị trưởng thẻ thực sự xuất hiện.  
Năm 1996, ngân hàng ngoại thương Vietcombank kết hợp cùng ngân hàng  
nhà nước triển khai lắp đặt 2 chiếc máy rút tiền tự động tại Hà Nội.  
Đến nay, chúng ta đã chứng kiến sự phát triển vượt bậc của thị trưởng thẻ và máy ATM tại Việt Nam: với hơn 20 ngân hàng thương mại phát hành Thẻ nội địa, trong đó có 8 Ngân hàng phát hành thẻ Quốc tế. Tại hội thảo Banking Việt Nam 2008 diễn ra tại Hà Nội, Ngân hàng nhà nƣớc đã công bố số liệu thống kê về thị trƣờng thẻ Việt Nam. Trong đó, tính đến quý I/2008, toàn thể hệ thống ngân hàng Việt Nam có hơn 4.500 máy rút tiền tự động ATM, gần 15000 điểm chấp nhận thẻ (POS) và phát hành hơn 10 triệu thẻ thanh toán.

Khi các mạng lưới ATM được mở rộng thì việc đảm bảo an toàn cho hệ thống ATM trở nên cấp thiết. Khi khách hàng chấp nhận thanh toán tiền qua hệ thống ATM thì có nghĩa là họ đã tin tưởng vào sự an toàn và tiện lợi mà hệ thống ATM mang lại, do đó việc đảm bảo an toàn thông tin trên hệ thống ATM rất quan trọng.

Nhiều chủ thẻ không thấy được tầm quan trọng của việc bảo mật những thông tin cá nhân của thẻ (như mã PIN) nên đã bị kẻ gian “nhìn trộm” mật mã, sau đó ăn cắp thẻ để thực hiện hành vi rút tiền/thanh toán bất hợp pháp. Không ít trường hợp, khách hàng bị mất thẻ ATM, giấy tờ tùy thân (CTM, Hộ chiếu,…) và bị kẻ gian tóm được từ đó rút hết tiền do chủ thẻ đã đặt mã PIN là những con số dễ nhớ như ngày sinh, số căn cước công dân…

Ngoài ra phát sinh các vấn đề mới, những thông tin dữ liệu nằm ở cơ sở dữ liệu hay đang truyền trên đường truyền có thể bị trộm cắp, làm sai lệch và có thể bị giả mạo.

Điều đó ảnh hưởng đến các công ty, các tổ chức hay cả một quốc gia. Những bí mật kinh doanh, tài chính là mục tiêu của các đối thủ cạnh tranh. Những thông tin ATM liên quan đến kinh tế và đó là thông tin rất nhạy cảm của ngân hàng do vậy việc đảm bảo an toàn an ninh thông tin trên đường truyền máy ATM đóng một vai trò đặc biệt quan trọng. Để giải quyết vấn đề trên, thì an toàn thông tin cho máy ATM được đặt ra cấp thiết.

Hiện nay thế giới đã thường xuyên đưa ra những cảnh báo về lừa đảo cùng với đó là các giải pháp cho ngân hàng , khách hàng để bảo mật thông tin một cách an toàn nhất.Bên cạnh đó sự an toàn của các giao dịch ATM dựa chủ yếu vào sự toàn vẹn của bộ xử lý cryptoprocessor: các máy ATM thường sử dụng các thành phần hàng hóa nói chung mà đôi khi không được coi là "hệ thống đáng tin cậy".

Mã hóa thông tin cá nhân, được yêu cầu bởi luật pháp ở nhiều khu vực tài phán, được sử dụng để ngăn chặn gian lận. Dữ liệu nhạy cảm trong các giao dịch ATM thường được mã hóa bằng DES, nhưng các bộ xử lý giao dịch hiện nay thường yêu cầu sử dụng Triple DES. Kỹ thuật Nạp khóa từ xa có thể được sử dụng để đảm bảo bí mật của quá trình khởi tạo khóa mã hóa trong máy ATM. Mã xác thực tin nhắn (MAC) hoặc MAC một phần cũng có thể được sử dụng để đảm bảo tin nhắn không bị giả mạo trong khi chuyển giữa ATM và mạng tài chính.

1. **Một số những vấn đề khó khăn**

Về bảo mật, an toàn và an ninh: Đặc điểm của các giao dịch ngân hàng kỹ thuật số thường qua hệ thống mạng, do đó khách hàng luôn có tâm lý phải đối mặt với những rủi ro như hacker, virus máy tính… Việc thực hiện các giao dịch qua mạng đem đến cho khách hàng sự thuận tiện và nhanh chóng, tuy nhiên, các giao dịch lại phụ thuộc vào công nghệ. Bảo mật, an ninh là một trong những vấn đề lớn nhất của ngân hàng kỹ thuật số. Cho dù sử dụng hình thức bảo mật nào thì vẫn có khả năng bị đánh cắp thông tin cá nhân bởi máy tính truy cập có thể bị cài những mã độc hại. Vấn đề này thường nằm ngoài tầm kiểm soát của ngân hàng vì bọn tội phạm luôn sử dụng nhiều chiêu thức mới nhằm lấy cắp thông tin khách hàng.

Sự gian lận: Gian lận là mối lo ngại chung khi sử dụng ngân hàng kỹ thuật số vì tính năng bảo mật, ví dụ như mật khẩu hoặc mã PIN có thể bị đánh cắp và sử dụng mà không thể xác định. Mọi người có thể ăn cắp mã PIN và sử dụng nó trực tuyến không cần sự cho phép của chủ sở hữu. Việc chuyển tiền cũng có thể xảy ra thông qua các trang web ngân hàng trực tuyến.

Ngày nay cùng với sự bùng nổ của internet, mobile, mạng xã hội… các dịch vụ ngân hàng hiện đại internet banking, mobile banking, SMS banking… bên cạnh những ưu điểm của ngân hàng kỹ thuật số mang lại cho khách hàng vẫn còn một số không ít khách hàng vẫn lo lắng và e ngại bởi do thiếu hiểu biết, sử dụng không đúng cách nên đã bị kẻ gian lợi dụng lừa đảo, gian lận thẻ tín dụng chiếm đoạt tiền.

Sự cố mạng và vấn đề kỹ thuật: Hệ thống mạng vẫn có những sự cố làm gián đoạn giao dịch hoặc “chập chờn” trong giao dịch; mạng lưới ATM và sự kết nối thanh toán thẻ qua POS của hệ thống ngân hàng chưa có được sự thống nhất. Một số vấn đề liên quan đến an toàn kỹ thuật vẫn khiến khách hàng không hài lòng như hiện tượng máy ATM bị rò điện, vấn đề bị ăn cắp thông tin sử dụng máy ATM. Dịch vụ viễn thông ngày càng xuất hiện thêm nhiều nhà cung cấp, nhưng chất lượng sử dụng chưa được bảo đảm. Tình trạng mất sóng, nghẽn mạng do quá tải còn thường xuyên xảy ra ảnh hưởng đến chất lượng của các dịch vụ. Dù các rủi ro, tổn thất này mới được ghi nhận ở quy mô và phạm vi nhỏ lẻ nhưng đang phần nào khiến cho một số bộ phận khách hàng có tâm lý hoang mang, lo sợ khi sử dụng dịch vụ. Do đó, việc sử dụng dịch vụ đúng cách, thực hiện đúng nguyên tắc về an toàn bảo mật, nắm rõ các chiêu trò lừa đảo của kẻ gian sẽ giúp phòng tránh hiệu quả các rủi ro để an tâm tận hưởng dịch vụ ngân hàng kỹ thuật số.

# **Chương 2: Nội dung thực hiện**

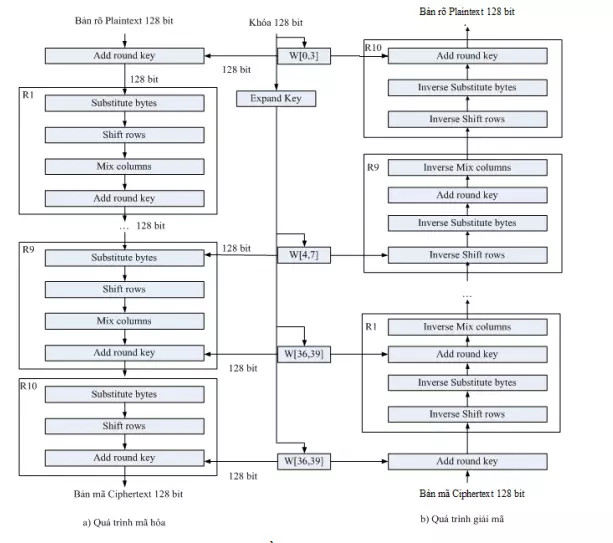
ATM được coi như là một máy PC trong hệ thống mạng. Do đó, cần có những giải pháp nhằm đảm bảo an toàn khi các giao dịch được thực hiện.

Để đảm bảo an toàn thông tin giao dịch trong quá trình truyền thông giữa ATM và Server, hệ thống phải mã hoá và giải mã thông tin giao dịch.

## ***Phương án 1*: Sử dụng thuật toán AES**

Thuật toán AES sử dụng cùng một khóa cho việc mã hóa và giải mã dữ liệu, là một dạng mã hóa đối xứng. AES hoạt động trên các khối dữ liệu có kích thước cố định (128 bit) và có thể sử dụng các khóa với độ dài khác nhau (128, 192 hoặc 256 bit) để tăng cường tính bảo mật. Độ dài khóa được biểu diễn bằng Nk = 4, 6 hoặc 8 thể hiện số lượng các từ 32 bít (số cột) của khóa mã. Đối với thuật toán AES, số

vòng được thay đổi trong quá trình thực hiện thuật toán phụ thuộc vào kích cỡ khóa. Số vòng này được ký hiệu là Nr. Nr = 10 khi Nk = 4, Nr = 12 khi Nk = 6 và Nr = 14 khi Nk = 8



* Ưu điểm:

*Tính bảo mật cao*: AES là một thuật toán mã hóa đối xứng mạnh, có khả năng đảm bảo tính bảo mật cao trong việc mã hóa và giải mã dữ liệu.

*Tốc độ nhanh*: Thuật toán này có tốc độ mã hóa và giải mã rất nhanh, phù hợp với các ứng dụng đòi hỏi tốc độ cao như truyền dữ liệu qua mạng.

*Linh hoạt*: AES cũng có thể sử dụng các khóa với độ dài khác nhau (128, 192 hoặc 256 bit) để tăng cường tính bảo mật. Ngoài ra, thuật toán này có thể sử dụng trên các nền tảng phần cứng và phần mềm khác nhau.

*Chuẩn quốc tế*: AES là một chuẩn mã hóa quốc tế, được chấp nhận rộng rãi trên toàn cầu.

* Nhược điểm:

AES phụ thuộc vào độ dài khóa để đảm bảo tính bảo mật. Nếu khóa ngắn hoặc dễ đoán, AES có thể bị tấn công và dữ liệu có thể bị tiết lộ. AES cần sử dụng khóa an toàn để đảm bảo tính bảo mật. Nếu khóa bị mất hoặc rơi vào tay của kẻ xấu, dữ liệu có thể bị tiết lộ.

AES không thể đảm bảo tính bảo mật nếu hệ thống bị tấn công bởi các phương thức khác như tấn công mạng, tấn công từ chối dịch vụ (DoS), tấn công đánh cắp thông tin đăng nhập,...

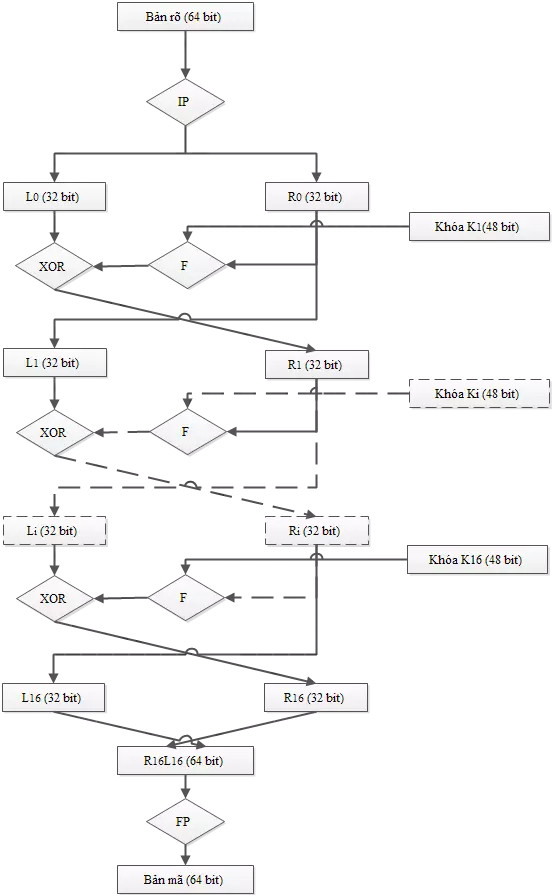
Ngoài ra việc triển khai AES có thể đòi hỏi chi phí phần cứng và phần mềm khá lớn để bảo vệ dữ liệu, đặc biệt là trong các hệ thống lớn và phức tạp.

## ***Phương án 2*: Sử dụng thuật toán DES**

DES là thuật toán mã hóa theo khối, nó xử lý từng khối thông tin của bản rõ có độ dài xác định là 64 bit. DES được thiết kế để mã hóa và giải mã các khối dữ liệu 64 bít với một khóa có độ dài 64 bít. Việc giải mã phải được thực hiện bởi một khóa tương ứng như trong quá trình mã hóa, mỗi khóa gồm 64 bít, trong đó 56 bít được sử dụng để thực hiện mã hóa/giải mã trong thuât toán. 8 bít còn lại được dùng để kiểm tra/phát hiện lỗi.

Mã hóa DES được thực hiện qua 16 vòng. Thông tin đầu vào là 64 bít, sẽ được chia thành 2 khối (block) trái (L) và phải (R). Sau đó từ khóa (56 bít) người ta tạo ra các khóa con (subkey) 48 bít gọi là Ki. Hàm f ở trên thực chất là 1 hàm hoán vị.

Trong quá trình mã hóa, dữ liệu đầu vào phải thực hiện quá trình hoán vị đầu (initial permutation) và hoán vị cuối (final permutation) sau vòng thứ 16. Việc thực hiện hoán vị phục vụ cho quá trình đưa thông tin vào và lấy thông tin ra từ các khối phần cứng, tạo điều kiện cho việc cài đặt phần cứng. Hàm cơ sở f cho phép đảm bảo tính bảo mật trong thuật toán DES này. Việc thực hiện nhiều lần các bước lặp với tác dụng của f là nhằm tăng cường tính phi tuyến và tính khuếch tán đã có trong hàm f.



* Ưu điểm: Thuật toán mã hoá DES tốc độ mã hoá dữ liệu rất nhanh, có thể triển khai trên thiết bị có kích thước nhỏ.
* Nhược điểm: Do DES có kích cỡ của không gian khoá 256 là quá nhỏ, không đủ an toàn, cho nên những máy có mục đích đặc biệt có thể sẽ bẻ gãy và dò ra khoá rất nhanh.

## 

## ***Phương án 3*: Sử dụng thuật toán RSA**

Thuật toán RSA sử dụng hai key khác nhau là public key (khóa công khai) và private key (khóa riêng tư) để mã hoá và giải mã. Public key có thể được chia sẻ với mọi người, riêng private key thì cần phải giữ bí mật.

* Ưu điểm:

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.

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.

* Nhược điểm:

RSA được bảo mật phần lớn phụ thuộc vào chính khả năng phân tích thừa số nguyên tố từ những giá trị lớn lý do vì chúng ta cung cấp rộng rãi chế độ public cho nên theo logic, nếu như việc phân tích các thừa số nguyên tố trở nên quá dễ dàng thì đương nhiên, các private bị lộ cũng dễ dàng, khiến cho RSA không thể bảo mật được.

Sau khi tìm hiểu và thử qua các phương án trên, nhóm em quyết định chọn phương án 3: sử dụng thuật toán RSA

* Phương án sử dụng thuật toán AES được lập trình chủ yếu bằng ngôn ngữ HTML nhưng với trình độ và lượng kiến thức về ngôn ngữ HTML để thực hiện thì nhóm em còn rất hạn chế, chưa thành viên nào nắm được
* Phương án sử dụng thuật toán DES là một phương án bảo mật tốt và thường được sử dụng trong bảo mật hệ thống atm và ngân hàng, tuy nhiên nhóm em gặp khó khăn khi làm mô phỏng bảo mật.
* Phương án sử dụng thuật toán RSA

+ Quy tắc mã hoá và giải mã dễ hiểu

+ Mô phỏng dễ dàng hơn, ngôn ngữ chủ yếu sử dụng là C#, việc thiết lập form cũng dễ hơn so với hai phương án trên

# **Chương 3: Kết quả thực hiện**

Public/private key program Public/private key program

Tương tác

client

Server

Để mã hoá được thì phải cần public key và private key.

Khi server có public key của client, server có thể sử dụng key đó để mã hóa dữ liệu muốn bảo mật. Khi nó đã được mã hóa bằng public key, nó chỉ có thể được giả mã bằng private key từ cùng một cặp key. Và ngược lại, client có public key của server, client cũng có thể sử dụng public key đó để mã hoá dữ liệu, và để giải mã được thì phải sử dụng private key của cặp key.

Encrypt thì phải có public key và chuỗi cần mã hoá.

Không thể mã hoá nguyên chuỗi ban đầu được mà chỉ mã hoá được các mảng byte

Quy trình mã hoá:

- Encryptor chỉ có public key của chính nó. Có thể nạp public key hoặc sử dụng public key từ chính nó → encryptor có public key

- Mã hoá data dựa trên public key đó. Do encrypt chỉ làm việc với mảng byte nên chuyển từ chuỗi ban đầu thành mảng byte. Lấy mảng byte vừa chuyển mã hoá với public key đã nạp.

- Encrypt xong sẽ trả về mảng byte mới

- Muốn người dùng đọc được text đã được mã hoá phải chuyển về dạng base64

Thay vì server sử dụng public key của nó để mã hoá thì nó sử dụng public key của client để mã hoá. Để giải mã thì phải sử dụng private key của client để giải.

Quy trình giải mã:

* Chuyển ngược từ chuỗi base64 về mảng byte
* Nạp private key để giải mã
* Decrypt xong sẽ nhận về mảng byte mới
* Sau đó chuyển thành dạng có thể đọc được (chuỗi ban đầu)

Client sẽ tương tác với server qua môi trường mạng.

Client ---------mạng--------- Server

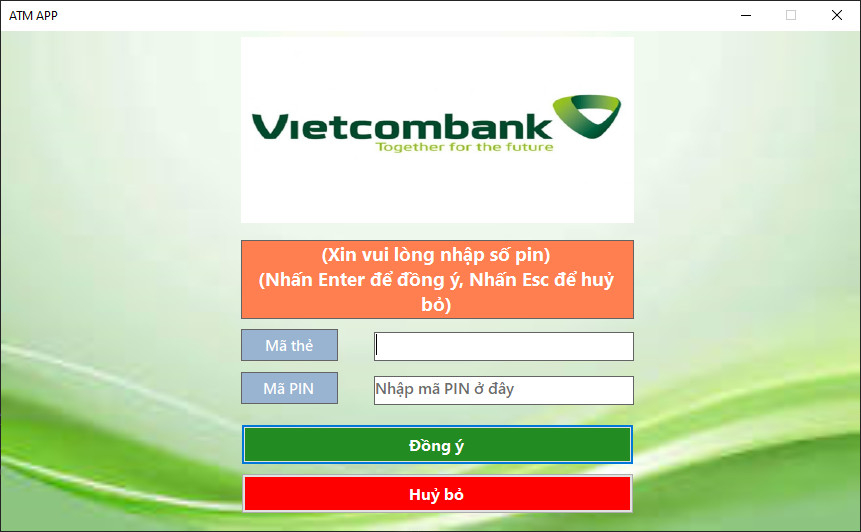
Client sẽ gửi http request tới server

Server sẽ gửi http reponse tới client

Client API Database

Client không thể tác động trực tiếp vô database nên client sẽ tác động thông qua API rồi mới tác động vô database. API sẽ kiểm tra lại dữ liệu thêm một lần nữa trước và phân quyền người dùng khi cho vào database.

Giao diện được tạo ra từ winform c#



Kết quả đã thực hiện được: Chương trình đã mã hoá đươc thông tin truyền qua truyền về giữa client và server

# **Chương 4: Kết luận, kiến nghị**

Việc bảo mật là rất quan trọng trong thời đại chuyển đổi số hiện nay. Tình hình bảo mật thông tin ngày càng trở nên phức tạp và khó khăn hơn do sự phát triển của công nghệ thông tin. Việc bảo mật ATM giúp ngăn chặn các hành vi lừa đảo và tấn công mạng vào các thông tin cá nhân và tài khoản ngân hàng của khách hàng. Ngoài ra, việc bảo mật ATM còn giúp ngăn chặn các hành vi xâm phạm quyền riêng tư của khách hàng. Nhận thức được tầm quan trọng đó chúng em đã nghiên cứu, thực hiện bảo mật đường truyền của máy atm. Với phương pháp sử dụng thuật toán RSA, tuy không phải là phương án tối ưu nhất nhưng lại là phương án phù hợp nhất với điều kiện kiến thức hiện tại mà nhóm chúng em có. Hơn nữa, 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. Không chỉ vậy, bảo mật tốt còn giúp phía ngân hàng thu hút nhiều khách hàng sử dụng dịch vụ, tăng sự uy tín của ngân hàng đối với khách hàng tham gia sử dụng dịch vụ ngân hàng.

Trong quá trình thực hiện đề tài chúng em có gặp một số khó khăn như không có nhiều tài liệu, hạn chế về kiến thức chuyên ngành chưa được học và những thử nghiệm các phương án thất bại, nhưng lại giúp chúng em trau dồi thêm được các kiến thức bảo mật và nhận thức thêm được tầm quan trọng của việc bảo mật trong thời đại bùng nổ công nghệ thông tin như hiện nay.

* Phần mềm chạy trên window
* Môi trường code là dotnet 6.0

Link tải: dotnet-sdk-6.0.408-win-x64.exe

* Phần mềm hỗ trợ cơ sở dữ liệu là SQL server

# ***Tài liệu tham khảo***

DES (mã hóa) - Bách khoa toàn thư mở Wikipedia

AES (mã hóa) - Bách khoa toàn thư mở Wikipedia

RSA (mã hóa) - Bách khoa toàn thư mở Wikipedia

Báo Tin học và Tài chính - *Bộ tài chính số 58, tháng 4/2008* Sự hình thành và phát triển của máy ATM

Giáo trình môn an toàn và bảo mật thông tin (*Đại học Thương Mại, Đại học Thuỷ Lợi*)

NCR – MICROTEC (2007), Tài liệu giới thiệu hệ thống máy ATM

Đề tài: tìm hiểu vấn đề bảo mật thông tin trên hệ thống ATM  
(Automatic Teller Machine) (Luận văn tốt nghiệp trường đại học quản lý và công nghệ Hải Phòng - 2010)