LỜI CẢM ƠN

-------o0o-------

Em xin gửi lời biết ơn sâu sắc tới thầy giáo Ths. Nguyễn Trịnh Đông. Thầy đã rất nhiệt tình hướng dẫn và giúp đỡ em trong suốt quá trình làm Đồ Án tốt nghiệp.

Đồng thời em xin chân thành cảm ơn các Thầy Cô giáo khoa Công nghệ thông tin, những người đã tận tình chỉ dạy cho em trong suốt quá trình học tập tại trường.

Xin gửi lời cảm ơn đến những người thân và bạn bè đã tạo điều kiện cũng như giúp đỡ và động viên mình trong suốt quá trình thực hiện luận văn này.

Em xin chân thành cảm ơn !

Sinh viên

Đàm Quang Trung

MỤC LỤC

Tiêu đề

LỜI GIỚI THIỆU

Công nghệ thông tin đang dần trở thành một phần quan trọng trong cuộc sống và các ứng dụng của công nghệ đang bao trùm hầu hết các lĩnh vực trong cuộc sống của con người, trong đó lĩnh vực tài chính, ngân hàng cũng có nhiều chuyển biến do tiếp thu các ứng dụng của công nghệ thông tin vào công tác quản lý, giao dịch với khách hàng.

Một trong những công cụ góp phần rất lớn vào công cuộc đổi mới đó là máy ATM. Xuất hiện năm 1939 tại Thành phố New York thuộc Hoa kỳ, ATM không ngừng phát triển và đổi mới tới nay máy ATM đã được sử dụng phổ biến ở hầu khắp các ngân hàng trên toàn thế giới, Do máy ATM hoạt động hoàn toàn tự động và có tính chính xác cao cũng như các dịch vụ hỗ trợ khách hàng tốt và phong phú như:

- Khi sử dụng thẻ ATM khách hàng sẽ tiết kiệm được thời gian và tránh được các thủ tục phiền hà do không phải tới ngân hàng rút tiền.
- Giảm tới mức tối đa các rủi ro như khi sử dụng tiền mặt: Tiền giả, mất cắp…
- Người sử dụng có thể rút tiền mọi lúc, mọi nơi ở các máy ATM được lắp đặt ở: Các trung tâm mua sắm, đường phố, nhà sách, bệnh viện…
- Việc quản lý số tiền trong thẻ trên máy ATM rất đơn giản, dễ sử dụng, hiệu quả và kinh tế.
- Thông qua việc nghiên cứu về mô hình Máy ATM có thể được ứng dụng sang các hình thức kinh doanh khác.

Qua những lợi ích của máy ATM đem lại, em đã quyết tâm thực hiện đề tài:

"**Nghiên cứu một số giải pháp Công nghệ Thông tin ứng dụng trong máy rút tiền tự động ATM**"

CHƯƠNG 1: MỞ ĐẦU

1.1 Lý do thực hiện đề tài

Ngày nay, máy rút tiền tự động ATM không còn xa lạ với người sử dụng nữa, nó như là một "nhân viên ngân hàng" ngày đêm phục vụ khách hàng không biết mệt mỏi, không ca thán nửa lời, không lương và sai sót trong lúc làm việc hầu như không có.

Tuy nhiên không thể phụ nhận được thực trạng: công nghệ ngày một phát triển, sự phát triển liên tục và đổi mới từng ngày, ngày hôm nay công nghệ này còn đứng ở vị trí độc tôn, nhưng ngày mai có thể nó đã là một công nghệ đã lỗi thời, lạc hậu. Công nghệ tuy hiện đại tới đâu nhưng bản thân nó vẫn có những lỗi, lỗ hổng mà trong quá trình đưa vào vận hành sử dụng mới phát hiện ra chúng. Những lỗi trên tùy từng mức độ mà hậu quả do chúng gây ra ở những mức độ khác nhau.

Do đó những công nghệ sử dụng trong máy ATM chưa hẳn đã là tối ưu và không có lỗi. Vì đặc thù của ngân hàng là cần tính bảo mật rất cao và khi các lỗi xảy ra đều gây ra những hậu quả rất nghiêm trọng như: thất thoát tiền bạc, ảnh hưởng rất lớn tới uy tín của ngân hàng, cũng như quyền lợi của khách hàng.

Từ những thực tế và lý do đó em nhận thấy cần nghiên cứu các ứng dụng, các kĩ thuật công nghệ được áp dụng vào thiết bị này để từ đó có thể tìm kiếm được những lỗi phát sinh và đưa ra được những hướng phát triển giúp thiết bị ATM ngày một hoàn thiện để phục vụ người sử dụng được tốt hơn.

1.2 Mục tiêu của đề tài

Máy ATM được kết hợp bởi rất nhiều thiết bị điện tử, trong đó trái tim của máy là một hệ thống máy tính được tích hợp để xử lý các tác vụ giao dịch từ phía người dùng và chuyển tải các dữ kiện đó tới ngân hàng cũng như nhận các dữ kiện từ phía ngân hàng để đưa ra các quyết định nhằm thỏa mãn các yêu cầu của người sử dụng.

Như vậy, đề tài cần giải quyết các công việc sau:

- ❖ Tìm hiểu các lý thuyết cơ sở phục vụ đề tài.
- ❖ Tìm hiểu và nghiên cứu về cấu tạo máy ATM: thiết bị phần cứng và phần mềm.
- ❖ Tìm hiểu và nghiên cứu về hạ tầng mạng của máy ATM: các thiết bị phần cứng, phần mềm, nguyên lý hoạt động.
- ❖ Tìm hiểu và nghiên cứu về cách thức bảo mật thông tin, dữ liệu của hệ thống.
- ❖ Nghiên cứu và chỉ ra các thiếu sót hoặc lỗi (nếu có) của máy ATM và nêu ra được hướng phát triển cho tương lai.

1.3 Khái quát nội dung

Nội dung gồm 5 chương:

Chương 1. Mở đầu: Lý do thực hiện đề tài, các mục tiêu cần đạt được.

Chương 2. Cơ sở lý thuyết: Giới thiệu cơ sở lý thuyết về mạng, bảo mật, nguyên lý hoạt động.

Chương 3. Máy ATM: Cấu tạo máy ATM, hạ tầng mạng, giao dịch trên máy ATM, một số lưu đồ thuật toán.

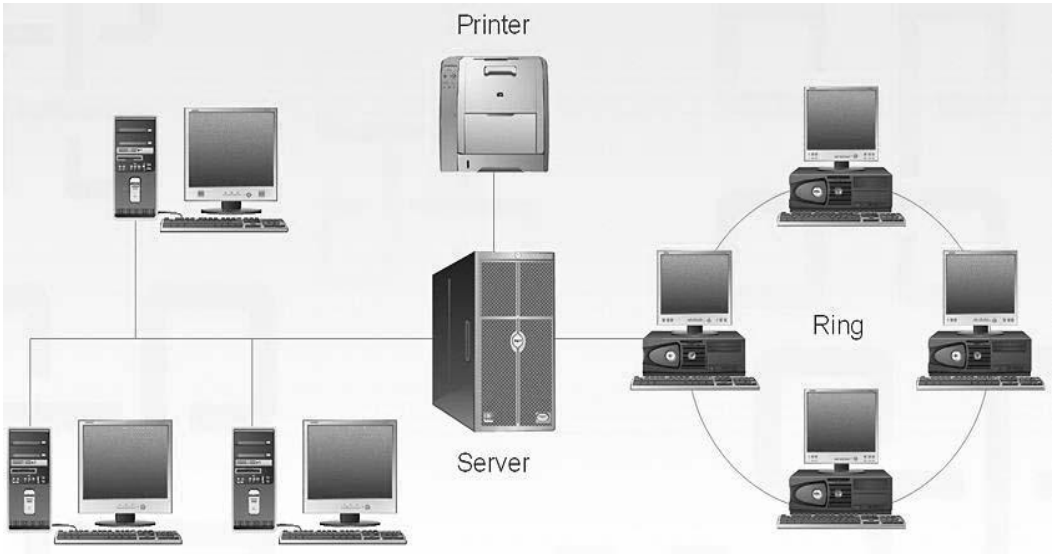
Chương 4. Chuẩn ISO 8583: Trình bày giao thức truyền tin chuẩn ISO 8583.

Chương 5. Kết quả nghiên cứu hệ thống: Trình bày các kết quả đạt được và hướng phát triển cho tương lai.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT VỀ MẠNG VÀ BẢO MẬT.

2.1 Khái niệm cơ bản về mạng máy tính

Mạng máy tính là hai hay nhiều máy tính được kết nối với nhau theo một cách nào đó sao cho chúng có thể trao đổi thông tin qua lại với nhau.



Hình 1: Mạng máy tính.

Mạng máy tính ra đời xuất phát từ nhu cầu muốn chia sẻ và dùng chung dữ liệu. Không có hệ thống mạng thì dữ liệu ở các máy tính độc lập khi muốn chia sẻ cho nhau thì phải thông qua việc in ấn hay sao chép qua các thiết bị lưu trữ chung gian như: CD rom, DVD rom,… điều này gây rất bất tiện cho người dùng.

Các máy tính khi được kết nối thành mạng cho phép:

- Sử dụng chung các công cụ tiện ích.
- Chia sẻ kho dữ liệu dùng chung.
- Tăng độ tin cậy của hệ thống.
- Trao đổi thông điệp, hình ảnh.
- Dùng chung các thiết bị ngoại vi (Máy in,Fax,modem…)
- Giảm thiểu chi phí và thời gian đi lại.

2.1.1 Phân loại mạng

Phương thức kết nối mạng được sử dụng chủ yếu trong liên kết mạng: có hai phương thức chủ yếu, đó là điểm - điểm và điểm - nhiều điểm.

− Với phương thức "điểm - điểm", các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Mỗi máy tính có thể truyền và nhận trực tiếp dữ liệu hoặc có thể làm trung gian như lưu trữ những dữ liệu mà nó nhận được rồi sau đó chuyển tiếp dữ liệu đi cho một máy khác để dữ liệu đó đạt tới đích.

− Với phương thức "điểm - nhiều điểm", tất cả các trạm phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một máy tính sẽ có thể được tiếp nhận bởi tất cả các máy tính còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi máy tính căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình không nếu đúng thì nhận còn nếu không thì bỏ qua.

Phân loại mạng máy tính theo vùng địa lý:

− GAN (Global Area Network) kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thực hiện thông qua mạng viễn thông và vệ tinh.

− WAN (Wide Area Network) - Mạng diện rộng, kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong cùng một châu lục. Thông thường kết nối này được thực hiện thông qua mạng viễn thông. Các WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.

− MAN (Metropolitan Area Network) kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50-100 Mbit/s).

− LAN (Local Area Network) - Mạng cục bộ, kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao ví dụ cáp đồng trục thay cáp quang. LAN thường được sử dụng trong nội bộ một cơ quan/tổ chức...Các LAN có thể được kết nối với nhau thành WAN.

Phân loại mạng máy tính theo tôpô

− Mạng dạng hình sao (Star topology): Ở dạng hình sao, tất cả các trạm được nối vào một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển tín hiệu đến trạm đích với phương thức kết nối là phương thức "điểm - điểm".

− Mạng hình tuyến (Bus Topology): Trong dạng hình tuyến, các máy tính đều được nối vào một đường dây truyền chính (bus). Đường truyền chính này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là terminator (dùng để nhận biết là đầu cuối để kết thúc đường truyền tại đây). Mỗi trạm được nối vào bus qua một đầu nối chữ T (T_connector) hoặc một bộ thu phát (transceiver).

− Mạng dạng vòng (Ring Topology): Các máy tính được liên kết với nhau thành một vòng tròn theo phương thức "điểm - điểm", qua đó mỗi một trạm có thể nhận và truyền dữ liệu theo vòng một chiều và dữ liệu được truyền theo từng gói một.

− Mạng dạng kết hợp: trong thực tế tuỳ theo yêu cầu và mục đích cụ thể ta có thể thiết kế mạng kết hợp các dạng sao, vòng, tuyến để tận dụng các điểm mạnh của mỗi dạng.

Phân loại mạng theo chức năng

− Mạng Client-Server: một hay một số máy tính được thiết lập để cung cấp các dịch vụ như file server, mail server, Web server, Printer server, … Các máy tính được thiết lập để cung cấp các dịch vụ được gọi là Server, còn các máy tính truy cập và sử dụng dịch vụ thì được gọi là Client.

− Mạng ngang hàng (Peer-to-Peer): các máy tính trong mạng có thể hoạt động vừa như một Client vừa như một Server.

− Mạng kết hợp: Các mạng máy tính thường được thiết lập theo cả hai chức năng Client-Server và Peer-to-Peer.

2.1.2 Giao thức kết nối mạng TCP/IP

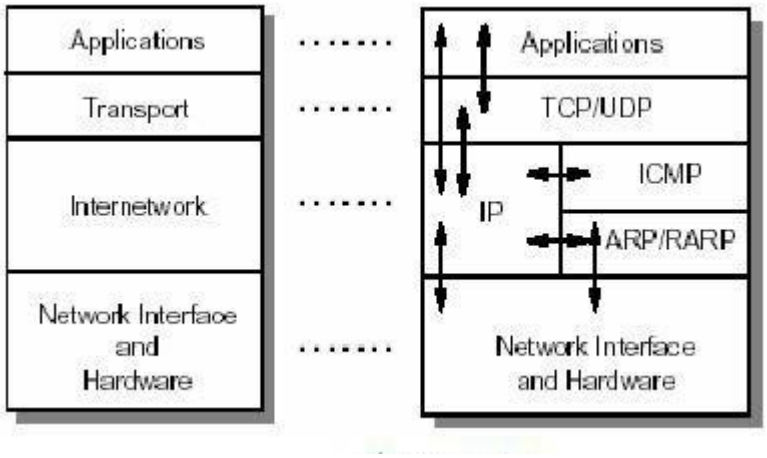
TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu. TCP/IP được xem là giản lược của mô hình tham chiếu OSI với bốn tầng như sau:

− Tầng liên kết mạng (Network Access Layer)

− Tầng Internet (Internet Layer)

− Tầng giao vận (Host-to-Host Transport Layer)

− Tầng ứng dụng (Application Layer)



Hình 2: kiến trúc TCP/IP

Tầng liên kết:

Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng đó.

Tầng Internet:

Tầng Internet (còn gọi là tầng mạng) xử lý qua trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Messages Protocol).

Tầng giao vận:

Tầng giao vận phụ trách luồng dữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol)

TCP cung cấp một luồng dữ liệu tin cậy giữa hai trạm, nó sử dụng các cơ chế như chia nhỏ các gói tin của tầng trên thành các gói tin có kích thước thích hợp cho tầng mạng bên dưới, báo nhận gói tin,đặt hạn chế thời gian time-out để đảm bảo bên nhận biết được các gói tin đã gửi đi. Do tầng này đảm bảo tính tin cậy, tầng trên sẽ không cần quan tâm đến nữa.

UDP cung cấp một dịch vụ đơn giản hơn cho tầng ứng dụng. Nó chỉ gửi các gói dữ liệu từ trạm này tới trạm kia mà không đảm bảo các gói tin đến được tới đích. Các cơ chế đảm bảo độ tin cậy cần được thực hiện bởi tầng trên.

Tầng ứng dụng:

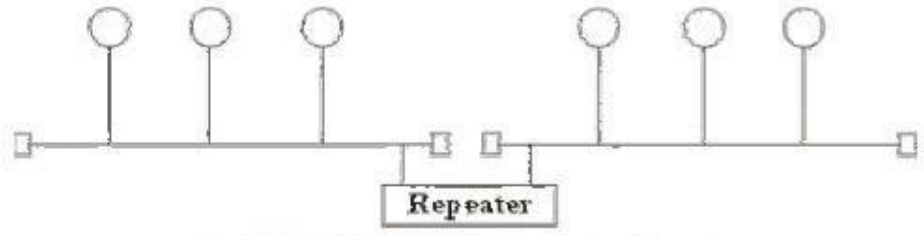
Tầng ứng dụng là tầng trên cùng của mô hình TCP/IP bao gồm các tiến trình và các ứng dụng cung cấp cho người sử dụng để truy cập mạng. Có rất nhiều ứng dụng được cung cấp trong tầng này, mà phổ biến là: Telnet: sử dụng trong việc truy cập mạng từ xa, FTP (File Transfer Protocol): dịch vụ truyền tệp, Email: dịch vụ thư tín điện tử, WWW (World Wide Web).

2.1.3 Một số thiết bị sử dụng trong kết nối mạng và tính năng của chúng

Bộ lặp tín hiệu (Repeater)

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong tầng vật lý của mô hình OSI. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng.



Hình 3: Mô hình liên kết mạng sử dụng Repeater

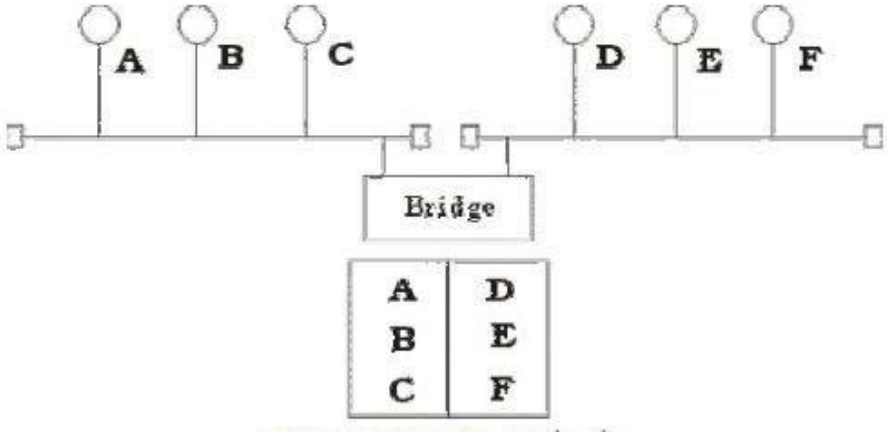
Bộ tập trung (Hub)

Hub là một trong những yếu tố quan trọng nhất của LAN, đây là điểm kết nối dây trung tâm của mạng, tất cả các trạm trên mạng LAN được kết nối thông qua Hub.

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao. Một hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng. Khi tín hiệu được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của. Các hub thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý hub.

Cầu (Bridge)

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau. Cầu nối hoạt động trên tầng liên kết dữ liệu nên không như bộ tiếp sức phải phát lại tất cả những gì nó nhận được thì cầu nối đọc được các gói tin của tầng liên kết dữ liệu trong mô hình OSI và xử lý chúng trước khi quyết định có chuyển đi hay không. Khi nhận được các gói tin Bridge chọn lọc và chỉ chuyển những gói tin mà nó thấy cần thiết. Điều này làm cho Bridge trở nên có ích khi nối một vài mạng với nhau và cho phép nó hoạt động một cách mềm dẻo.



Hình 4: Hoạt động của cầu nối.

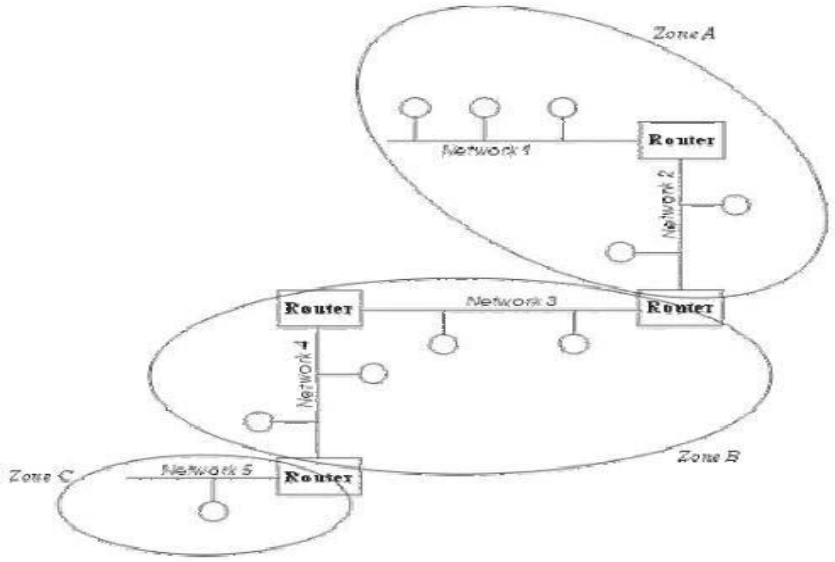
Bộ chuyển mạch (Switch)

Bộ chuyển mạch là sự tiến hoá của cầu, nhưng có nhiều cổng và dùng các mạch tích hợp nhanh để giảm độ trễ của việc chuyển khung dữ liệu. Switch giữa bảng địa chỉ MAC của mỗi cổng và thực hiện giao thức Spanning-Tree. Switch cũng hoạt động ở tầng data link và trong suốt với các giao thức ở tầng trên.

Bộ định tuyến(Router)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với

nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.



Hình 5: Hoạt động của Router.

2.2 Bảo mật thông tin trên mạng

2.2.1 Tổng quan về công nghệ mật mã(Cryptography)

Một trong những nguyên nhân sơ đẳng mà tin tặc có thể thành công là hầu hết các thông tin chúng ta truyền trên mạng đều ở dạng dễ đọc, dễ hiểu. Khi chúng ta kết nối WAN bằng công nghệ IP thì tin tặc dễ dàng thấy có thể bắt các gói tin bằng công cụ bắt gói (network sniffer), có thể khai thác các thông tin này để thực hiện tấn công mạng. Một giải pháp để giải quyết vấn đề này là dùng mật mã để ngăn tin tặc có thể khai thác các thông tin chúng bắt được khi nó đang được truyền trên mạng.

Mã hoá (Encryption) là quá trình dịch thông tin từ dạng nguồn dễ đọc sang dạng mã khó hiểu.Giải mã (Decryption) là quá trình ngược lại. Việc dùng mật mã sẽ đảm bảo tính bảo mật của thông tin truyền trên mạng, cũng như bảo vệ tính toàn vẹn, tính xác thực của thông tin khi lưu trữ.

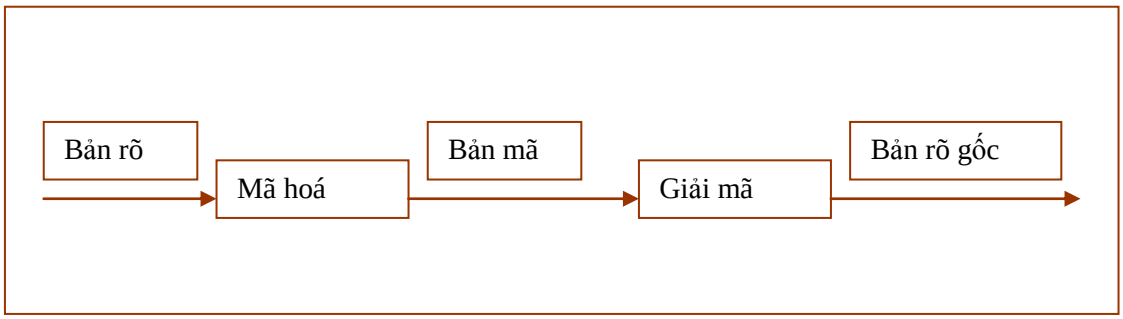
Mã mật được xây dựng để đảm bảo tính bảo mật (confidentiality), khi dữ liệu lưu chuyển trên mạng. Khi dữ liệu đã được mã hóa thì chỉ khi biết cách giải mã mới có khả năng sử dụng dữ liệu đó. Hiện nay các kỹ thuật mã hóa đã phát triển rất mạnh

với rất nhiều thuật toán mã hóa khác nhau. Các hệ mã khoá được chia làm hai lớp chính: Mã khoá đối xứng hay còn gọi là mã khoá bí mật. Mã khoá bất đối xứng hay còn gọi là mã khoá công khai.

2.2.2 Các khái niệm cơ bản

- Bản rõ (plaintext or cleartext) Chứa các xâu ký tự gốc, thông tin trong bản rõ là thông tin cần mã hoá để giữ bí mật.
- Bản mã (ciphertext): Chứa các ký tự sau khi đã được mã hoá, mà nội dung được giữ bí mật.
- Sự mã hoá (Encryption): Quá trình che dấu thông tin bằng phương pháp nào đó để làm ẩn nội dung bên trong gọi là sự mã hoá.
- Sự giải mã (Decryption): Quá trình biến đổi trả lại bản mã bản thành bản rõ gọi là giải mã.

  Quá trình mã hoá và giải mã được thể hiện trong sơ đồ sau:



- Hệ mật mã : là một hệ bao gồm 5 thành phần (P, C, K, E, D) thoả mãn các tính chất sau
  - P (Plaintext) là tập hợp hữu hạn các bản rõ có thể.
  - C (Ciphertext) là tập hợp hữu hạn các bản mã có thể.
  - K (Key) là tập hợp các bản khoá có thể.
  - E (Encrytion) là tập hợp các qui tắc mã hoá có thể.
  - D (Decrytion) là tập hợp các qui tắc giải mã có thể.

Chúng ta đã biết một thông báo thường được tổ chức dưới dạng bản rõ. Người gửi sẽ làm nhiệm vụ mã hoá bản rõ, kết quả thu được gọi là bản mã. Bản mã này được gửi đi trên một đường truyền tới người nhận sau khi nhận được bản mã người nhận giải mã nó để tìm hiểu nội dung.

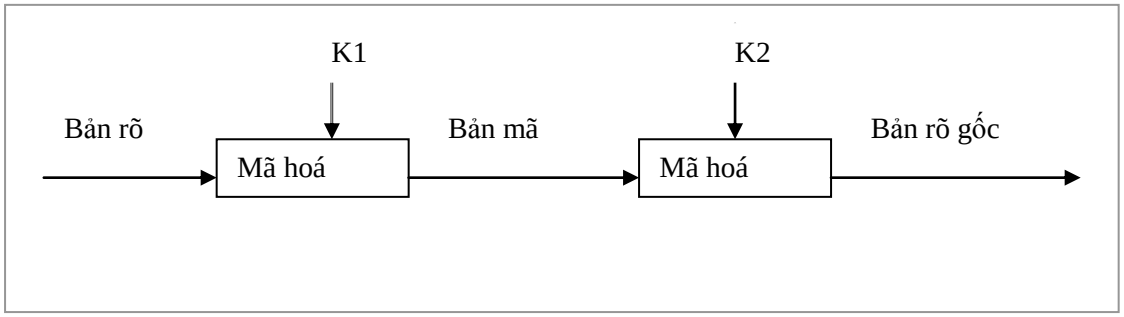
2.2.3 Hệ mã đối xứng – Khoá mã bí mật

Thuật toán đối xứng hay còn gọi thuật toán mã hoá cổ điển là thuật toán mà tại đó khoá mã hoá có thể tính toán ra được từ khoá giải mã. Trong rất nhiều trường hợp, khoá mã hoá và khoá giải mã là giống nhau. Thuật toán này còn có nhiều tên gọi khác như thuật toán khoá bí mật, thuật toán khoá đơn giản, thuật toán một khoá. Thuật toán này yêu cầu người gửi và người nhận phải thoả thuận một khoá trước khi thông báo được gửi đi, và khoá này phải được cất giữ bí mật. Độ an toàn của thuật toán này vẫn phụ thuộc và khoá, nếu để lộ ra khoá này nghĩa là bất kỳ người nào cũng có thể mã hoá và giải mã thông báo trong hệ thống mã hoá.

Sự mã hoá và giải mã của thuật toán đối xứng biểu thị bởi :

$$E_K(P) = C$$

$$D_K(C) = P$$



Trong hình vẽ trên thì :

K1có thể trùng K2, hoặc K1 có thể tính toán từ K2, hoặc K2 có thể tính toán từ K1.

Một số nhược điểm của hệ mã hoá cổ điển

- Các phương mã hoá cổ điển đòi hỏi người mã hoá và người giải mã phải cùng chung một khoá. Khi đó khoá phải được giữ bí mật tuyệt đối, do vậy ta dễ dàng xác định một khoá nếu biết khoá kia.
- Hệ mã hoá đối xứng không bảo vệ được sự an toàn nếu có xác suất cao khoá người gửi bị lộ. Trong hệ khoá phải được gửi đi trên kênh an toàn nếu kẻ địch tấn công trên kênh này có thể phát hiện ra khoá.
- Vấn đề quản lý và phân phối khoá là khó khăn và phức tạp khi sử dụng hệ mã hoá cổ điển. Người gửi và người nhận luôn luôn thông nhất với nhau về vấn đề khoá. Việc thay đổi khoá là rất khó và dễ bị lộ.
- Khuynh hướng cung cấp khoá dài mà nó phải được thay đổi thường xuyên cho mọi người trong khi vẫn duy trì cả tính an toàn lẫn hiệu quả chi phí sẽ cản trở rất nhiều tới việc phát triển hệ mật mã cổ điển.

Có nhiều thuật toán khoá bí mật khác nhau nhưng giải thuật được dùng nhiều nhất trong loại này là:

DES (Data Encryption Standard). DES mã hoá khối dữ liệu 64 bit dùng khoá 56 bit. Hiện nay trong một số hệ thống sử dụng DES3(sử dụng 168bit khoá thực chất là 3 khoá 56bit)

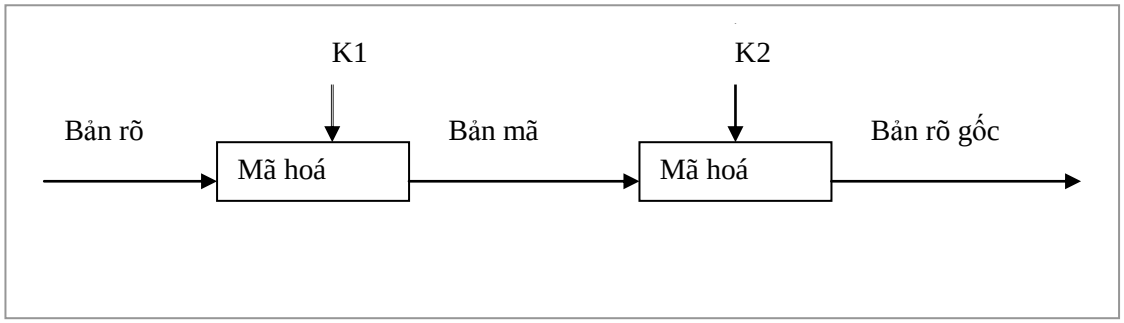
IDEA (International Data Encryption Standard).IDEA trái với DES, nó được thiết kế để sử dụng hiệu quả hơn bằng phần mềm. Thay vì biến đổi dữ liệu trên các khối có độ dài 64 bit, IDEA sử dụng khóa 128 bit để chuyển đổi khối dữ liệu có độ dài 64 bit tạo ra khối mã cũng có dài 64 bit. Thuật toán này đã được chứng minh là khá an toàn và rõ ràng là hơn hẳn DES.

Các hệ mã hoá đối xứng thường được sử dụng trong quân đội, nội vụ, ngân hàng,...và một số hệ thống yêu cầu an toàn cao.

Vấn đề khó khăn khi sử dụng khoá bí mật là vấn đề trao đổi khoá. Trao đổi khoá bí mật luôn phải truyền trên một kênh truyền riêng đặc biệt an toàn, tuyệt đối không sử dụng kênh truyền là kênh truyền dữ liệu.

2.2.4 Hệ mã bất đối xứng – Khoá mã công khai

Thuật toán mã hoá công khai là khác biệt so với thuật toán đối xứng. Chúng được thiết kế sao cho **khoá** sử dụng vào việc mã hoá là khác so với **khoá** giải mã. Hơn nữa khoá giải mã không thể tính toán được từ khoá mã hoá. Chúng được gọi với tên hệ thống mã hoá công khai bởi vì khoá để mã hoá có thể công khai, một người bất kỳ có thể sử dụng khoá công khai để mã hoá thông báo, nhưng chỉ một vài người có đúng khoá giải mã thì mới có khả năng giải mã. Trong nhiều hệ thống, khoá mã hoá gọi là khoá công khai (public key), khoá giải mã thường được gọi là khoá riêng (private key).



Trong hình vẽ trên thì :

K1 không thể trùng K2, hoặc

K2 không thể tính toán từ K1.

Đặc trưng nổi bật của hệ mã hoá công khai là cả khoá công khai(public key) và bản tin mã hoá (ciphertext) đều có thể gửi đi trên một kênh thông tin không an toàn.

Các điều kiện của một hệ mã hoá công khai như sau :

1. Việc tính toán ra cặp khoá công khai K_B và bí mật k_B dựa trên cơ sở các điều kiện ban đầu phải được thực hiện một cách dễ dàng, nghĩa là thực hiện trong thời gian đa thức.
2. Người gửi A có được khoá công khai của người nhận B và có bản tin P cần gửi đi thì có thể dễ dàng tạo ra được bản mã C.

C = EKB (P) = EB (P)

Công việc này cũng trong thời gian đa thức.

3. Người nhận B khi nhận được bản tin mã hóa C với khoá bí mật k_B thì có thể giải mã bản tin trong thời gian đa thức.
    a. P = DkB (C) = DB[EB(M)]
4. Nếu kẻ địch biết khoá công khai K_B cố gắng tính toán khoá bí mật thì khi đó chúng phải đương đầu với trường hợp nan giải, trường hợp này đòi hỏi nhiều yêu cầu không khả thi về thời gian.
5. Nếu kẻ địch biết được cặp (K_B,C) và cố gắng tính toán ra bản rõ P thì giải quyết bài toán khó với số phép thử là vô cùng lớn, do đó không khả thi.

2.2.5 Hệ mã hóa RSA ứng dụng bảo mật trong mô hình Client/Server

a. Khái niệm

Khái niệm hệ mật mã RSA đã được ra đời năm 1976 bởi các tác giả R.Rivets, A.Shamir, và L.Adleman. Hệ mã hoá này dựa trên cơ sở của hai bài toán :

+ Bài toán Logarithm rời rạc (Discrete logarith)

+ Bài toán phân tích thành thừa số.

Trong hệ mã hoá RSA các bản rõ, các bản mã và các khoá (public key và private key) là thuộc tập số nguyên $Z_N = \{1, \ldots, N-1\}$. Trong đó tập Z_N với $N=p\times q$ là các số nguyên tố khác nhau cùng với phép cộng và phép nhân Modulo N tạo ra modulo số học N.

Khoá mã hoá E_{KB} là cặp số nguyên (N,K_B) và khoá giải mã D_{kb} là cặp số nguyên (N,k_B), các số là rất lớn, số N có thể lên tới hàng trăm chữ số.

Các phương pháp mã hoá và giải mã là rất dễ dàng.

Công việc mã hoá là sự biến đổi bản rõ P (Plaintext) thành bản mã C (Ciphertext) dựa trên cặp khoá công khai K_B và bản rõ P theo công thức sau đây :

$$C = E_{KB}(P) = E_B(P) = P^{KB} \pmod N . \qquad (1)$$

Công việc giải mã là sự biến đổi ngược lại bản mã C thành bản rõ P dựa trên cặp khoá bí mật k_B , modulo N theo công thức sau :

$$P = D_{kB}(C) = D_B(C) = C^{kB} \pmod N . \qquad (2)$$

Dễ thấy rằng, bản rõ ban đầu cần được biến đổi một cách thích hợp thành bản mã, sau đó để có thể tái tạo lại bản rõ ban đầu từ chính bản mã đó :

$$P = D_B(E_B(P)) \qquad (3)$$

Thay thế (1) vào (2) ta có :

$$(P^{KB})^{kB} = P \pmod N \qquad (4)$$

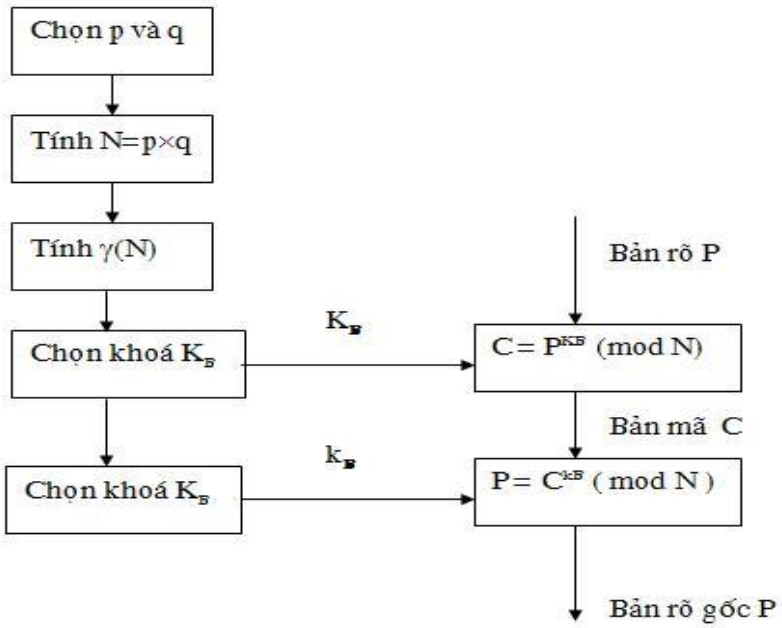
Trong toán học đã chứng minh được rằng, nếu N là số nguyên tố thì công thức (4) sẽ có lời giải khi và chỉ khi $K_B.k_B = 1 \pmod{N-1}$, áp dụng thuật toán ta thấy $N=p\times q$ với p, q là số nguyên tố, do vậy (4) sẽ có lời giải khi và chỉ khi :

$$K_B.k_B \equiv 1 \pmod{\gamma(N)} \qquad (5)$$

trong đó $\gamma(N) = LCM(p-1,q-1)$.

LCM (Lest Common Multiple) là bội số chung nhỏ nhất.

Nói một cách khác, đầu tiên người nhận B lựa chọn một khoá công khai K_B một cách ngẫu nhiên. Khi đó khoá bí mật k_B được tính ra bằng công thức (5). Điều này hoàn toàn tính được vì khi B biết được cặp số nguyên tố (p,q) thì sẽ tính được $\gamma(N)$.



Hình 6: Sơ đồ các bước thực hiện mã hoá theo thuật toán RSA.

b. Độ an toàn của RSA

Một nhận định chung là tất cả các cuộc tấn công giải mã đều mang mục đích không tốt. Trong phần độ an toàn của hệ mã hoá RSA sẽ đề cập đến một vài phương thức tấn công điển hình của kẻ địch nhằm giải mã trong thuật toán này.

Chúng ta xét đến trường hợp khi kẻ địch nào đó biết được modulo N, khoá công khai K_B và bản tin mã hoá C, khi đó kẻ địch sẽ tìm ra bản tin gốc (Plaintext) như thế nào. Để làm được điều đó kẻ địch thường tấn vào hệ thống mật mã bằng hai phương thức sau đây:

- Phương thức thứ nhất :

Trước tiên dựa vào phân tích thừa số modulo N. Tiếp theo sau chúng sẽ tìm cách tính toán ra hai số nguyên tố p và q, và có khả năng thành công khi đó sẽ tính được $\lambda(N)$ và khoá bí mật k_B. Ta thấy N cần phải là tích của hai số nguyên tố, vì nếu N là tích của hai số nguyên tố thì thuật toán phân tích thừa số đơn giản cần tối đa $\sqrt{N}$ bước, bởi vì có một số nguyên tố nhỏ hơn $\sqrt{N}$. Mặt khác, nếu N là tích của n số nguyên tố, thì thuật toán phân tích thừa số đơn giản cần tối đa $N^{1/n}$ bước.

Một thuật toán phân tích thừa số có thể thành phức tạp hơn, cho phép phân tích một số N ra thành thừa số trong O($\sqrt{P}$) bước, trong đó p là số chia nhỏ nhất của N, việc chọn hai số nguyên tố là cho thuật toán tăng hiệu quả.

- Phương thức thứ hai :

Phương thức tấn công thứ hai vào hệ mã hoá RSA là có thể khởi đầu bằng cách giải quyết trường hợp thích hợp của bài toán logarit rời rạc. Trường hợp này kẻ địch đã có trong tay bản mã C và khoá công khai K_B tức là có cặp (K_B,C)

Cả hai phương thức tấn công đều cần một số bước cơ bản, đó là :

O(exp $\sqrt{\ln N \ln(\ln N)}$), trong đó N là số modulo.

c. Tính chất của hệ mã hóa RSA

- ***Trong các hệ mật mã RSA, một bản tin có thể được mã hoá trong thời gian tuyến tính.***

Đối với các bản tin dài, độ dài của các số được dùng cho các khoá có thể được coi như là hằng. Tương tự như vậy, nâng một số lên luỹ thừa được thực hiện trong thời gian hằng, các số không được phép dài hơn một độ dài hằng. Thực ra tham số này che dấu nhiều chi tiết cài đặt có liên quan đến việc tính toán với các con số dài, chi phí của các phép toán thực sự là một yếu tố ngăn cản sự phổ biến ứng dụng của phương pháp này. Phần quan trọng nhất của việc tính toán có liên quan đến việc mã hoá bản tin. Nhưng chắc chắn là sẽ không có hệ mã hoá nào hết nếu không tính ra được các khoá của chúng là các số lớn.

- ***Các khoá cho hệ mã hoá RSA có thể được tạo ra mà không phải tính toán quá nhiều.***

Một lần nữa, ta lại nói đến các phương pháp kiểm tra số nguyên tố. Mỗi số nguyên tố lớn có thể được phát sinh bằng cách đầu tiên tạo ra một số ngẫu nhiên lớn, sau đó kiểm tra các số kế tiếp cho tới khi tìm được một số nguyên tố. Một phương pháp đơn giản thực hiện một phép tính trên một con số ngẫu nhiên, với xác suất 1/2

sẽ chứng minh rằng số được kiểm tra không phải nguyên tố. Bước cuối cùng là tính p dựa vào thuật toán Euclid.

Như phần trên đã trình bày trong hệ mã hoá công khai thì khoá giải mã (private key) k_B và các thừa số p,q là được giữ bí mật và sự thành công của phương pháp là tuỳ thuộc vào kẻ địch có khả năng tìm ra được giá trị của k_B hay không nếu cho trước N và K_B. Rất khó có thể tìm ra được k_B từ K_B cần biết về p và q, như vậy cần phân tích N ra thành thừa số để tính p và q. Nhưng việc phân tích ra thừa số là một việc làm tốn rất nhiều thời gian, với kỹ thuật hiện đại ngày nay thì cần tới hàng triệu năm để phân tích một số có 200 chữ số ra thừa số. Độ an toàn của thuật toán RSA dựa trên cơ sở những khó khăn của việc xác định các thừa số nguyên tố của một số lớn. Bảng dưới đây cho biết các thời gian dự đoán, giả sử rằng mỗi phép toán thực hiện trong một micro giây.

Số các chữ số trong số được phân tích	Thời gian phân tích
50	4 giờ
75	104 giờ
100	74 năm
200	4.000.000 năm
300	5×10^{15} năm
500	4×10^{25} năm

2.2.6 Mã hoá và giải mã thông tin

Khi một người dùng A muốn gửi thông tin cho người dùng B Người dùng A sẽ mã hoá thông tin bằng khoá công khai của người dùng B (K2B). Khi người dùng B nhận được thông tin nó sẽ giải mã thông tin bằng khoá bí mật của mình (K1B).

2.2.7 Chuyển đổi khoá

Khi người dùng A gửi thông tin khoá cho người dùng B. Người dùng A mã hoá thông tin khoá 2 lần. Lần đầu bằng khoá bí mật của bản thân (K1A); Lần hai bằng mã công khai của người nhận (K2B). Người dùng B nhận được thông tin khoá sẽ giải mã thông tin khoá hai lần. Lần đầu bằng khoá bí mật của bản thân (K1B). Lần 2 bằng khoá công khai của người gửi (K2A).

Một số giải thuật cho mã khoá công khai được sử dụng như: Diffie_Hellman, RSA, ECC, LUC, DSS,...

CHƯƠNG 3: MÁY ATM

3.1 Khái niệm máy ATM

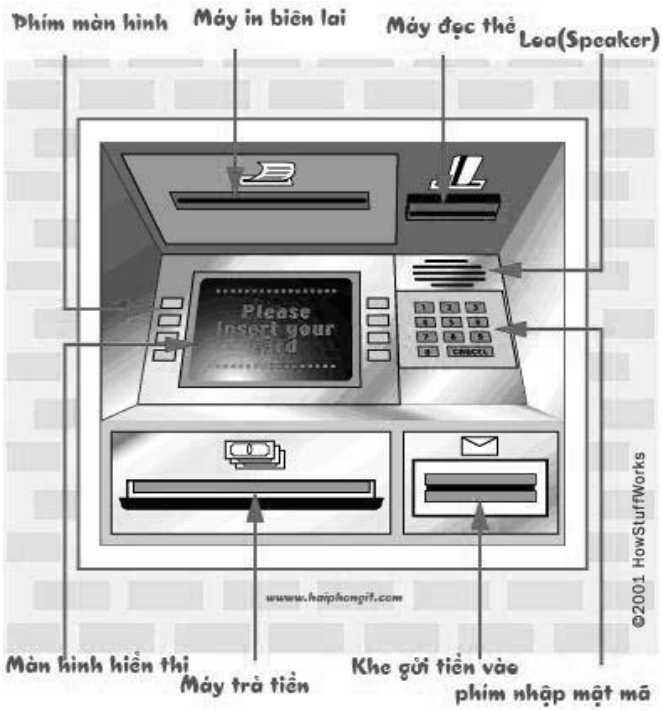
- *ATM (Automatic Teller Machine)* - là một thiết bị ngân hàng giao dịch tự động với khách hàng, thực hiện việc nhận dạng khách hàng thông qua thẻ ATM (thẻ ghi nợ, thẻ tín dụng) hay các thiết bị tương thích, và giúp khách hàng kiểm tra tài khoản, rút tiền mặt, chuyển khoản, thanh toán tiền hàng hóa dịch vụ.

Hình 7: Máy ATM.

3.2 Cấu tạo máy ATM

3.2.1 Phần cứng

Bao gồm : *máy đọc thẻ, phím nhập mật mã, màn hình hiển thị, Speaker ,máy vi tính chuyên biệt, máy đếm tiền, máy in nhật ký, máy in biên lai, bộ phận trả tiền và két sắt.*



Hình 8: Các thiết bị tương tác với người dùng.

Hình 9: Cấu tạo bên trong của máy ATM.

Máy đọc thẻ: Bộ phận này nắm bắt thông tin về tài khoản được lưu giữ trên dải băng từ ở mặt sau của thẻ ATM, thẻ nợ hoặc thẻ tín dụng. Máy chủ sử dụng thông tin này truyền gửi giao dịch cho ngân hàng của chủ thẻ.

Phím nhập mật mã: cũng không phải là loại bàn phím thông thường dùng để bấm số. Bàn phím này được thiết kế gắn liền với phần mềm an ninh. Khi bỏ thẻ vào máy và ấn phím, ngay lập tức con số được mã hóa và xóa hết các con số mà người dùng máy bấm vào vì vậy không một ai có thể nhận biết được con số mã pin.

Màn hình hiển thị: Màn hình hiển thị đưa ra lời nhắc cho chủ thẻ theo từng bước của quá trình giao dịch. Các máy ATM thuê đường dây thường sử dụng màn hình đen trắng hoặc màn hình màu chân không. Máy ATM quay số thường sử dụng màn hình đen trắng hoặc màn hình màu tinh thể lỏng.

Speaker(Loa): Speaker đưa ra cho chủ thẻ thông tin phản hồi bằng giọng nói khi phím được bấm.

Máy vi tính chuyên biệt: được đặt trong máy ATM có khả năng nhận biết hệ thống sắp bị mất điện. Khi chuẩn bị mất điện (nhiệt ở nguồn bị hạ xuống), ngay lập tức (chỉ trong nửa giây) máy sẽ ghi nhận tình trạng đang xảy ra. Khi có điện, máy sẽ tự khởi động và viết lại giao dịch.

Máy đếm tiền (chi tiền): chủ yếu sử dụng kỹ thuật đếm chân không (kéo tiền lên bằng lực kiểu như giác hơi) hoặc kỹ thuật ma sát. Máy nhận tiền có chức năng nhận tiền mặt do khách hàng trực tiếp gửi vào máy.

Máy in nhật ký: máy in này sẽ ghi lại tất cả dữ liệu liên quan đến chiếc máy ATM: từ ngày giờ khách hàng tra thẻ vào máy, thời gian giao dịch, chuyển khoản, rút tiền...

Máy in biên lai: Bộ phận in hóa đơn cung cấp cho chủ thẻ hóa đơn in trên giấy của giao dịch.

Bộ phận trả tiền: Phần quan trọng nhất của một máy ATM là cơ chế trả tiền và cơ chế an toàn. Toàn bộ phần đáy của hầu hết các máy ATM nhỏ là một két sắt để đựng tiền.

Cơ chế trả tiền có một mắt điện tử để đếm mỗi tờ giấy bạc khi nó ra khỏi máy trả tiền. Tổng số tờ giấy bạc và tất cả các thông tin liên quan đến một giao dịch cụ thể được ghi vào một cuốn sổ. Cuốn sổ thông tin này được in ra định kỳ và bản in trên giấy được người chủ sở hữu máy ATM lưu giữ trong vòng hai năm. Bất cứ khi nào một chủ thẻ có tranh chấp về một giao dịch, anh ta có thể yêu cầu bản in chỉ ra giao dịch, và sau đó tiếp xúc với bên sở hữu máy chủ. Nếu nơi nào không cung cấp bản in từ cuốn sổ, chủ thẻ cần phải thông báo cho ngân hàng hoặc định chế phát hành thẻ biết và điền vào một mẫu đơn và mẫu đơn này sẽ được fax cho bên sở hữu máy chủ. Trách nhiệm giải quyết tranh chấp thuộc về bên sở hữu máy chủ.

Bên cạnh mắt điện tử để đếm từng tờ giấy bạc, cơ chế trả tiền cũng có một bộ phận cảm biến để đánh giá độ dày của mỗi tờ tiền. Nếu hai tờ tiền bị kẹt với nhau, khi đó thay vì được trả ra cho chủ thẻ, tờ tiền này được chuyển vào một thùng loại bỏ ở trong máy. Máy cũng sẽ làm tương tự đối với các tờ tiền bị sờn, rách, bị gấp.

Số lượng tờ giấy bạc bị loại bỏ cũng được ghi lại, vì thế chủ sở hữu máy có thể biết được chất lượng của những tờ giấy bạc được xếp vào trong máy. Một tỷ lệ loại bỏ cao sẽ cho thấy các tờ tiền hoặc cơ chế trả tiền có vấn đề.

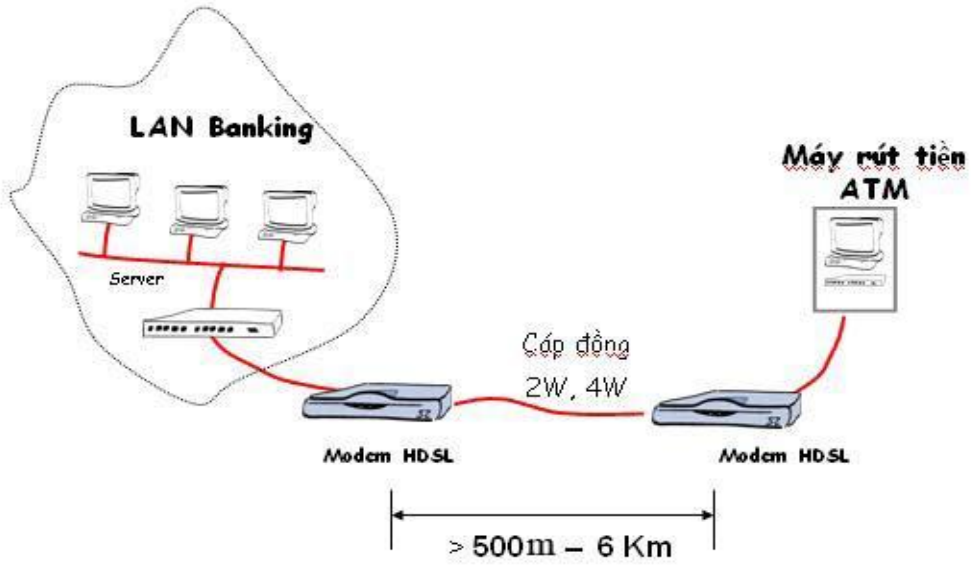
Két sắt: bộ phận chuyên biệt dùng để chứa tiền trong máy ATM.

3.2.2 Phần mềm

Bao gồm: bộ điều hành (OS-operate system) có thể là windows hoặc hệ điều hành mã nguồn mở, phần mềm điều khiển thiết bị, phần mềm tự phục hồi (trường hợp mất điện), phần mềm hoàn trả (reversal) và phần mềm an ninh. Chẳng hạn khi người sử dụng thẻ đang rút tiền, đột nhiên bị mất điện, người dùng chưa nhận được tiền trong khi tài khoản đã bị trừ.

Dựa vào phần mềm phục hồi và phần mềm hoàn trả, khi có điện lại máy sẽ nhận biết được tình trạng trước khi điện tắt và tự động hoàn trả số tiền chưa lấy ra khỏi máy vào tài khoản của người sử dụng. Phần mềm an ninh sẽ bảo mật các thông tin cho thẻ và pin.

3.3 Sơ lược về việc chuyển dẫn dữ liệu giữa máy ATM với ngân hàng



Hình 10: Mô hình kết nỗi giữa máy ATM với ngân hàng.

Máy ATM đơn giản là một trạm thu nhận dữ liệu. Giống như bất kỳ trạm thu nhận dữ liệu nào khác, máy ATM phải kết nối với một máy chủ (bộ xử lý chủ) và chuyển thông tin qua máy chủ này. Máy chủ này tương tự như một thiết bị cung cấp dịch vụ mạng (Internet Service Provider - ISP) ở chỗ nó là cổng vào mà qua đó tất cả các mạng lưới ATM khác nhau trở nên có thể sử dụng được đối với chủ thẻ (người muốn rút tiền).

Hầu hết các máy chủ đều có thể kết nối được với các máy ATM thuê đường dây hoặc các máy ATM quay số. Các máy thuê đường dây nối trực tiếp với máy chủ qua một đường dây điện thoại riêng gồm 4 dây, điểm nối điểm. Các máy ATM quay số nối với máy chủ qua một đường dây điện thoại thường sử dụng một modem và một số điện thoại miễn phí, hoặc thông qua một ISP sử dụng số điện thoại địa phương qua một modem.

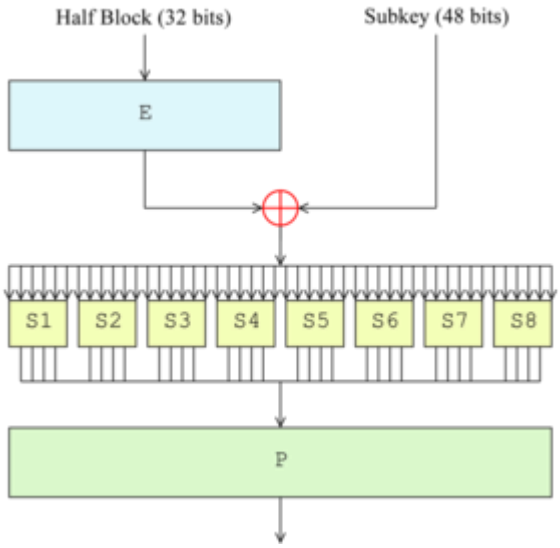
Máy ATM thuê đường dây riêng thích hợp đối với các điểm giao dịch số lượng lớn vì khả năng giao dịch nhanh và máy ATM quay số thích hợp với các điểm bán lẻ nơi mà chi phí là một yếu tố quan trọng hơn là tốc độ giao dịch. Chi phí ban đầu cho một máy quay số chỉ chưa bằng một nửa chi phí ban đầu cho một máy thuê đường dây. Các chi phí hoạt động hàng tháng của một máy quay số chỉ là một phần nhỏ so với chi phí hoạt động của một máy thuê đường dây.

Máy chủ có thể do một ngân hàng hoặc một tổ chức tài chính sở hữu, hoặc có thể do một nhà cung cấp dịch vụ độc lập sở hữu. Máy chủ do ngân hàng sở hữu thường chỉ phục vụ các máy ATM của ngân hàng.

3.4 Bảo mật trong hệ thống máy ATM

Dữ liệu từ máy ATM gửi tới ngân hàng đều được mã hoá, thường là dùng hệ thống 16bit, nhưng nay có một số ngân hàng trang bị hiện đại hơn, mã hoá trên bộ 32bit, đảm bảo bảo mật thông tin hơn. Mã hoá sẽ dựa trên 1 key được cung cấp từ ngân hàng cho mỗi máy, chứ không dùng chung giống nhau cho tất cả máy ATM trên hệ thống của ngân hàng, do đó thông tin được bảo mật rất tốt.

Ngoài ra các thông tin nhạy cảm trong ATM thường được mã hoá bằng một loại mã hoá nào đó như mã DES điển hình trong ngân hàng thường sử dụng Triple DES.



Hình 11: Sơ đồ mã DES.

- Thuật toán bảo mật DES và Triple-DES.

- Về mặt khái niệm, thông thường thuật toán mã hoá DES là thuật toán mở, nghĩa là mọi người đều biết thuật toán này. Điều quan trọng nhất là chìa khoá của DES có độ dài tới 56 bit, nghĩa là số lần thử tối đa để tìm được chìa khoá lên đến 2^56, trung bình là 2^55 = 36.028.797.018.963.968 lần, một con số rất lớn!.

- DES được thực hiện nhờ các phép dịch, hoán vị và các phép toán logic trên các bit. Mỗi ký tự trong bức thư hay bản tin cần mã hoá được biểu diễn bởi 2 số hexa hay 8 bít. DES mã hoá từng khối 64 bít tương đương 16 số hexa. Để thực hiện việc mã hoá DES sử dụng một chìa khoá cũng dưới dạng 16 số hexa hay 64 bít tức 8 byte, nhưng các bít thứ 8 trong các byte này bị bỏ qua trong khi mã hoá vì vậy độ lớn thực tế của chìa khoá là 56 bit. Ví dụ, ta mã hoá một bản tin hexa "0123456789ABCDEF" với chìa khoá là "5A5A5A5A5A5A5A5A" thì kết quả là "72AAE3B3D6916E92". Nếu kết quả này được giải mã với cùng chìa khoá "5A5A5A5A5A5A5A5A" thì ta sẽ thu lại được đúng bản tin "0123456789ABCDEF".

- DES bao gồm 16 vòng, nghĩa là thuật toán chính được lặp lại 16 lần để tạo ra bản tin được mã hoá.
  Thuật toán DES mã hoá đoạn tin 64 bit thành đoạn tin mã hoá 64 bit. Nếu mỗi khối 64 bit được mã hoá một cách độc lập thì ta có chế độ mã hoá ECB (Electronic Code Book). Có hai chế độ khác của mã hoá DES là CBC (Chain Block Coding) và CFB (Cipher Feedback), nó làm cho mỗi đoạn tin mã hoá 64 bit phụ thuộc vào các đoạn tin trước đó thông qua phép toán XOR.

  Trong đó Triple-DES chính là DES với hai chìa khoá 56 bit. Cho một bản tin cần mã hoá, chìa khoá đầu tiên được dùng để mã hoá DES bản tin đó, kết quả thu được lại được cho qua quá trình giải mã DES nhưng với chìa khoá là chìa khoá thứ hai, bản tin sau qua đã được biến đổi bằng thuật toán DES hai lần như vậy lại được mã hoá DES với một lần nữa với chìa khoá đầu tiên để ra được bản tin mã hoá cuối cùng. Quá trình mã hoá DES ba bước này được gọi là Triple-DES.

  - Xác thực mã Pin:

  Mã Pin được xác thực qua thuật toán mã hoá và một khoá bí mật, xác thực off-line và on-line.

- Xác thực on-line:

Khi ở chế độ này ATM sẽ xác nhận mã Pin của khách hàng sau khi mã hoá sẽ được gửi tới trung tâm cơ sở dữ liệu của ngân hàng để so sánh.

- Xác thực off-line:

Khi ở chế độ này ATM xác thực mã Pin không cần kết nối tới trung tâm cơ sở dữ liệu của ngân hàng, nó sẽ so sánh mã Pin do khách hàng nhập vào với mã Pin được mã hoá trong thẻ ATM, tuy nhiên việc thực hiện so sánh ở các máy ATM là tương đối chậm.

3.5 Nghiệp vụ giao dịch tiền trên máy ATM

Khi một chủ thẻ muốn thực hiện một giao dịch ATM, anh ta nhập vào những thông tin cần thiết thông qua bộ phận đọc thẻ và bàn phím. Máy ATM gửi thông tin này cho máy chủ, máy chủ sẽ truyền yêu cầu giao dịch đến ngân hàng hoặc định chế phát hành thẻ của chủ thẻ. Nếu chủ thẻ yêu cầu tiền mặt, máy chủ tạo ra một giao dịch chuyển tiền điện tử từ tài khoản séc của khách hàng sang tài khoản của bên sở hữu máy chủ. Khi tiền đã được chuyển đến tài khoản tại ngân hàng của bên sở hữu máy chủ, máy chủ gửi một mã số chấp thuận cho máy ATM ra lệnh cho máy trả tiền. Sau đó qua trung tâm thanh toán bù trừ, máy chủ thực hiện chuyển tiền của chủ thẻ sang tài khoản của đơn vị chấp nhận thẻ thông thường là vào ngày làm việc hôm sau. Bằng cách này, đơn vị chấp nhận thẻ được hoàn lại tất cả số tiền mà máy ATM đã trả.

- Dưới đây là cách sử dụng một loại máy ATM thông dụng. Sử dụng máy ATM bằng cách nhấn vào phím hay chạm vào màn hình ở mục cần chọn. Màn hình của máy sẽ hiện ra lần lượt các bước sau

Bước 1: Đưa thẻ vào khe của máy theo chiều có chú thích trên máy (Please insert your card). Thông thường mặt có số thẻ nổi lên trên. Chờ trong giây lát (Please ait)

Bước 2: Chọn ngôn ngữ (Select language). Máy sẽ liệt kê một số ngôn ngữ để chủ thẻ lựa chọn (Anh, Pháp, Trung Quốc,...). Ngôn ngữ thông dụng là tiếng Anh

Bước 3: Nhập số PIN của thẻ (Please enter your PIN - Personal Verification Number). Trên máy xuất hiện các ký hiệu * khi nhập số PIN vào máy. Nếu nhập sai số PIN, nhấn Clear và nhập lại số PIN đúng. Nhấn phím enter hay OK để kết thúc.

Bước 4: Chọn loại giao dịch (Select Transaction): chọn loại rút tiền mặt (withdraw Cash).

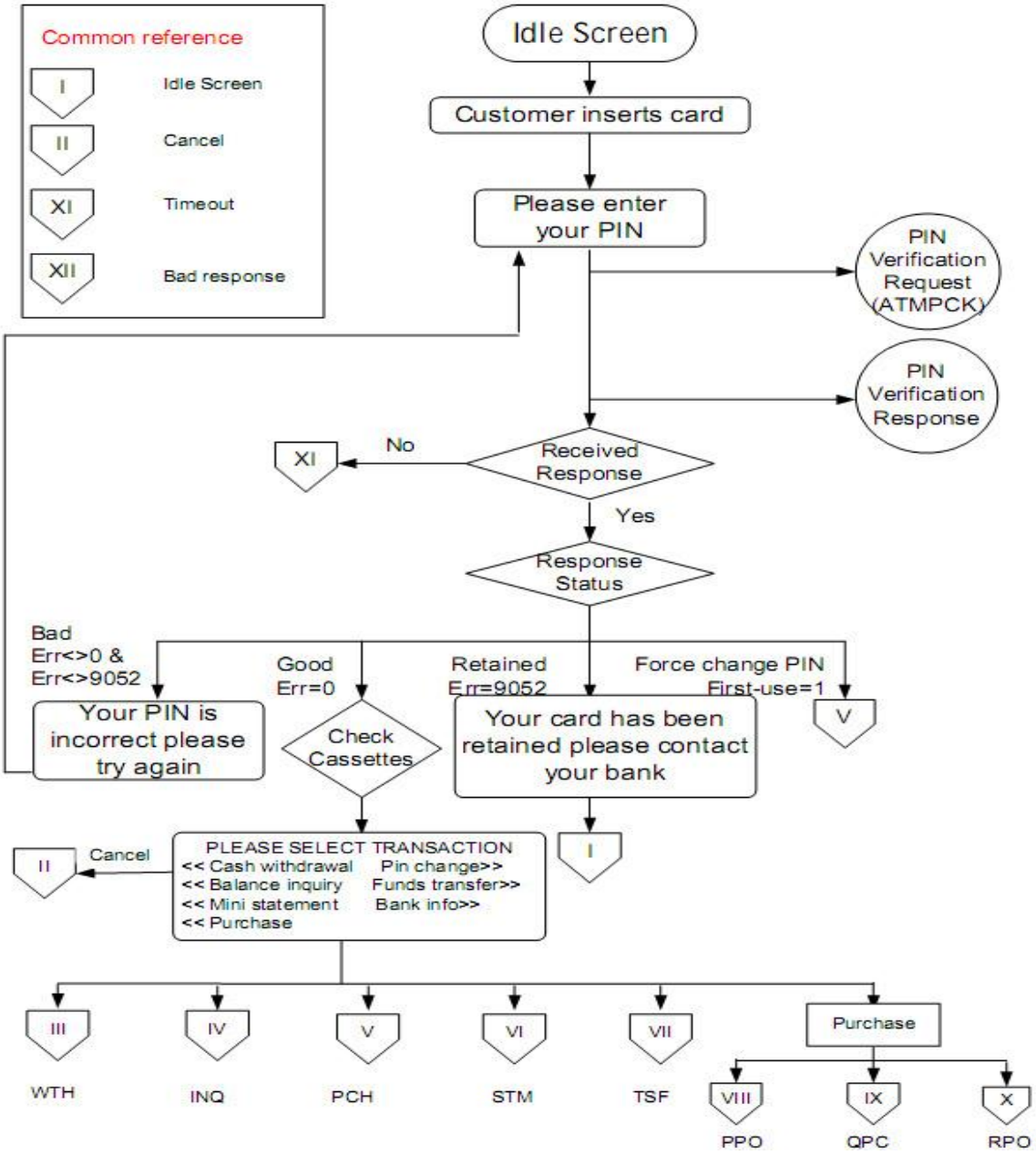
Bước 5: Chọn số tiền cần rút (Select Amount). Chọn một trong những số tiền liệt kê sẵn trong máy. Hoặc tự nhập số tiền bằng cách nhấn phím "Other" và nhấn phím "OK" hay "Enter" để kết thúc.

Bước 6: Chọn loại tài khoản (Select Account): chọn loại thẻ tín dụng (Credit Card Account).

Bước 7: Nhận tiền khi máy đưa ra. Nhận thẻ khi máy đưa ra. Nhận hóa đơn do máy in ra

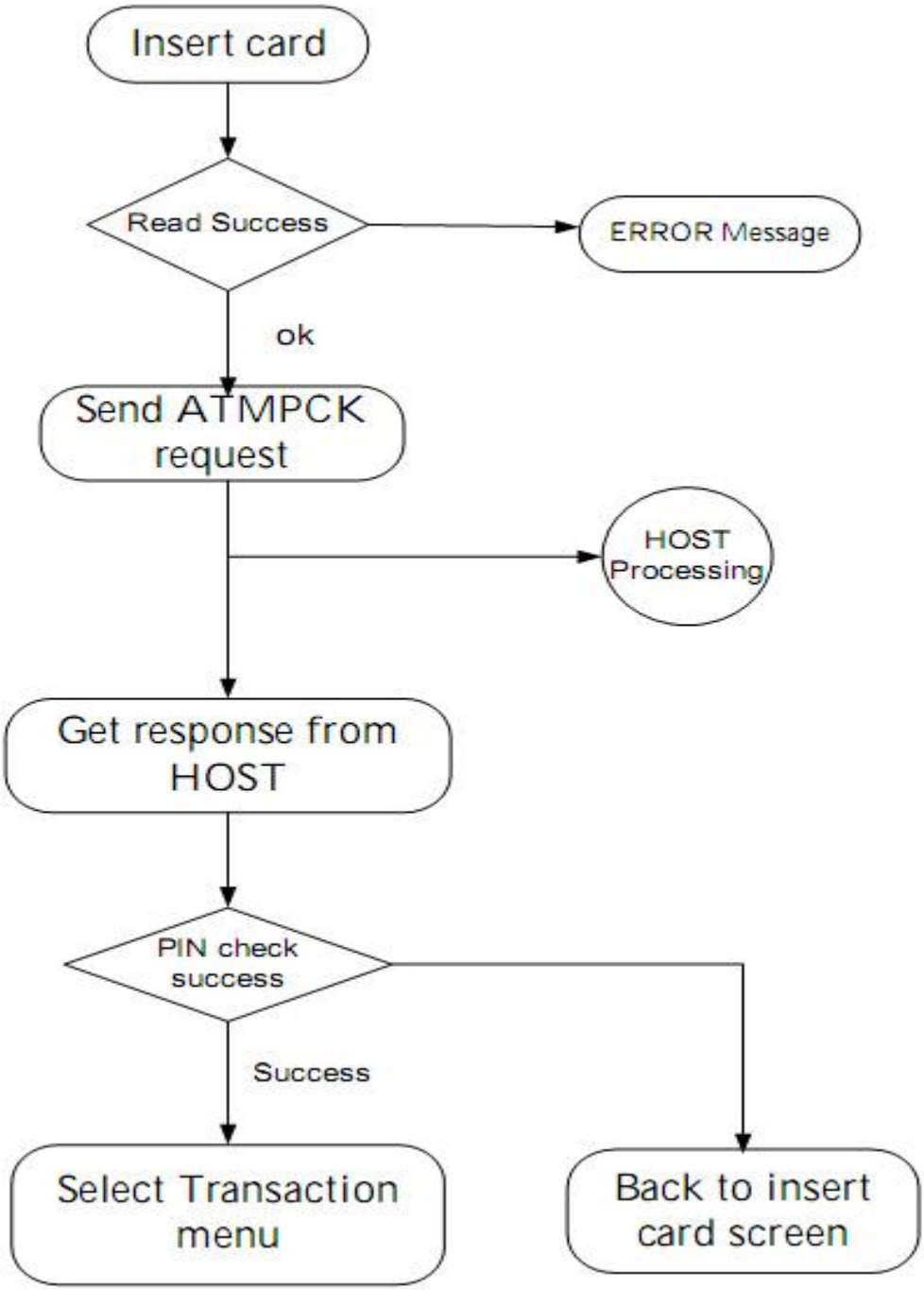
3.6 Các lưu đồ được sử dụng trong máy ATM

- Màn hình thao tác:



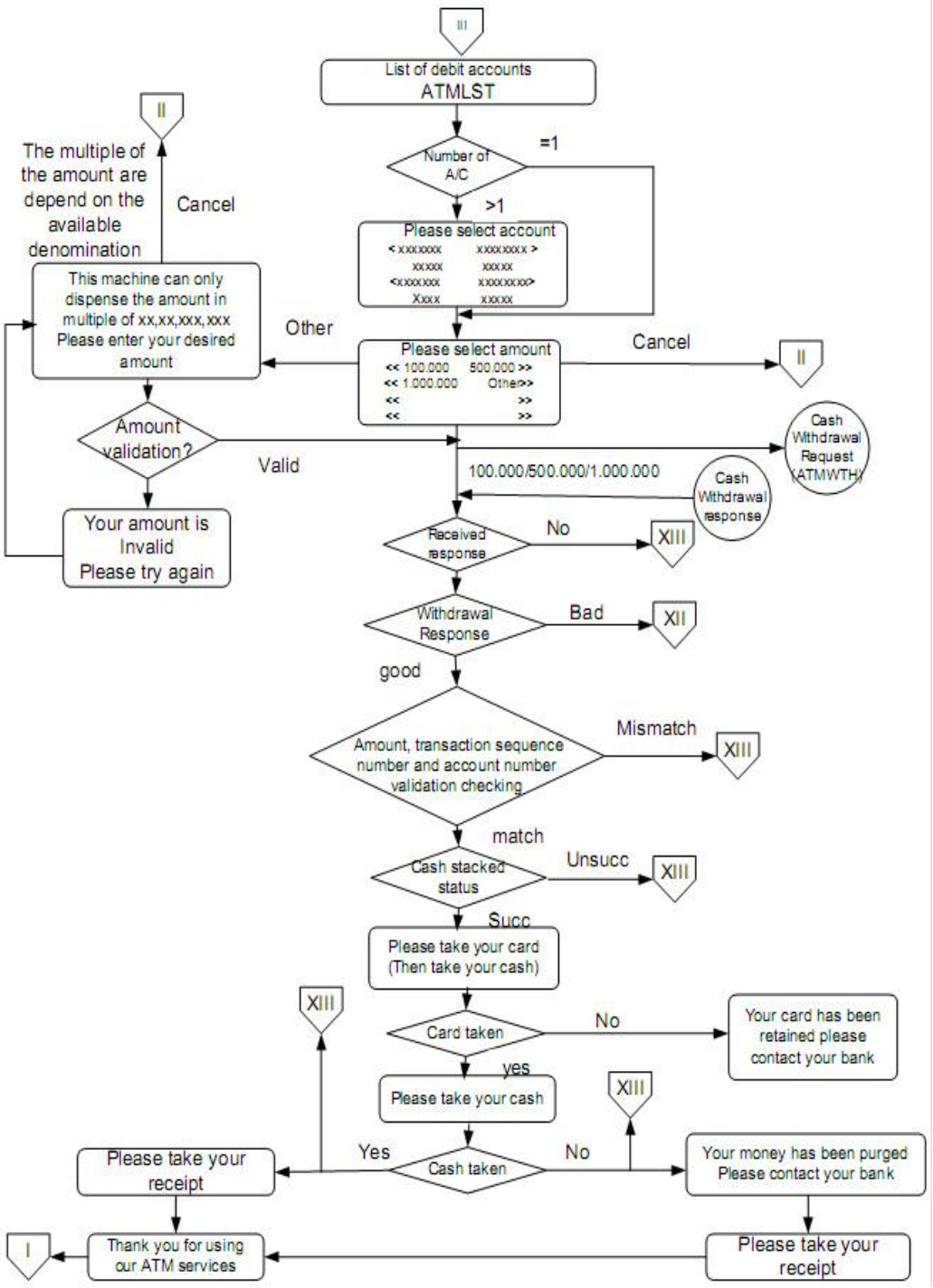
Hình 112: Màn hình thao tác.

- Quá trình kiểm tra mã pin:



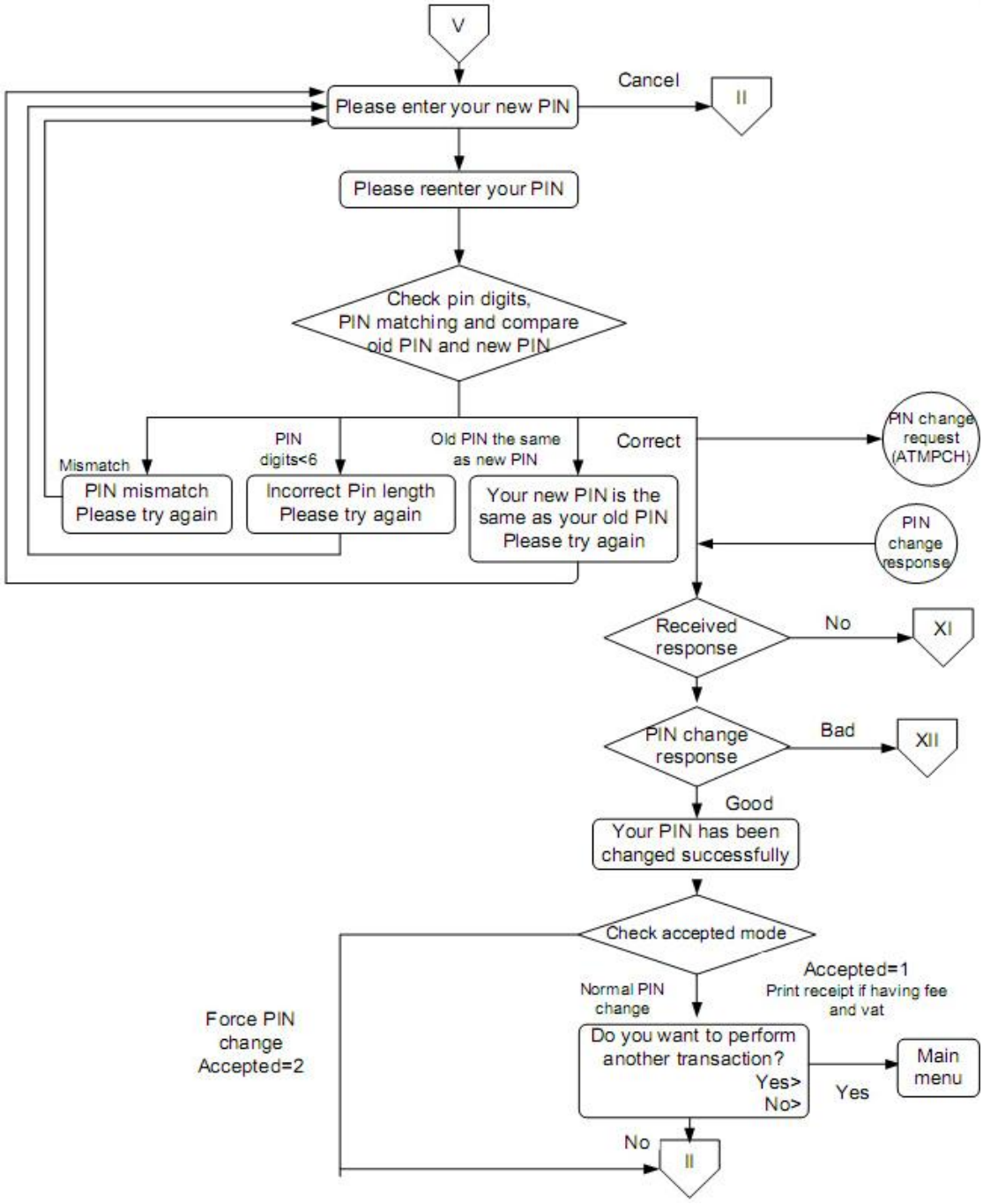
Hình 12: Quá trình kiểm tra mã pin

- Quá trình rút tiền mặt:



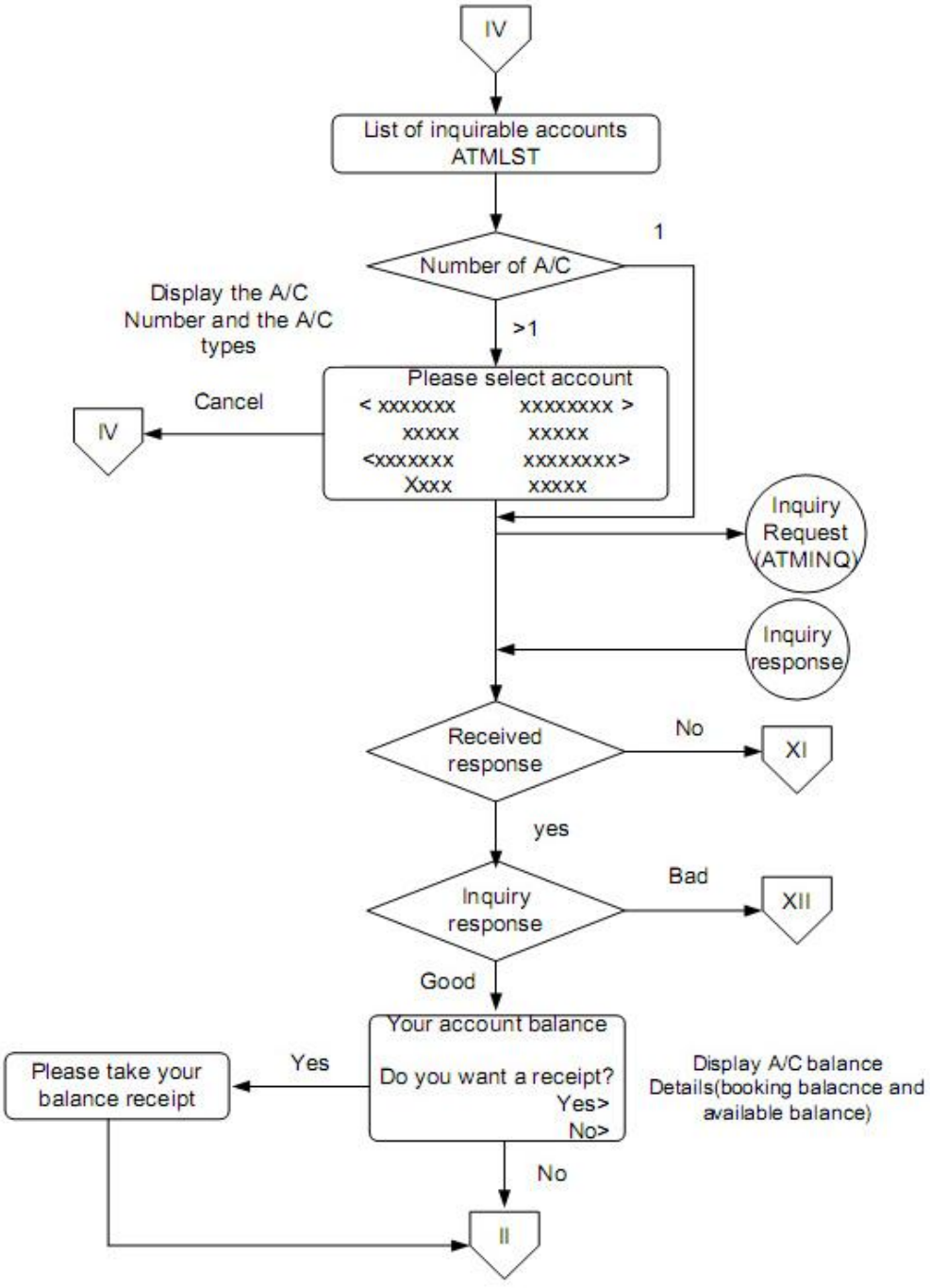
Hình 134: Quá trình rút tiền mặt.

- Quá trình thay đổi mã pin:



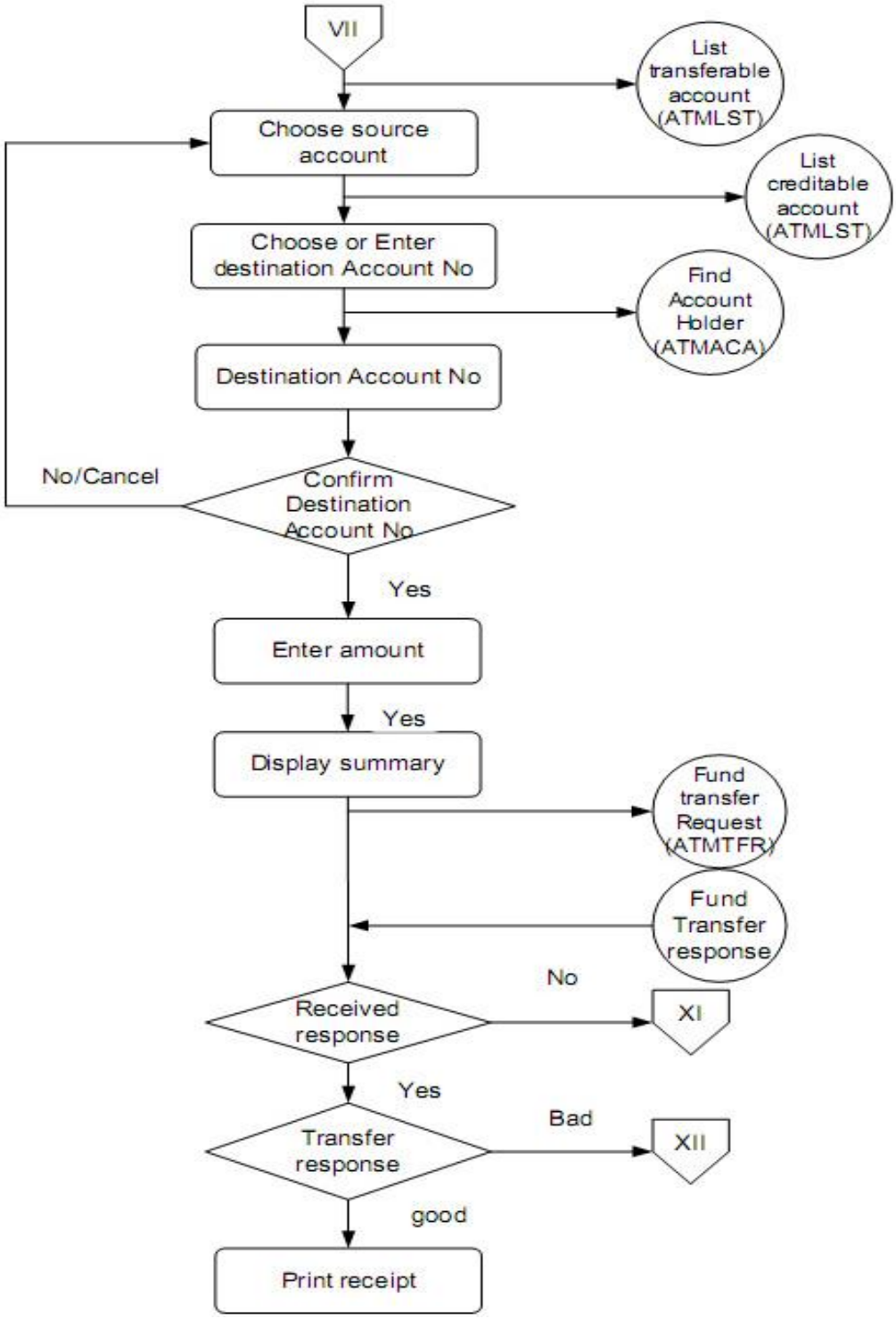
Hình 145: Quá trình thay đổi mã pin.

- Quá trình kiểm tra số dư tài khoản.



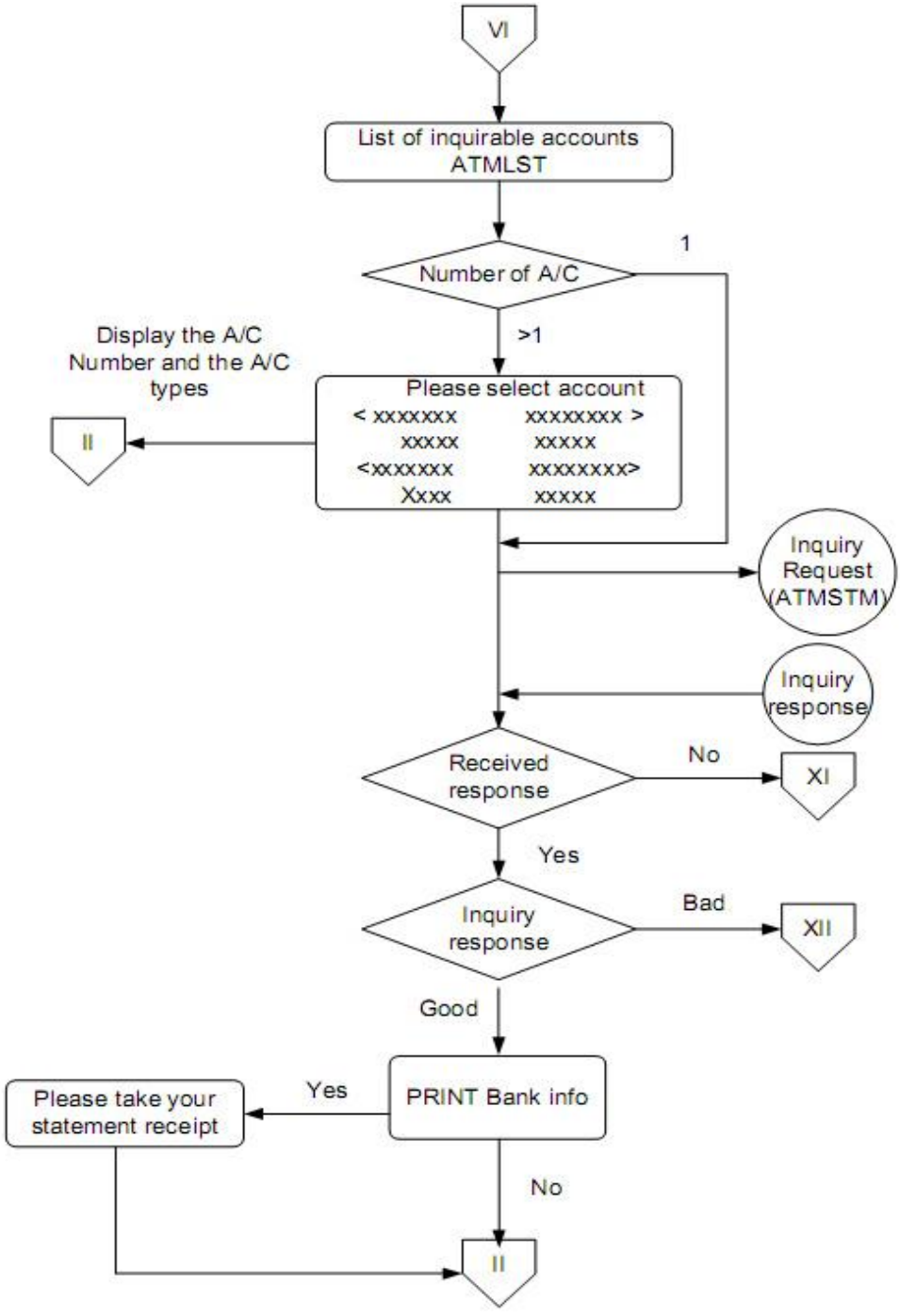
Hình 156: Quá trình kiểm tra số dư tài khoản.

- Quá trình chuyển khoản.



Hình 167: Quá trình chuyển khoản.

- Quá trình in hóa đơn giao dịch.

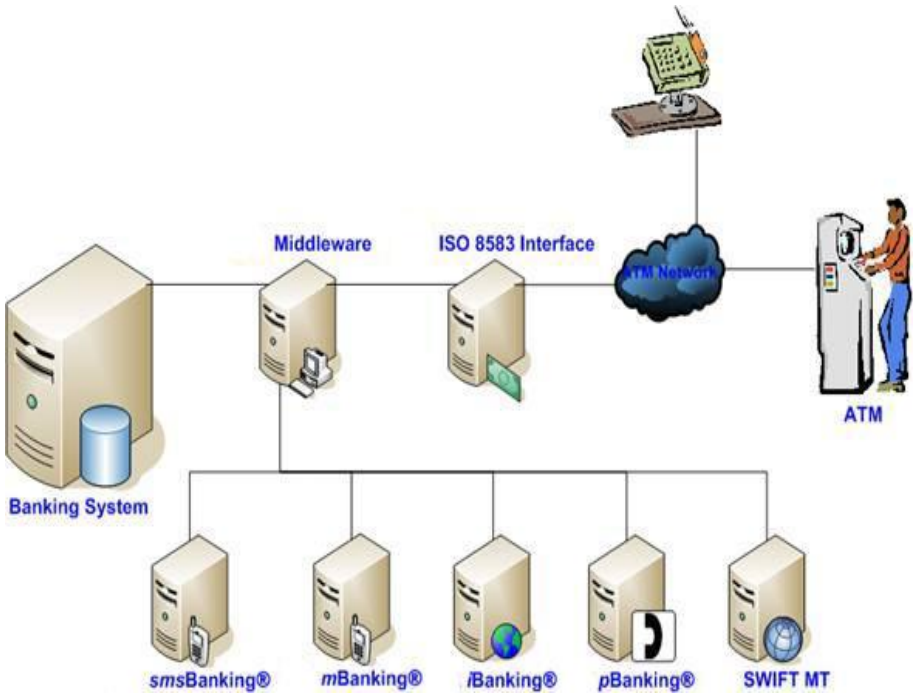


Hình 178: Quá trình in hóa đơn giao dịch.

CHƯƠNG 4: CHUẨN ISO 8583

Máy ATM giao dịch với ngân hàng thông qua hệ thống Switching financial bằng các thông điệp theo chuẩn ISO8583 trên nền TCP/IP.

Các Switch có thể là Switch cứng hoặc Switch mềm, trong đó Switch cứng là do một hãng nào đó sản xuất nó đã được tích hợp các phần mềm cần thiết, Switch mềm thực chất là phần mềm được cài đặt trên Server.



Hình 189: Mô hình liên kết nỗi giữa máy ATM với hệ thống ngân hàng.

Trong đó Máy ATM truyền đi các gói Message thông qua ATM Network theo giao thức ISO 8583 trên nền TCP/IP tới Middleware là một hệ thống server được cài đặt các phần mềm tích hợp nó là cầu nối trung gian giữa hệ thống ngân hàng và các kênh phân phối ngân hàng (ví dụ: Máy ATM, Máy Pos, phone banking, Internet banking, mobile banking, …)

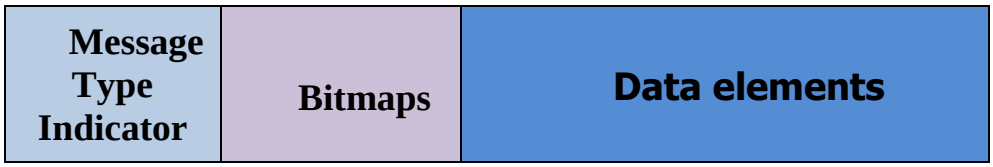
4.1 Khái niệm về chuẩn ISO 8583

Tiêu chuẩn ISO 8583 là tiêu chuẩn tài chính cho các giao dịch thẻ có tạo ra các thông điệp(messages) - trao đổi thông điệp. với các đặc tính kỹ thuật được quy định

thuộc chuẩn quốc tế là các tiêu chuẩn cho các hệ thống trao đổi các giao dịch điện tử của các máy sử dụng thẻ thanh toán.

4.2 Cấu trúc message ISO 8583

Cấu trúc của message ISO 8583 gồm: Thông điệp chỉ thị (Message Type Indicator), Các Bitmaps, Các yếu tố dữ liệu kèm theo.



❖ **Thông điệp chỉ thị:**

Là một mã gồm 4 kí tự, nó chứa thông tin về các kiểu message hiện hành, bao gồm những thông tin về phiên bản ISO, chức năng của message và ai đã gửi chúng.

- ký tự đầu trong 4 ký tự của thông điệp chỉ thị chứa thông tin về kiểu ISO hiện hành:

Ký tự đầu của thông điệp chỉ thị	Diễn tả
0XXX	Phiên bản ISO 8583-1:1987
1XXX	Phiên bản ISO 8583-2:1993
2XXX	Phiên bản ISO 8583-1:2003
9XXX	Để dành

- ký tự thứ 2 trong 4 ký tự của thông điệp chỉ thị xác định mục đích của thông điệp:

Ký tự thứ 2 của thông điệp chỉ thị	Diễn tả
X1XX	Thông điệp ủy quyền.
X2XX	Thông điệp tài chính.
X3XX	Thông điệp tương tác.
X4XX	Gửi lại thông điệp.
X5XX	Thông điệp phân luồng .
X6XX	Thông điệp quản trị.
X7XX	Thông báo chi phí đóng góp.
X8XX	Điều khiển thông điệp mạng.
X9XX	Để dành.

- ký tự thứ 3 trong 4 ký tự của thông điệp chỉ thị xác định chức năng của thông điệp:

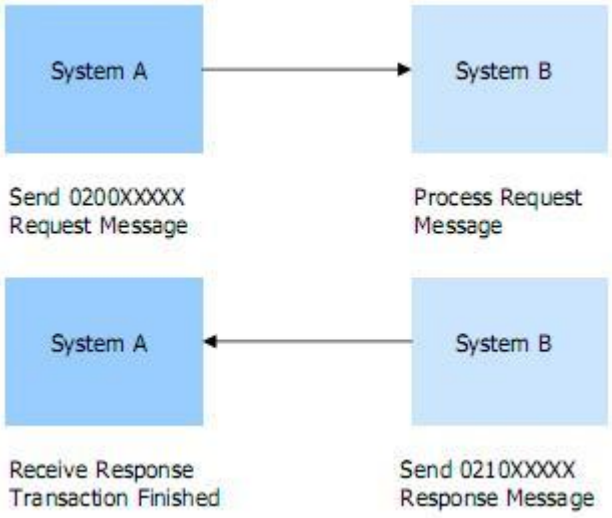
Ký tự thứ 3 của thông điệp chỉ thị	Diễn tả
XX0X	Yêu cầu.
XX1X	Trả lời yêu cầu.
XX2X	Hướng dẫn, tư vấn.
XX3X	Trả lời tư vấn.
XX4X	Thông báo.
XX8X	Ghi nhận.
XX9X	Không ghi nhận.

- ký tự cuối trong 4 ký tự của thông điệp chỉ thị xác định xuất xứ của thông điệp:

Ký tự cuối của thông điệp chỉ thị	Diễn tả
XXX0	Nhận được
XXX1	Nhận được lần nữa.
XXX2	Phát đi.
XXX3	Phát đi lần nữa.
XXX4	Khác
XXX5	Lặp lại lần khác.

Một ví dụ minh họa:

Thông điệp tài chính mang mã định danh 02XX: khi ở trạng thái này nó sẽ bắt đầu với mã là 0200 từ nơi yêu cầu và sẽ trả lời lại nơi gửi một message với tiêu đề 0210 và chỉ ra rằng đó là thông điệp trả lời từ những yêu cầu trước đó.

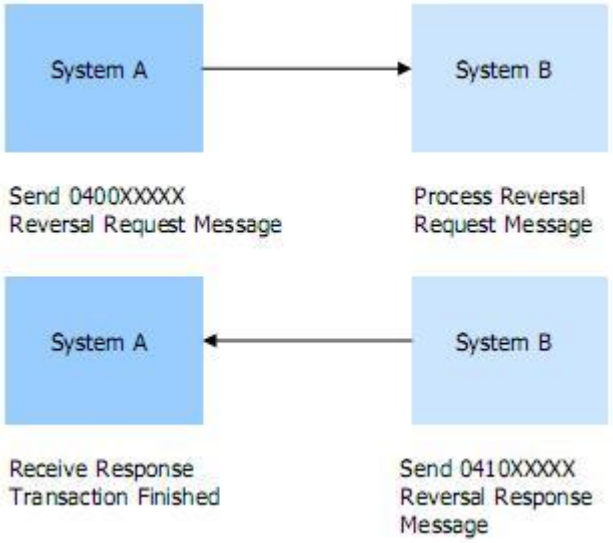


Hình 20: Trạng thái thông điệp giao dịch Flow.

Thông báo giao dịch tài chính có thể được hoặc tiền tệ hay phi tiền tệ.

Thông điệp phi tiền tệ là các thông báo hiện đang có yêu cầu từ phía hệ thống từ xa và các giao dịch phi tiền tệ khác.

Thông điệp tiền tệ là các thông báo yêu cầu hệ thống từ xa ghi vào thẻ tín dụng hay thẻ ghi nợ một số tiền vào tài khoản thẻ.



Hình 19: Trạng thái đáp lại thông điệp Flow.

Đáp lại thông điệp được xác định bởi tiêu đề là 04XX:

- Đối với các tương tác giao dịch: được nhận biết là thông điệp 0400 và các máy chủ từ xa sẽ đáp ứng lại các yêu cầu với thông điệp 0410

- Đối với các tương tác phi giao dịch: được nhận biết là thông điệp 0420 và sẽ được trả lời với thông điệp 0430

Ví dụ:

Khi một thông điệp được gửi đi trước khi thành công về giao dịch tài chính (02XX) khi đang được xác lập tại thẻ tín dụng ở máy ATM,

Thông điệp lặp lại được tự động gửi đi khi thiết bị yêu cầu không nhận được câu trả lời trong một khoảng thời gian nhất định.

Các thông điệp được lặp lại có định dạng 0401 cho giao dịch và 0421 cho các phi giao dịch.

Loại thông điệp tiếp theo được nhận biết là thông điệp 0800 hay mạng quản lý thông điệp, loại thông điệp này được gửi đi để kiểm soát giao mạng bằng cách hỗ trợ hoặc mô tả tình trạng hệ thống hoặc hệ thống an ninh.

❖ **Bitmap:**

Trong chuẩn ISO 8583, một bipmap là một lĩnh vực hoặc lĩnh vực phụ nào đó đã được quy định. Trong 1 thông điệp có thể có tới 3 Bitmap. Trong 1 thông điệp có ít nhất 1 bitmap, gọi là bitmap chính, nó chỉ ra phần tử dữ liệu hiện diện từ 1 tới 64. Một bitmap phụ cũng có thể được đưa ra, bitmap này chỉ ra sự hiện diện của các phần tử khác từ 65 tới 128. Tương tự, một bitmap thứ 3 có thể được sử dụng để chỉ sự hiện diện hoặc vắng mặt trong lĩnh vực 129 tới 192, mặc dù những dữ liệu này rất ít gặp.

Các bitmap có thể được truyền bằng 8 bytes dữ liệu nhị phân hoặc 16 kí tự hex 0-9, A-F trong các kí tự ASCII hoặc bộ kí tự EBCDIC.

Hexadecimal Character	Bit map represented
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

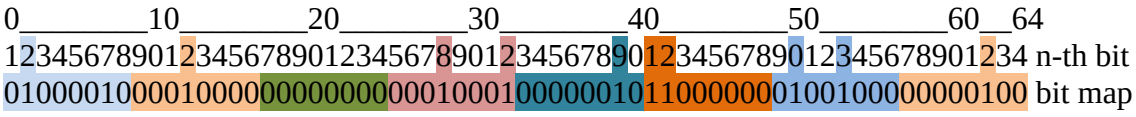
Một lĩnh vực được trình bày khi có xuất hiện các bitmap tương ứng trong thông điệp, giá trị là 1 khi có mặc là 0 khi vắng mặt các lĩnh vực tương ứng.

ví dụ:

Bitmap	Xác định hiện diện của lĩnh vực
4210001102C04804	2, 7, 12, 28, 32, 39, 41, 42, 50, 53, 62
7234054128C28805	2, 3, 4, 7, 11, 12, 14, 22, 24, 26, 32, 35, 37, 41, 42, 47, 49, 53, 62, 64 ,100.
8000000000000001	1, 64
0000000000000003 (bitmap Phụ)	127, 128

Giải thích bitmap thuộc lĩnh vực 4210001102C04804

01000010 = 42x (Đếm từ phía bên trái, Vị trí thứ 2 và thứ 7 là bit 1, nên có sự hiện diện của lĩnh vực 2 và 7)
00010000 = 10x (hiện diện của lĩnh vực 12)
00000000 = 00x (Không có lĩnh vực nào)
00010001 = 11x (hiện diện của lĩnh vực 28 và 32)
00000010 = 02x (hiện diện của lĩnh vực 39)
11000000 = C0x (hiện diện của lĩnh vực 41 và 42)
01001000 = 48x (hiện diện của lĩnh vực 50 và 53)
00000100 = 04x (hiện diện của lĩnh vực 62)



- Các lĩnh vự xuất hiện trong thông điệp: 2, 7, 12, 28, 32, 39, 41, 42, 50, 53, 62

❖ **Yếu tố dữ liệu:**

Là các yếu tố dữ liệu mang tính chất cá nhân như các lĩnh vực triển khai, các thông tin giao dịch. Hiện có đến 128 yếu tố dữ liệu đầu được xác định trong chuẩn ISO 8583:1987 và lên đến 192 yếu tố dữ liệu trong phiên bản sau này. Các phiên bản năm 1993 mới được thêm vào các định nghĩa, xóa một số tuy nhiên định dạng vẫn không thay đổi.

Trong khi đó mỗi yếu tố dữ liệu mang một yếu tố xác định ý nghĩa và định dạng, mỗi yếu tố dữ liệu được diễn tả trong một định dạng chuẩn mà xác định nội dung được cho phép của các trường(Số, nhị phân,...) và các lĩnh vực(Hoặc các biên cố định) theo bảng sau:

Tên viết tắt	Ý nghĩa
a	Alpha, bao gồm cả ký tự trống.
n	Giá trị số.
s	Các ký tự đặc biệt.
an	Kiểu chữ số.
as	Alpha và các ký tự đặc biệt.
ns	Số và các ký tự đặc biệt.
ans	Kiểu chữ số, số và ký tự đặc biệt
b	Số nhị phân.
z	2 và 3 mã số cài đặt như được định nghĩa trong tiêu chuẩn ISO 4909 và ISO / IEC 7813
. or .. or …	Biến chiều dài.
xx or xx or xxx	Chiều dài cố định hoặc tối đa của trường dữ liệu.

Ngoài ra, trong mỗi trường có thể cố định hoặc biến đổi chiều dài. Nếu có thay đổi theo độ dài thì độ dài của trường sẽ được chỉ ra bởi biến báo độ dài.

Loại	Ý nghĩa
Cố định.	Biến không chiều dài không cần.
LLVAR or (..xx)	Chỗ nào có LL <100, có nghĩa là hai chữ số hàng đầu LL chỉ rõ chiều dài trường VAR
LLLVAR or (...xxx)	Chỗ nào có LLL <1000, có nghĩa là ba chữ số đầu LLL xác định độ dài của trường VAR

Yếu tố dữ liệu	Loại	Dùng để
2	n..19	Số tài khoản chính.
3	n-6	Đang xử lý mã.
4	n-12	Số tiền giao dịch.
7	n-10	Ngày và giờ giao dịch.
11	n-6	Hệ thống theo dõi kiểm toán số.
12	n-6	Thời gian, địa điểm giao dịch.
13	n-4	Ngày, địa điểm giao dịch
32	n..11	Nơi nhận và mã số nhận dạng.
39	an-2	Mã hồi đáp.
48	asn…999	Các dữ liệu mang tính chất tư nhân.
49	n-3	Mã tiền tệ.
90	n-42	Các yếu tố dữ liệu ban đầu.

Một số ví dụ về thông điệp ISO 8583:

This is an example ISO network management message.

0800823A000000000000040000000000000004200906139000010906130420042000 1

This is an example ISO network management message response.

0810823A000002000000048000000000000004200906139000010906130420042000 00103112

This is an example ISO financial transaction message.

0200323A400108418010380000000000000000042005080501139212080504200422513207200000100000011560408004110125114633315633600029 9

This is an example ISO financial transaction message response.

0210323A40010A41801038000000000000000042005080501139212080504200422513207200000100000011560400080041116301151146333156 3GBAAASDDERRR

1300101B5439100100001765435000000000090300000268410000000300000000000008981000094310000000000000000 0000000000000000036000299

This is an example ISO reversal message.

0400F23A400108418202000000400000000019111111111000000000018000000000030000090806465100331613451909080909601006000200000000000343 0003948

0380811001200000409656573320000000300000136003000331700039480908064651000000000313202000033160908064519000000002000000000000 0

This is an example ISO reversal message response.

0410F23A40010A41820200000040000000001911111111100000000001800000000003000009080646510033161345190908090860100600020000000000034300000 3948

0380811001200000628110012000004096565733236003000331700039480908064651000000000313202000033160908064519000000002000000000000 0

This is an example ISO reversal repeat message.

0401F23A400108418202000000400000000019111111111000000000018000000000030000090806465200331613451909080909601006000200000000000343 0003948

038081100120000040965657332000000030000013600300033180003948090806465200000000313202000033160908064519000000002000000000000

This is an example ISO reversal repeat message response.

0410F23A40010A4182020000004000000000191111111110000000000180000000000300000908064652003316134519090809086010060002000000000003439400039480380811001200000409656573320000000300000136003000331800039480908064652000000003132020000331609080645190000000020000000000000

4.3 Một số message trong ISO 8583 - 1993

Bảng tổng lược các kiểu Message chính được hỗ trợ trong ISO 8583-1993.

Nhóm	Mã	Ý nghĩa
(11xx) Thông điệp ủy quyền		Hỗ trợ xử lý trên thẻ tín dụng được phát hành, các MDS qua tin nhắn yêu cầu cấp phép/01xx đến và từ mạng Banknet, thay mặt Banknet xử lý. Tuy nhiên các MDS chỉ liên lạc với bộ xử lý bằng cách sử dụng định dạng tin nhắn giao dịch tài chính/02xx.
(12xx) Thông điệp giao dịch tài chính	1200	Yêu cầu giao dịch tài chính.
	1210	Trả lời yêu cầu giao dịch tài chính.
	1280	Ghi nhận giao dịch tài chính [a].
	1290	Phủ nhận giao dịch tài chính.
	1220	Tư vấn giao dịch tài chính.
	1230	Trả lời tư vấn giao dịch tài chính.
(13xx) Thông điệp tệp tin thực thi.	1302	Yêu cầu tệp tin thực thi.
	1312	Trả lời yêu cầu tệp tin thực thi.
(14xx) Gửi lại thông điệp [b]	1420	Nhận lại tư vấn.

	1430	Nhận lại trả lời tư vấn.
	1422	Phát lại tư vấn.
	1432	Phát lại trả lời tư vấn.
(15xx) Thông điệp phân luồng	1520	Nhận lại phân luồng
	1530	Nhận lại trả lời phân luồng
	1522	Phát lại phân luồng .
	1532	Phát lại trả lời phân luồng .
(16xx) Thông điệp tư vấn quản trị	1620	Tư vấn quản trị.
	1630	Hồi đáp tư vấn quản trị.
	1644	Tư vấn quản trị [c]
(18xx) Quản lý thông điệp mạng	1800	Yêu cầu quản lý mạng lưới.
	1810	Hồi đáp yêu cầu quản lý mạng lưới.
	1820	Tư vấn quản lý mạng.

Trong đó:

Aqcuirer: Phía ngân hàng.

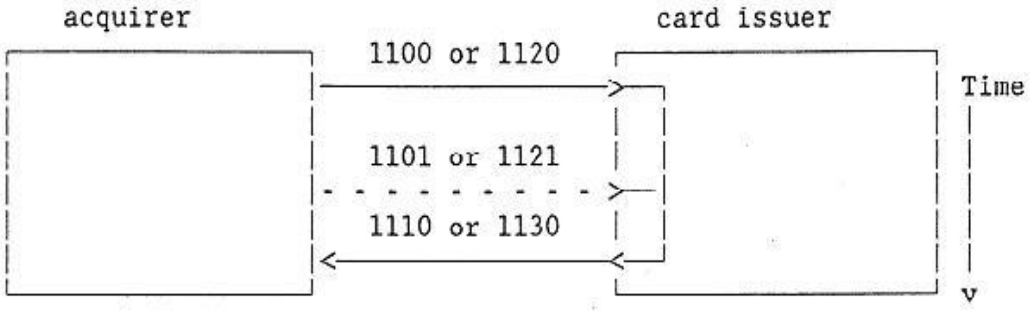
Card issuer: đơn vị chấp hành thẻ (Máy ATM).

4.3.1 (11xx) Giao dịch ủy quyền

Ủy quyền là sự chấp thuận hoặc đảm bảo số tiền trong tài khoản thẻ của ngân hàng phát hành.

Tin nhắn yêu cầu cấp phép (01xx) có thể hỗ trợ tìm hiểu số dư giao dịch.

- Thông điệp yêu cầu ủy quyền được dùng khi các giao dịch có thể không hoàn thành tại điểm cung cấp dịch vụ cho đến khi nhận được thông điệp trả lời cho các thao tác tiếp theo.
- Thông điệp yêu cầu ủy quyền hồi đáp được dùng để đáp lại thông điệp yêu cầu ủy quyền, nó cho biết sự chấp thuận, sự đảm bảo về tiền tệ hoặc các thao tác được đưa vào xác định trong mã các yếu tố dữ liệu kèm theo (Data elements).
- Thông điệp tư vấn ủy quyền được dùng để thông báo cho đơn vị chấp hành thẻ (ATM) là 1 giao dịch ủy quyền đã được hoàn thành tại thời điểm cung cấp dịch vụ.
- Thông điệp tư vấn ủy quyền hồi đáp được dùng để đáp lại thông điệp tư vấn ủy quyền, nếu bên đơn vị chấp hành thẻ (ATM) chấp thuận hoặc từ chối chuyển giao tài chính.
- Thông điệp thông báo ủy quyền được sử dụng để thông báo cho đơn vị chấp hành thẻ (ATM) khi một giao dịch ủy quyền đã hoàn thành tại thời điểm cung cấp dịch vụ, không có thông điệp trả lời cho thông điệp thông báo ủy quyền.



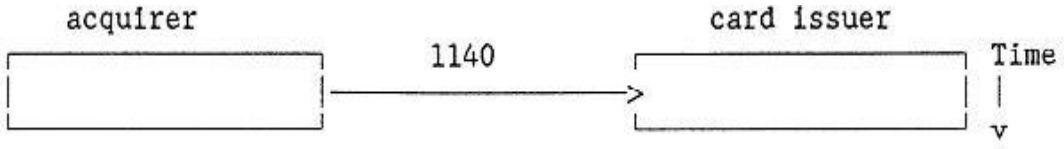
Hình 20

1100/1101: yêu cầu ủy quyền/ nhắc lại yêu cầu ủy quyền.

1110 : Trả lời yêu cầu ủy quyền.

1120/1121: Tư vấn ủy quyền/ nhắc lại tư vấn ủy quyền.

1130: Trả lời tư vấn ủy quyền.



Hình 213

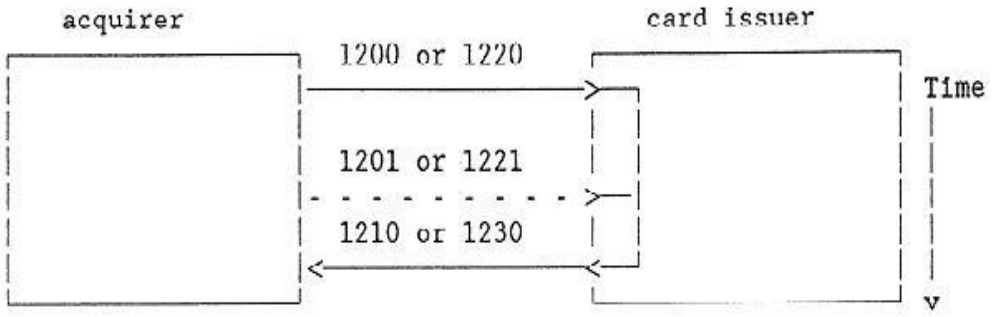
1140: Thông báo ủy quyền.

4.3.2 (12xx) Giao dịch tài chính

Giao dịch tài chính cho phép chấp thuận các ứng dụng của giao dịch tiền tệ vào tài khoản thẻ thanh toán.

Được áp dụng khi dữ liệu chứa trong các giao dịch cá nhân không đủ để cung cấp cho các thông điệp thực tế của các tài khoản tại hệ thống xử lý (card issuer).

- Thông điệp yêu cầu tài chính được dùng khi các giao dịch có thể không hoàn thành tại điểm cung cấp dịch vụ cho đến khi nhận được thông điệp trả lời cho các thao tác tiếp theo. Việc sử dụng thông điệp yêu cầu tài chính không bao hàm các dịch vụ mở rộng(ví dụ: điện thoại hoặc mail).
- Thông điệp yêu cầu tài chính hồi đáp được dùng để đáp lại Thông điệp yêu cầu tài chính, nó cho biết sự chấp thuận, sự đảm bảo về tiền tệ hoặc các thao tác được đưa vào xác định trong mã các yếu tố dữ liệu kèm theo (Data elements).
- Thông điệp tư vấn tài chính được dùng để thông báo cho bên đơn vị chấp hành thẻ (ATM) là một giao dịch tài chính đã hoàn thành tại thời điểm cung cấp dịch vụ.
- Thông điệp tư vấn tài chính hồi đáp được dùng để đáp lại thông điệp tư vấn tài chính, nếu bên đơn vị chấp hành thẻ (ATM) chấp thuận hoặc từ chối chuyển giao tài chính.
- Thông điệp thông báo tài chính được sử dụng để thông báo cho đơn vị chấp hành thẻ (ATM) khi một giao dịch tài chính đã hoàn thành tại thời điểm cung cấp dịch vụ, không có thông điệp trả lời cho thông điệp thông báo tài chính.



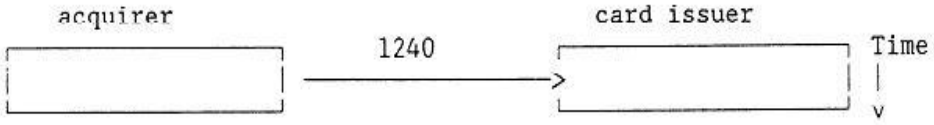
Hình 22

1200/1201: yêu cầu tài chính/ nhắc lại yêu cầu tài chính.

1210: Trả lời yêu cầu tài chính.

1220/1221: Tư vấn tài chính/nhắc lại tư vấn tài chính.

1230: trả lời tư vấn tài chính.



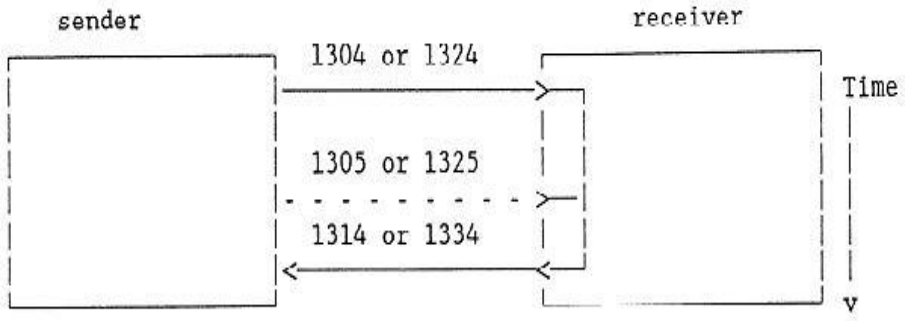
Hình 23

1240: Thông báo tài chính

4.3.3 (13xx) Tệp tin thực thi giao dịch.

Thông điệp tệp tin thực thi sẽ được dùng để thêm, thay đổi, xóa bỏ hoặc thay thế một tệp tin, hồ sơ.

Ngoài ra, thông điệp tệp tin thực thi còn có thể được sử dụng để thẩm tra một tệp tin hoặc quản lý thẻ (ví dụ: báo cáo mất thẻ)



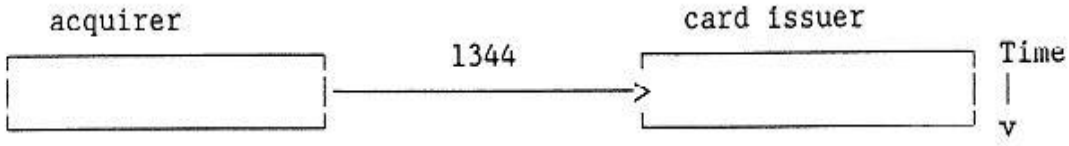
Hình 24

1304/1305: Yêu cầu tệp tin thực thi/ lặp lại yêu cầu tệp tin thực thi.

1314: Đáp lại yêu cầu tệp tin thực thi.

1324/1325: Tư vấn tệp tin thực thi/ Lặp lại tư vấn tệp tin thực thi.

1334: Đáp lại tư vấn tệp tin thực thi.

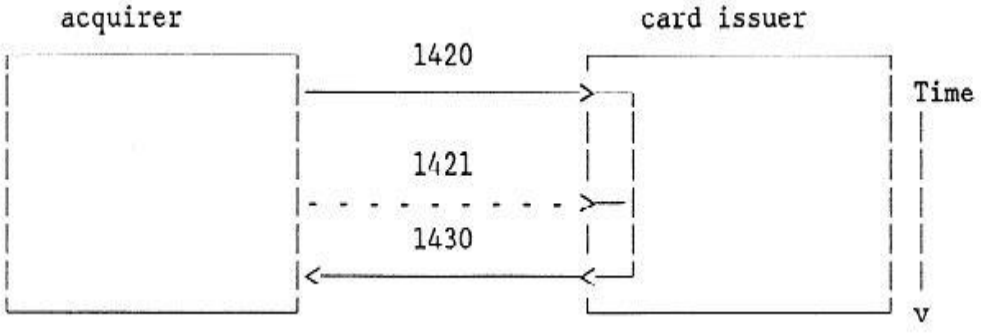


Hình 25

1344: Thông báo tệp tin thực thi.

4.3.4 (14xx) Chuyển đổi giao dịch.

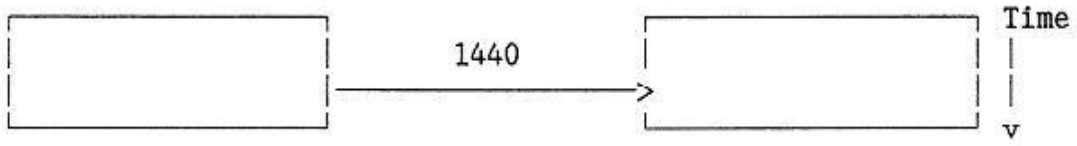
Chuyển đổi này có thể hủy bỏ 1 phần hoặc hoàn toàn giao dịch trước hoặc các ủy quyền giao dịch.



Hình 26

1420/1421: Chuyển đổi tư vấn/ Nhắc lại chuyển đổi tư vấn.

1430: Đáp lại chuyển đổi tư vấn.



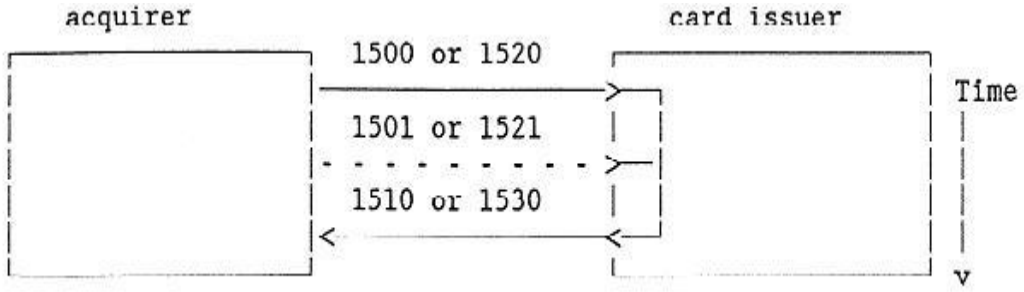
Hình 27

1440: Thông báo chuyển đổi.

4.3.5 (15xx) Phân luồng giao dịch.

Phân luồng giao dịch cung cấp tổng các giao dịch tài chính giữa 1 acquirer và 1 card issuer.

- **Acquirer => Card issuer**



Hình 30

1500/1501: Yêu cầu phân luồng từ phía acquirer/ Nhắc lại yêu cầu phân luồng từ phía acquirer .

1510: Trả lời yêu cầu phân luồng từ phía acquirer .

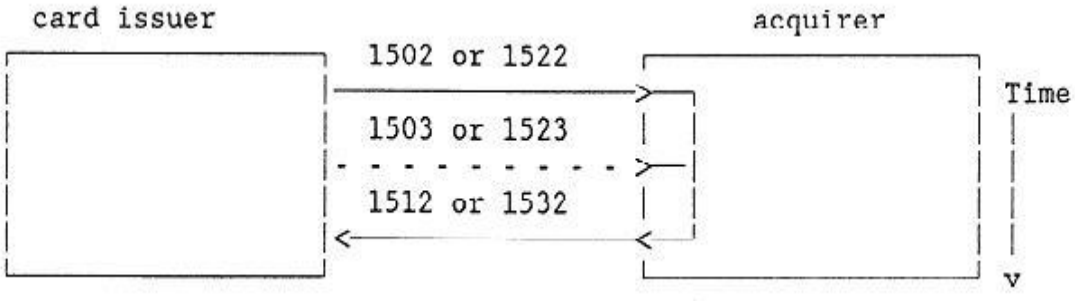
1520/1521: Tư vấn phân luồng từ phía acquirer/ Nhắc lại tư vấn phân luồng từ phía acquirer.

1530: Trả lời tư vấn phân luồng từ phía acquirer

Hình 28

1540: Thông báo phân luồng từ phía acquirer.

- **Card issuer => Acquirer**



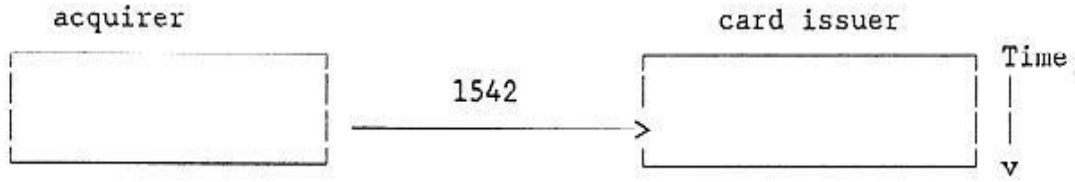
Hình 29

1502/1503: Yêu cầu phân luồng từ phía card issuer/ Nhắc lại yêu cầu phân luồng từ phía card issuer.

1512: Đáp lại yêu cầu phân luồng từ phái card issuer.

1522/1523: Tư vấn phân luồng từ phía card issuer/ Nhắc lại tư vấn phân luồng từ phía card issuer.

1532: Đáp lại tư vấn phân luồng từ phía card issuer.

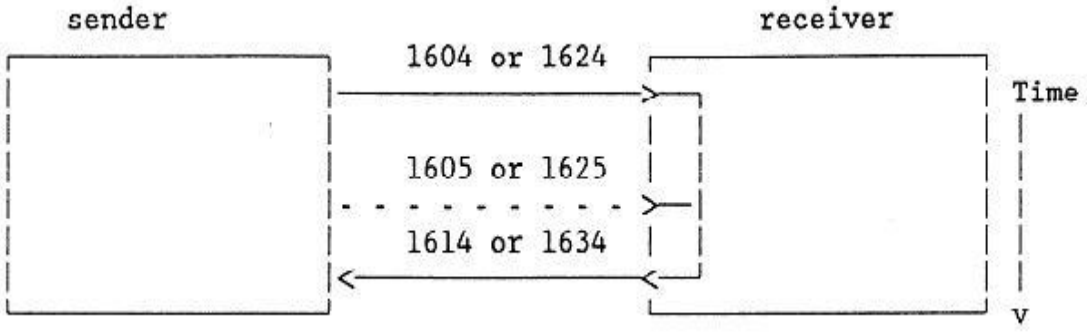


Hình 30

1542: Thông báo phân luồng từ phía card issuer.

4.3.6 (16xx) Thông điệp tư vấn quản trị

Thông điệp tư vấn quản trị được sử dụng khi có tới 2 thiết lập được xác định là cần thiết cho việc trao đổi thông tin (ví dụ: yêu cầu chuyển đổi)



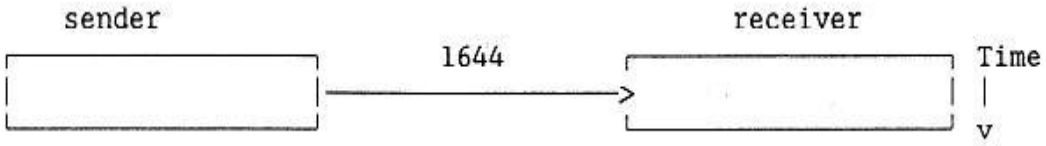
Hình 31

1604/1605: Yêu cầu quản trị/ Nhắc lại yêu cầu quản trị.

1614: Đáp lại yêu cầu quản trị.

1624/1625: Tư vấn quản trị/ Nhắc lại tư vấn quản trị.

1634: Đáp lại tư vấn quản trị.



Hình 32

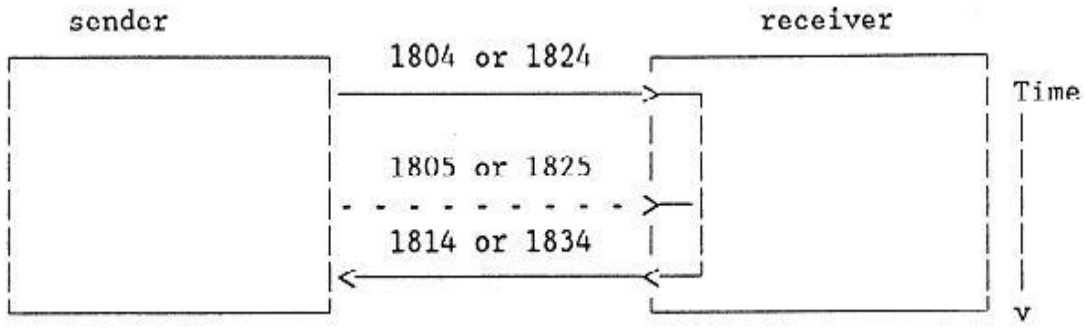
1644: Thông báo quản trị.

4.3.7 (18xx) Quản lý thông điệp mạng

Quản lý thông điệp mạng sẽ được sử dụng để kiểm soát hệ thống an ninh, điều kiện hoạt động và các thay đổi trên mạng.

- Thông điệp trạng thái hệ thống: có thể được dùng để thiết lập và báo cáo hệ thống hiện tại và đưa ra các hướng dẫn liên quan tới các thông điệp xử lý khi hệ thống không hoạt động. Thông điệp này được sử dụng như là một phần của hệ thống khởi động hoặc tắt máy hoặc như là một phần của chương trình phục hồi hệ thống.

- Thông điệp an toàn hệ thống: có thể dùng để kiểm soát an ninh của các phương diện như: hệ thống quản lý khóa, mật khẩu và cảnh báo bảo mật. Các thông điệp này có thể được sử dụng như một phần của thủ tục an ninh(ví dụ như tự động thay đổi khóa định kỳ).
- Thông điệp tài khoản hệ thống: có thể được sử dụng để xác định sự kết thúc của khoảng thời gian phân luồng. Các thông điệp này có thể được sử dụng như một phần của tiến trình phân luồng. Thông điệp tài khoản hệ thống không bị từ chối bởi người nhận, trừ khi có lý do cụ thể được quy ước trước.
- Thông điệp hệ thống kiểm soát kiểm toán: Có thể được sử dụng để kiểm tra tính xác thực của sự thay đổi các mỗi quan hệ hoặc như là một phần của sự tích hợp kiểm tra hoặc khôi phục chương trình thất bại.



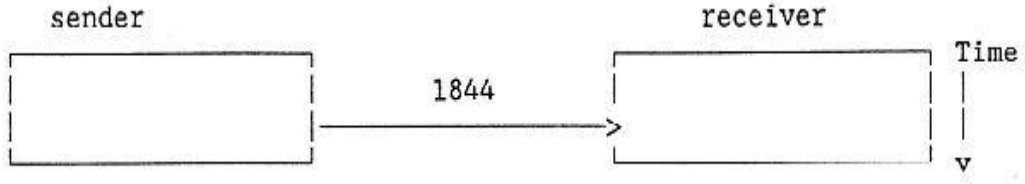
Hình 33

1804/1805: Yêu cầu quản lý mạng/ Nhắc lại yêu cầu quản lý mạng.

1814: Đáp lại yêu cầu quản lý mạng.

1824/1825: Tư vấn quản lý mạng/ Nhắc lại tư vấn quản lý mạng.

1834: Đáp lại tư vấn quản lý mạng.



Hình 34

1844: Thông báo tư vấn mạng.

CHƯƠNG 5: KẾT QUẢ NGHIÊN CỨU HỆ THỐNG

5.1 Lý thuyết

Qua quá trình nghiên cứu đề tài "**Nghiên cứu một số giải pháp Công nghệ Thông tin ứng dụng trong máy rút tiền tự động ATM**" em đã hiểu rõ được việc áp dụng công nghệ thông tin vào thực tiễn cuộc sống và qua đề tài em đã nghiên cứu kỹ nguyên lý hoạt động của hệ thống mạng ứng dụng trong việc trả tiền tự động thông qua thiết bị ATM của hệ thống ngân hàng đồng thời nghiên cứu hạ tầng viễn thông mạng cùng với nguyên lý hoạt động và cấu tạo của máy ATM. Toàn bộ các vấn đề đã tìm hiểu có thể tóm tắt thành các mục sau:

- Cơ sở lý thuyết về mạng, bảo mật, nguyên lý hoạt động.
- Bảo mật thông tin trên mạng.
- Máy ATM (Phần cứng và phần mềm) , chuyền dẫn dữ liệu, nghiệp vụ giao dịch tiền trên máy, các lưu đồ.
- Giao thức kết truyền tin giữa máy ATM với ngân hàng (ISO 8583).

5.2 Thực tiễn

5.2.1 Vấn đề bảo mật trên thẻ ATM

Vấn đề bảo mật trên thẻ ATM hiện nay còn nhiều lỗ hổng, bảo mật còn kém khả năng làm giả và sao chép cao. Kẻ gian có thể mua thẻ nhựa trắng và máy ghi thẻ qua mạng, sau đó dùng nhiều thủ đoạn đánh cắp thông tin thẻ và mật mã giao dịch của chủ thẻ. Các thủ đoạn đó có thể là dùng phần mềm lập các trang web giả của các công ty bán hàng qua mạng, sử dụng các thiết bị copy thẻ chuyên dụng và ngụy trang chúng nhằm copy thông tin thẻ, giá trung bình một bộ thiết bị làm thẻ ATM giả nếu tìm mua đúng địa chỉ mất khoảng 25 USD với giá rẻ như vậy việc làm thẻ giả là điều tương đối dễ dàng.

Vì thẻ ATM sử dụng công nghệ thẻ từ có nhiều nhược điểm về bảo mật như vậy nên phía ngân hàng đã sử dụng "Chữ ký điện tử" để nhận diện thẻ ATM vật lý nên cho dù kẻ gian có mã PIN, có tên khách hàng, có số tài khoản mà không có chiếc thẻ vật lý thì vẫn không có cách nào tạo thẻ giả được.

Lý do là trên các track của thẻ, ngoài thông tin về khách hàng ra, còn có thông tin đã được mã hóa kèm theo "chữ ký điện tử" mà ngân hàng ghi xuống thẻ để xác định danh tánh khách hàng, cũng như phát hiện và ngăn chặn một người cố tình thay đổi dữ liệu trên thẻ.

Quá trình tạo và phát hành thẻ của ngân hàng cũng hoạt động tự động hoàn toàn dựa trên thiết bị Hardware Security Module, nên ngay cả nhân viên ngân hàng cũng không thể nào tạo chữ ký điện tử hay giải mã được các track thông tin đã mã hóa này.

Riêng về mã PIN thì do việc làm giả thẻ từ ATM rất dễ nên người ta phải sử dụng mã PIN và công nghệ mã hóa để bảo mật giao dịch. Tuy nhiên, kẻ gian có thể dùng các đầu đọc thẻ ngụy trang để copy thẻ vật lý của khách hàng. Các thẻ này tuy là thẻ giả song nó lại mang thông tin và số PIN của thẻ thật, vì vậy hoàn toàn tương thích khi thực hiện các giao dịch rút tiền tại máy rút tự động.

ATM dễ bị trộm là do sử dụng thẻ từ thiếu tính bảo mật, nếu sử dụng công nghệ thẻ chip sẽ an toàn hơn vì mức độ bảo mật của thẻ chip gấp 13 lần thẻ từ. Về mặt công nghệ, thẻ chip giống một máy tính, có thể lưu trữ và xử lý thông tin. Tuy nhiên, vấn đề nan giải là thẻ chip mắc hơn 3- 4 lần so với thẻ từ, và các ngân hàng muốn sử dụng loại thẻ này phải đầu tư lại toàn bộ hệ thống máy móc với chi phí khổng lồ.

Tuy nhiên xét về khía cạnh bảo mật và những thiệt hại nếu xảy ra thì nên chọn công nghệ thẻ sử dụng chip, tuy có đầu tư tốn kém hơn thẻ Từ nhưng với những tiện lợi và mức độ an toàn mà nó đem lại thì thực sự đáng để lưu tâm.

5.2.2 Vấn đề bảo mật trong quá trình truyền dữ liệu giữa ATM với ngân hàng.

Còn về vấn đề bảo mật trong quá trình truyền dẫn dữ liệu giữa máy ATM với ngân hàng em thấy rằng tương đối an toàn do tất cả dữ liệu truyền giữa máy ATM và hệ thống máy chủ của ngân hàng đều được mã hóa bằng các chuẩn mã hóa do chính Viện Tiêu chuẩn và Công nghệ Mỹ (NIST) ban hành như AES (Advanced Encryption Standard) hay 3DES (Triple Data Encryption Standard).

Tất cả công đoạn mã hóa và giải mã dữ liệu truyền từ máy ATM về hệ thống máy chủ của ngân hàng đều được thực hiện bởi các thiết bị chuyên dụng (trong chuyên môn người ta gọi là Hardware Security Module). Các thiết bị này được thiết kế như một hộp đen, lưu trữ key để giải mã và mã hóa dữ liệu một cách hoàn toàn tự động, không tiết lộ bất kỳ thông tin nào ra bên ngoài, kể cả nhân viên của ngân hàng cũng không biết được nên có thể yên tâm về tính bảo mật của nó

Qua kết quả nghiên cứu kiến thức trong đồ án có thể là tài liệu tham khảo chuyên sâu cho những ai quan tâm đến lĩnh vực này. Do thời gian tìm hiểu đề tài không nhiều và với trình độ còn hạn chế nên em không tránh khỏi những thiếu xót, em rất mong nhận được sự chỉ bảo, góp ý tận tình từ phía Thầy Cô.

Em xin chân thành cảm ơn!

Tài liệu tham khảo

[1]. ISO8583-1993

[2]. ISO 8583 - A layman's guide to understanding the iso 8583 financial transaction message.

[3]. ISO8583-1987MessDef.

[4]. Atm Flowchart v1.1.

[5]. Tài liệu Mã hóa RSA.

[6]. Giáo trình thiết kế và xây dựng mạng LAN và WAN – *Trung tâm khoa học tự nhiên và công nghệ quốc gia viện công nghệ thông tin.*

[7]. Mạng internet.