LỜI CẢM ƠN

Trước hết em xin gửi lời cảm ơn đến TS. Hồ Văn Canh, người thầy đã hướng dẫn em rất nhiều trong suốt quá trình tìm hiểu và hoàn thành đồ án này từ lý thuyết đến ứng dụng của hệ thống ATM.

Đồng thời em cũng xin chân thành cảm ơn các thầy cô trong bộ môn cũng như các thầy cô trong trường đã trang bị cho em những kiến thức cơ bản cần thiết để em có thể hoàn thành tốt đồ án này.

Em xin gửi lời cảm ơn đến các thành viên lớp CT1001, những người bạn đã luôn ở bên cạnh động viên, tạo điều kiện thuận lợi và cùng em tìm hiểu, hoàn thành tốt đồ án.

Sau cùng, em xin gửi lời cảm ơn đến gia đình, bạn bè đã tạo mọi điều kiện để em xây dựng thành công đồ án này.

Hải Phòng, ngày 07 tháng 07 năm 2010

Sinh viên thực hiện

LƯƠNG TIẾN ĐÔNG

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

ATM	Automatic Teller Machine
BIN	Bank Identification Number
CVK	Card Verification Keys
CD	Check digit
CSDL	Cơ sở dữ liệu
DES	Data Encryption Standard
3DES	Triple DES
EMV	Eropay, MasterCard, Visa
EPP	Encrypt PIN Pad
HSM	Hardware Security Module
ISO	International Organization for Standardization
LMK	Local Master Keys
MD	Message Digest algorithm
MAC	Message Authentication Code
NH	Ngân hàng
PC	Personal Computer
POS	Point Of Service
PIN	Personal Identification Number
PAN	Primary Account Number
PVV	VISA PIN Verification Keys
PVK	PIN Verification Keys
RSA	Rivest, Shamir và Adleman
TMK	Terminal Master Keys
WK	Working Keys

MỤC LỤC

LỜI MỞ ĐẦU

Ngày nay, công nghệ ATM đang được ứng dụng rộng rãi trên phạm vi toàn thế giới và cả ở Việt Nam. Tại Việt Nam, năm 2009, Chính phủ ta đã ra quyết định trả tiền lương cho các cán bộ nhân viên qua thẻ ATM. Và hiện nay, rất nhiều cán bộ hưu trí của chúng ta đã nhận tiền lương qua thẻ ATM. Điều đó nói lên tầm quan trọng của công nghệ ATM. Có hai loại thẻ ATM được ứng dụng rộng rãi trên thế giới là thẻ từ và thẻ chip. Ở Việt Nam ta hiện nay chủ yếu là ứng dụng thẻ từ. Một trong những vấn đề đặt ra cho hệ thống ATM là vấn đề đảm bảo ATTT cho hệ thống. Nhận thấy tầm quan trọng và tính cấp thiết của nó nên qua tìm hiểu em đã chọn đề tài "Tìm hiểu hệ thống ATM và cơ chế ATTT cho hệ thống" làm đề tài đồ án tốt nghiệp của em. Trong đó, em tập trung tìm hiểu sâu 3 vấn đề sau đây:

Chương 1. Tìm hiểu tổng quan về hệ thống ATM.

Chương 2. Tìm hiểu sâu về hệ thống thanh toán bằng ATM đối với thẻ từ.

Chương 3. Tìm hiểu cơ chế ATTT trong hệ thống ATM.

Do tài liệu tham khảo chủ yếu là tiếng Anh, còn những tài liệu có tính chuyên ngành thì tiếng Việt rất hiếm. Trong lúc đó khả năng đọc hiểu của em bằng tiếng Anh còn nhiều hàn chế. Thêm vào đó, đề tài đồ án của em lại đụng đến các kiến thức toán học phức tạp, đặc biệt là lý thuyết số, lý thuyết về nhóm vành, trường. Do vậy, trong báo cáo đồ án của em chắc chắn còn nhiều thiếu sót. Em rất mong được quí các thầy, cô giúp đỡ, góp ý chỉ bảo để em có thể hoàn thiện đồ án của mình hơn nữa.

Chương 1. TÌM HIỂU TỔNG QUAN VỀ MÁY ATM

1.1. TỔNG QUAN VỀ MÁY ATM

1.1.1 Giới thiệu máy ATM (Automatic Teller Machine)

Máy rút tiền đầu tiên trên thế giới được thiết kế và hoàn thành bởi Luther George Simjian (Người Thổ Nhĩ Kỳ), vào năm 1939, máy được thiết kế tại thành phố NewYork cho ngân hàng City Bank of NewYork, nhưng 6 tháng sau thì bị bỏ đi vì ít người dùng.

Sau 25 năm, vào ngày 27/6/1967, máy rút tiền điện tử đầu tiên được hãng In-De- la- Rue thiết kế tại Enfield Town (gần London - Anh) cho ngân hàng Barclays Bank. Người phát minh là John Shepherd-Barron mặc dù Luther George Simjian và một vài người khác cũng đã đăng ký văn bằng phát minh cho loại máy này. Tuy nhiên, nhiều người cho rằng loại máy ATM đầu tiên theo đúng nghĩa ATM mà thế giới ngày nay đang sử dụng chính là loại máy được ra mắt vào năm 1969 tại Ngân hàng Chemical Bank ở NewYork (Mỹ). Tác giả là Don Wetzel, phó giám đốc một công ty chuyên về máy tự động xử lý hành lý.

ATM ngày nay là thiết bị để ngân hàng giao dịch chủ 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.

1.1.2 Tình hình sử dụng hệ thống ATM

Thanh toán tiền qua hệ thống ATM đã phổ biến trên toàn thế giới và ở Việt Nam hệ thống ATM cũng đang dần phổ biến.

Năm 1993, thị trường thẻ ngân hàng Việt Nam mới xuất hiện những sản phẩm thẻ đầu tiên do Vietcombank phát hành, đến năm 1996 thì thị trường thẻ bắt đầu thực sự xuất hiện.

Năm 1996, Ngân hàng ngoại thương Việt Nam Vietcombank (VCB) kết hợp cùng ngân hàng nhà nước lắp đặt 2 chiếc máy rút tiền tự động (ATM) tại Hà Nội.

Đến nay, chúng ta đã chứng kiến sự phát triển vượt bậc của thị trường 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 thương mại phát hành thẻ Quốc Tế.

Bảng 1.1 Số liệu thống kê thị trường thẻ Viêt Nam qua các năm

(*Theo hiệp hội ngân hàng Việt Nam và hội thảo Banking Viêt Nam 2008*)

Đơn vị: chiếc

Năm	**Số lượng thẻ phát hành gồm thẻ nội địa và quốc tế**	**Số máy ATM**
1996	360	
1997	460	
1998	4.500	
1999	2.500	
2000	5.000	
2001	15.000	
2002	40.000	
2003	230.000	
2004	560.000	
2005	1.250.000	
T6/2006	3.500.000	
2007	8.400.000	4.020
T3/2008	10.000.000	4.500

Tại hội thảo Banking Việt Nam 2008 diễn ra tại Hà Nội, Ngân hàng nhà nước đã công bố số liệu thống kê về thị trường 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.

Những tiện ích mà các dịch vụ thẻ mang lại đã góp phần từng bước thay đổi thói quen ưa sử dụng tiền mặt của người dân, giảm chi phí xã hội, nâng cao khả năng quản

lý tiền tệ của NH cũng như góp phần hữu ích vào việc tạo dựng nền móng cho sự hình thành một nền thương mại điện tử còn non trẻ của nước ta.

Việc còn quá ít máy ATM được một số ít các ngân hàng triển khai cũng không quá khó lý giải.Với mức chi phí đầu tư cho một máy ATM từ 20.000 USD đến 30.000 USD, không phải ngân hàng nào, nhất là các ngân hàng thương mại cổ phần cũng có thể đầu tư, nếu họ không " trường vốn " và không có chiến lược phát triển ATM.

1.1.3. Lợi ích và các dịch vụ trên máy ATM

1.1.3.1. Lợi ích đối với ngân hàng

ATM được biết đến như là một kênh tự phục vụ của ngân hàng,là một bộ phận chiến lược trong kênh phân phối của ngân hàng, giúp cho chủ thể truy cập một cách thuận tiện các dịch vụ được nhanh chóng, dịch vụ 24/7 ở bất cứ nơi đâu và vào thời gian nào.

Bên cạnh đó, máy ATM còn có một số ưu điểm sau:

- Các địa điểm đặt máy thuận lợi, thời gian phục vụ 24/24 giúp dễ tiếp cận với các dịch vụ ngân hàng, nên thu hút nhiều chủ thẻ hơn.
- Đối với mỗi máy ATM có thể coi là một "chi nhánh" của ngân hàng, do đó sẽ giảm thiểu chi phí vận hành chi nhánh ngân hàng.

Nhờ vậy, mà các ngân hàng có thể giữ được khách hàng cũ và thu hút được nhiều người sử dụng các dịch vụ ngân hàng.

1.1.3.2. Lợi ích đối với khách hàng

- Thuận tiện trong tiếp cận ngân hàng(địa điểm, 24x7 giờ).
- Nhanh hơn so với ở quầy giao dịch.

1.1.3.3. Các dịch vụ trên máy ATM

- Rút tiền mặt (Cash Withdrawal).
- Chuyển khoản (Fund Transfer).
- Tiện ích / Thanh toán hóa đơn (Điện thoại, Điện, Nước,…..)
- Gửi tiền.
- Các giao dịch Internet / Thương mại điện tử.

1.1.4. Một số vấn đề đối với hệ thống ATM

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.

Hiện nay, trên thế giới và cũng như ở Việt Nam thẻ từ vẫn chiếm một số lượng lớn so với thẻ chíp (thẻ thông minh). Do chi phí phát hành thẻ từ rất rẻ so với thẻ chíp nên hiện tại thẻ từ vẫn chiếm lĩnh thị trường thẻ.

Đối với thẻ chíp, hiện nay (8/2008) đã có một vài ngân hàng phát hành như VIB, VCD nhưng với số lượng rất ít và chủ yếu dùng cho thẻ tín dụng.

Tuy nhiên, những vấn đề rủi ro và gian lận thẻ đang đặt cho Ngân hàng một thách thức lớn, thẻ từ bộc lộ nhiều hạn chế về khả năng an toàn, lưu trữ thông tin cũng như tích hợp các ứng dụng, dịch vụ trên thẻ.

Thẻ từ rất dễ bị sao chép, chỉ với một bảng mạch điện tử 2 đầu đọc băng từ hoặc với công nghệ "hộp đen" phân tích tín hiệu từ đầu vào và đầu ra, tội phạm có thể làm ra những chiếc thẻ tương tự. Ngoài việc bị lấy cắp trực tiếp từ việc đọc trên băng từ, dữ liệu còn có thể bị đánh cắp từ trên đường truyền bưu điện mà Ngân hàng thuê.

Cũng không loại trừ trường hợp người của các Ngân hàng thông đồng với tội phạm để cài đặt các thiết bị lấy cắp dữ liệu vào máy ATM, từ đó lấy cắp dữ liệu thẻ của khách hàng. Không những vậy, bọn trộm còn gắn những camera bé xíu cho phép quay cận cảnh bàn phím trên ATM để ăn cắp số PIN (mật mã) truy cập tài khoản của chủ thẻ.

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 tư đó rút hết tiền do chủ thẻ đã đặt mã PIN là những con số dễ nhớ như ngày sinh, số CMT…

Ngoài ra phát sinh các vấn đề mới, những thông tin dữ liệu nằm ở CSDL 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 NH do vậy việc đảm bảo an toàn an ninh thông tin trên hệ thống ATM đóng một vai trò đặc biệt quan trọng.

Để giải quyết vấn đề trên, thì ***An toàn thông tin*** cho hệ thống ATM được đặt ra cấp thiết.

Do đó, mục đích của đồ án là tìm hiểu sâu hơn về cơ chế hoại động và bảo mật của hệ thống, trên cơ sở đó đề xuất lựa chọn giải pháp nhằm nâng cao tính bảo mật an toàn cho hệ thống ATM.

1.2. CẤU TẠO MÁY ATM

1.2.1 Định nghĩa ATM

1.2.1.1. Định nghĩa ATM (Automatic Teller Machine)

ATM được gọi là hệ thống giao dịch ngân hàng tự động, không đơn thuần là máy rút tiền mà còn nhiều dịch vụ khác như chuyển khoản, thanh toán hóa đơn, mua vé, các dịch vụ thương mại điện tử….

Hình 1.1 Máy ATM

1.2.1.2. Phân loại

1/. Theo vị trí

- ATM đặt tại sảnh, hành lang.
- ATM độc lập.
- ATM thường xuyên.
- ATM đặt tại nơi thu vé xe.

2/. Theo chức năng

- Máy chỉ có chức năng trả tiền.
- Máy có các chức năng cao cấp.

1.2.1.3. Luồng xử lý giao dịch trong hệ thống ATM

1/. Các bước xử lý giao dịch

- Chủ thẻ thực hiện giao dịch.
- ATM nhận thông tin giao dịch và gửi lệnh yêu cầu tới Switch.
- Switch nhận yêu cầu, xử lý và phản hồi lại lệnh cho ATM.
- ATM nhận lệnh phản hồi từ Switch và thực hiện lệnh.
- ATM nếu không thực hiện lênh được lệnh phản hồi sẽ gửi hủy lệnh đã yêu cầu.
- Switch sẽ chấp nhận lệnh hủy yêu cầu.

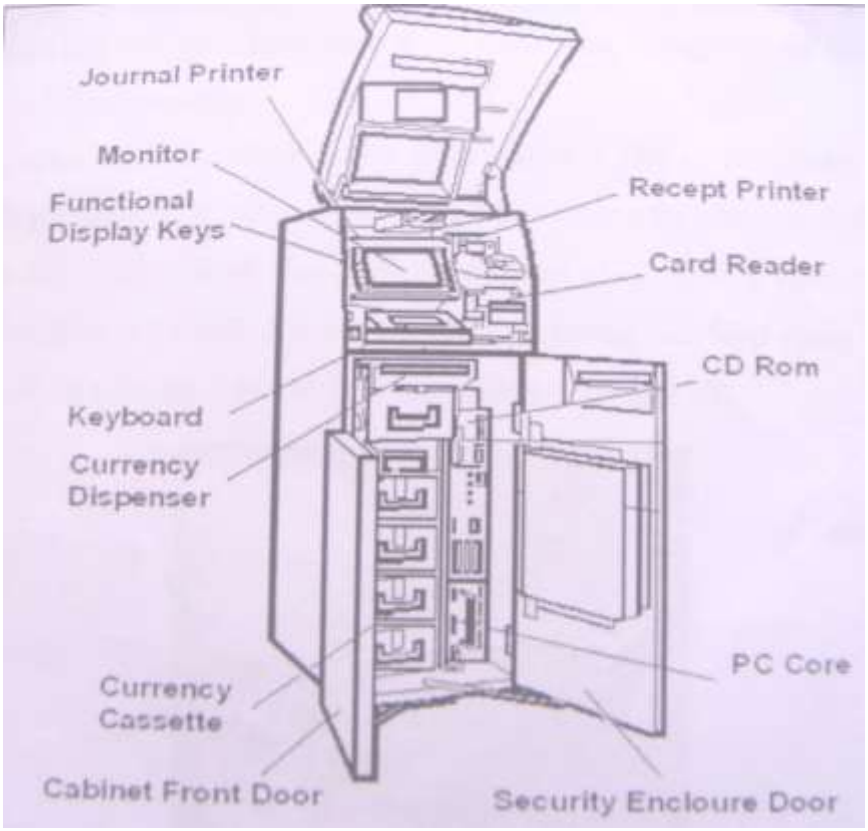
2/. Luồng giao dịch của hệ thống ATM

- Màn hình đợi (màn hình hiển thị quảng cáo của ngân hàng).
- Cho thẻ vào ATM và nhận số PIN.
- Kiểm tra số thẻ: Kiểm tra số Check Digit, kiểm tra số CVV/CVC.
- Kiểm tra PIN: Kiểm tra số PIN được nhập vào với PIN được lưu trong CSDL Core Bank của ngân hàng. Nếu đúng, sẽ hiển thị các loại giao dịch để chủ thẻ lựa chọn.
- Thực hiện giao dịch: Khi thực hiện thành công, thì tùy theo từng loại giao dịch mà ATM nhả thẻ hoặc không (Thường rút tiền xong thì ATM sẽ nhả thẻ ra).
- Trở về màn hình đợi: Khi không thực hiện các giao dịch nữa (khi nhả thẻ hoặc nuốt thẻ) màn hình ATM trở về trạng thái ban đầu.

1.2.2. Cấu tạo máy ATM

ATM là một thiết bị chuyên biệt được sử dụng trong lĩnh vực ngân hàng, được gọi là kênh phục vụ tự động của ngân hàng. Do đó, nó cần có một cấu tạo đặc biệt để có thể thực hiện các chức năng được yêu cầu.

Cấu tạo máy ATM gồm 2 phần là Phần cứng và Phần mềm:



Hình 1.2 Cấu tạo máy ATM

1/. Phần cứng

Bao gồm máy vi tính chuyên biệt, thiết bị đếm tiền, thiết bị trả tiền, thiết bị in nhật ký, thiết bị in biên lai, phím nhập mật mã, thiết bị đọc thẻ, hộp đựng tiền và két sắt chứa hộp đựng tiền….

2/. Phần mềm

Máy ATM đều có hệ điều hành (OS-operate system), phần mềm điều khiển thiết bị của máy ATM, phần mềm tiện ích kèm theo.

Hiện nay, hệ điều hành là Window NT, Window XP.

1.2.2.1. Màn hình

Có thể là màn hình CRT, màn hình LCD. Ví dụ

- Màn hình của Deibold 10.4” Color LCD (XGA).
- Màn hình của NCR 9” LCD text only or 9.5” VGA flat panel LCD.

1.2.2.2. Bộ phận trả tiền

Đây là bộ phận hết sức quan trọng của mỗi máy ATM, giúp máy phân loại, đếm và cung cấp tiền cho chủ thẻ. Bao gồm máy đếm tiền, băng truyền tải và khe trả tiền được đặt trên các hộp đựng tiền.

Khi thực hiện rút tiền, phần mềm điều khiển ATM sẽ tính toán số tiền được trả theo nhiều mệnh giá tiền khác nhau, được cấu hình theo yêu cầu của ngân hàng.

Máy đếm tiền chủ yếu sử dụng kỹ thuật đếm chân không (kéo tiền lên bằng lực hút), ngoài ra còn dùng kỹ thuật ma sát để lấy tiền trong các hộp đựng tiền. Máy có thể trả được 40 đến 50 tờ tiền và 1 đến 4 loại tiền trong một lần trả.

1.2.2.3. Bàn phím

1/. Bàn phím chức năng

Hình 1.3 Bàn phím chức năng

Là loại bàn phím thực hiện các giao dịch.

Chủ thẻ sử dụng bàn phím này để nhập mã PIN, số tiền giao dịch, số tài khoản…

Nếu chủ thẻ nhập số PIN sai 3 lần liên tiếp, máy ATM sẽ tự động nuốt thẻ(tùy thuộc chính sách NH), nhằm đảm bảo an toàn trong trường hợp thẻ bị đánh cắp và cố tình dò số PIN.

Bàn phím của máy ATM cũng chính là một thiết bị mã hóa theo thuật toán DES hay TripleDES bằng thiết bị phần cứng.

2/. Bàn phím kí tự

Là loại bàn phím dùng để nhập tham số cho hệ thống phần mềm ATM (như bàn phím thông thường của máy PC). Được dùng cho nhà quản trị.

1.2.2.4. Đầu Đọc thẻ

Dùng để đọc các thông tin trên rãnh từ ở mặt sau của thẻ. Các thông tin náy sẽ được gắn vào thông điệp và chuyển đến ngân hàng nơi chủ thẻ mở tài khoản.

Đầu đọc thẻ được thiết kế để có thể đọc được hai loại là thẻ từ và thẻ chip.

1.2.2.5. Máy ghi nhật ký giao dịch

Ghi lại thông tin toàn bộ các giao dịch được thực hiện tại máy ATM.

Các thông tin này sẽ được sử dụng để kiểm soát và đối chiếu khi kiểm quỹ và yêu cầu tra soát của chủ thẻ.

1..1.1. Máy in biên lai giao dịch

Thông thường sau mỗi giao dịch máy sẽ tự động in biên lai, giúp người sử dụng ATM dễ dàng nắm bắt được thông tin của lần giao dịch đó.

Thông tin trên biên lai giao dịch tùy thuộc ngân hàng và tùy theo từng loại giao dịch. Thông thường bao gồm: tên ngân hàng, ngày tháng giao dịch, mã máy ATM, khối lượng giao dịch…

1..1.2. Máy PC (core) điều khiển

Là máy tính PC chuyên dụng, được dùng cho máy ATM.

Máy PC này thông thường chạy hệ điều hành Windows XP hoặc Windows NT. (Hiện thời Microsoft ngừng hỗ trợ hệ điều hành Windows NT nên các dòng máy mới dùng hệ điều hành Windows XP).

Trên mỗi PC sẽ cài đặt phần mềm để kiểm soát các hoạt động của ATM.

- Với máy Diebold là Agilis^{TM}
- Với máy NCR là APTRA

Ví dụ cấu hình máy PC của Diebold và NCR: (tính đến năm 2007)

Bảng 1.2 So sánh cấu hình giữa hai máy PC của Diebold và NCR

Dòng máy Opteva của Diebold	Dòng máy của NCR
- Pentium 4 3Ghz (sk 775) (Codename Denver), 800 system bus speed. - 256MB DDR standard memory. - USB 2.0 Architecture. CD ROM Read/Write - 80Gb SATA HDD. - Intel Mainboard with 915 chipset family for Diebold only. - OS Windows XP.	- PIII 700 Mhz, or a PIII 850Mhz processor. - 128 MB RAM expandable to 256 MB - Read Only CD ROM. - Mixed Architecture (SDC and USB) - OS windows NT or XP.

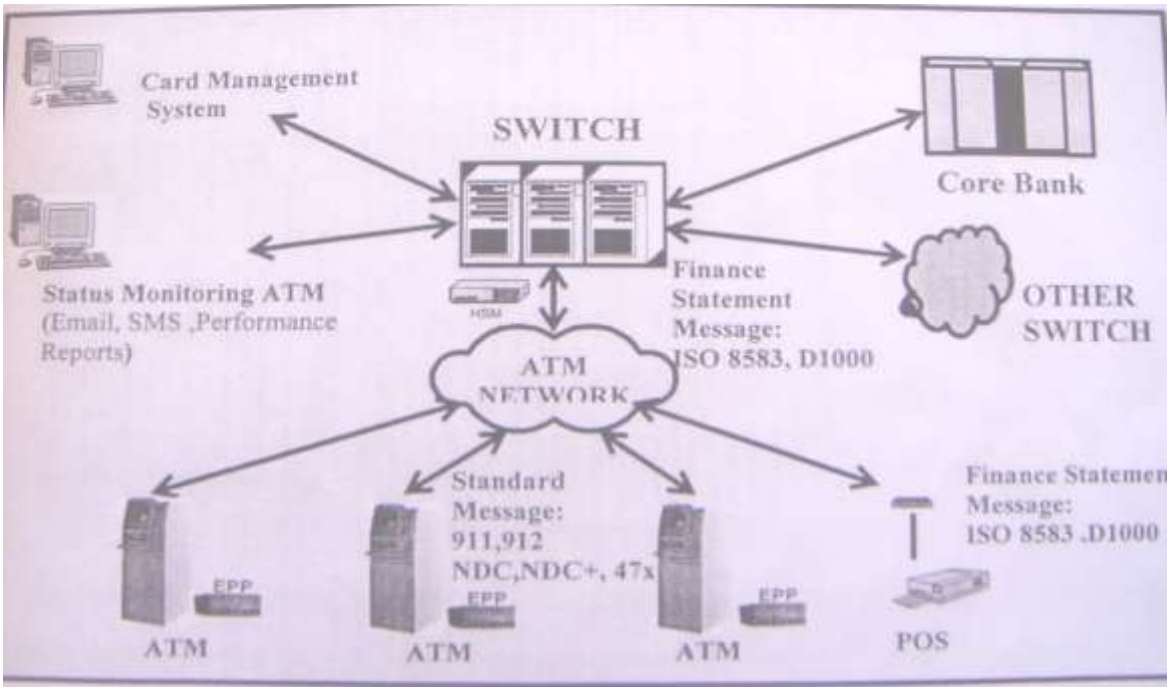
1..1.3. Khay chứa tiền

Mỗi máy ATM thường có 4 đến 5 khay đựng tiền, tùy theo nhà sản xuất. (NCR có 4, Deboil có 5) mỗi khay đựng tiền sẽ được cấu hình theo từng mệnh giá tiền khác nhau. Ngoài ra máy còn có các hộp để đựng tiền xu.

Mỗi khay đựng tiền thường chứa khoảng 3000 đến 4000 tờ tiền.

1.2.3 Mạng lưới ATM

Mạng lưới ATM là hệ thống mạng gồm có các thành phần trung tâm như Switch, CoreBank và các hệ thống mạng viễn thông dùng để kết nối các thiết bị thanh toán nhằm giúp cho khách hàng truy cập thuận tiện các dịch vụ một cách nhanh chóng, dịch vụ 24x7 ở bất cứ nơi đâu và vào thời gian nào. Ngoài ra có thể kết nối đến hệ thống mạng của NH khác.



Hình 1.4 Sơ đồ mạng lưới ATM

1.2.4. Giao thức kết nối hệ thống máy ATM

Mỗi ATM được coi như là một máy PC, do đó mỗi ATM có một địa chỉ IP xác định để có thể tham gia vào mạng, có thể đặt địa chỉ IP tĩnh hoặc IP động.

Hiện nay máy ATM hỗ trợ giao thức kết nối như là TCP/IP, X.25,….

Ở Việt Nam, máy ATM sử dụng giao thức TCP/IP để kết nối. Các giao thức này được hỗ trợ bởi các đường truyền thông như đường Lease-line, mega wan, Dial-up….

1.2.5. Hệ thống Switch

Switch rất quan trọng trong hệ thống ATM, cũng như các giao dịch tài chính khác. Switch là trung tâm của toàn bộ hệ thống, là một thành phần trung gian giữa ATM và cơ sở dữ liệu của ngân hàng. Mọi giao dịch từ ATM đều thông qua Switch.

Switch: Là hệ thống định tuyến các giao dịch tài chính bắt nguồn từ các kênh phân phối dịch vụ như: máy ATM, POS, Telephone Banking, Internet Banking,….

Hệ thống gồm phần mềm và phần cứng (Thường được gọi là hệ thống chuyển mạch) được kết nối trực tiếp với Core bank và các thiết bị đầu cuối ATM, POS.

Hệ thống này gômg mốt số chức năng sau:

- Quản lý thẻ (Card Management): cho phép kết nối đến hệ thống quản lý các thiết bị sản xuất thẻ, giám sát và quản lý các thẻ được phát hành.
- Kết nối các thiết bị đầu cuối như ATM, POS,…
- Giám sát và điều khiển toàn bộ hệ thống.
- Ghi nhật ký và lưu vết giao dịch.
- Hệ thống cung cấp các giao tiếp với thiết bị mã hóa cứng HSM, đảm bảo mã hóa và giải mã số PIN và xác thực các thông điệp.
- Kết nối đến các ngân hàng hay các tổ chức phát hành khác như VISA, Master Card, Euro Pay…

Core Bank

Hệ thống NH cốt lõi, là nơi tập trung CSDL thông tin về ngân hàng và thông tin về tài khoản, kiểu tài khoản số dư tài khoản, số hạn mức tài khoản của chủ thẻ tham gia vào hệ thống NH.

ATM (Automatic Teller Machine)

Là một kênh tự phục vụ thông qua thẻ của ngân hàng, như cho phép rút tiền tự động, chuyển khoản, thanh toán hóa đơn, mua vé, các dịch vụ thương mại, điện tử,,,

POS (Point of Service)

Là điểm thanh toán mua hàng bằng thẻ thanh toán.

Chương 2. HỆ THỐNG THANH TOÁN BẰNG MÁY ATM CHO THẺ TỪ

2.1. THẺ TỪ

Là loại thẻ nhựa cứng, các thông tin về thẻ được lưu trên băng từ. Thẻ có thể thực hiện được các giao dịch tự động như kiểm tra số dư, rút tiền, chuyển khoản v.v từ máy rút tiền ATM.

2.1.1. Tính chất vật lý của thẻ

Các tính chất vật lý của thẻ từ (kích cỡ, khối lượng, cấu trúc vật liệu, tính chất cứng, tính mềm dẻo, tính bền…) tuân theo tiêu chuẩn ISO 7810.

Chuẩn ISO 7810 là tập các chuẩn mô tả các đặc tính vật lý và kích cỡ của thẻ.

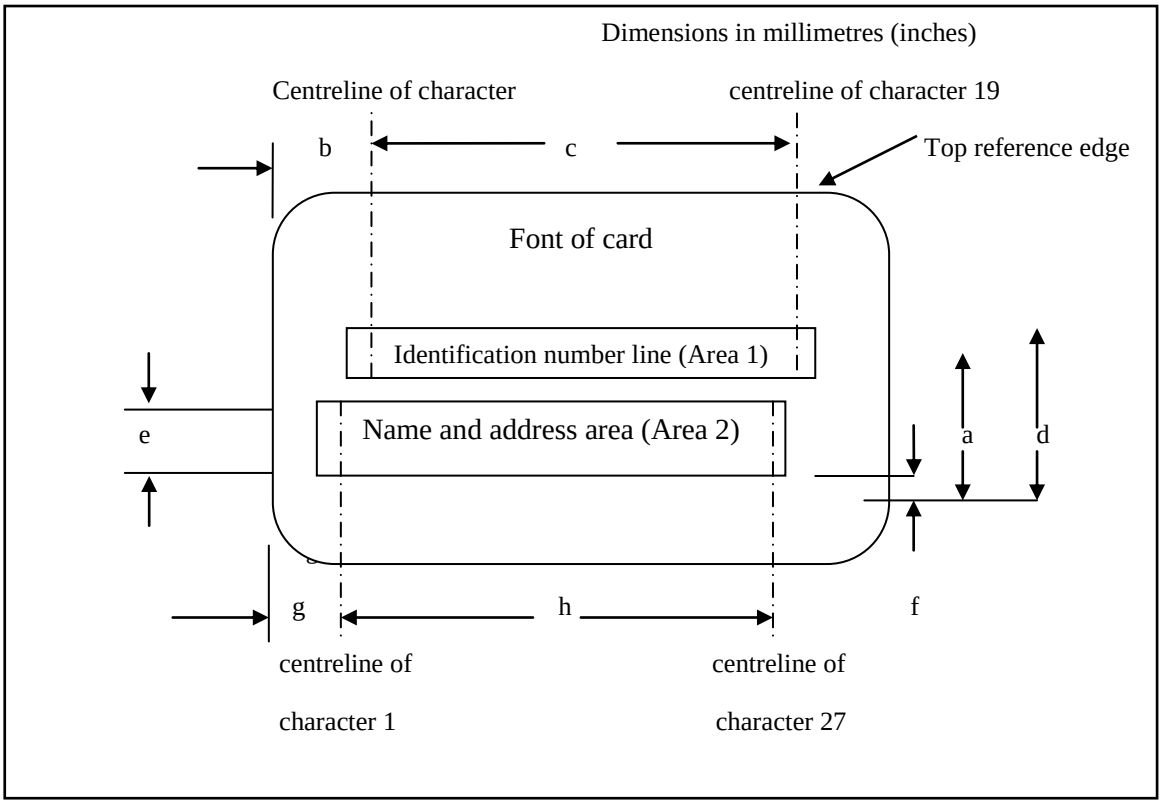
- Thẻ có 4 loại kích thước khác nhau:

+ ID-000 : Dài 25 mm Rộng 15 mm dầy 0.76mm
+ ID-1 : Dài 85.60 mm Rộng 53,98 mm dầy 0.76mm
+ ID-2 : Dài 105 mm Rộng 74 mm dầy 0.76mm
+ ID-2 : Dài 125 mm Rộng 88 mm dầy 0.76mm

Thẻ ATM là loại thẻ ID-1

2.1.2. Thông tin dập nổi trên thẻ

Các thông tin dập nổi trên thẻ tuân theo chuẩn ISO 7811-1



Bảng 2.1: Bảng định nghĩa kích thước vị trí dập nổi, đơn vị milimet (Inches)

Identification number line (Area 1)		**Identification number line (Area 2)**	
a	21,42 ± 0,12 (0.843 ± 0.005)	e	14,53 (0.572) maximum
b	10,18 ± 0,25 (0.401 ± 0.010)	f	2,54 (0.100) minimum 3,30 (0.130) maximum
c	65,31 ± 0,76 (2.571 ± 0.030)	g	7,65 ± 0,25 (0.301 ± 0.010)
d	24,03 (0.946) maximum	h	66,04 ± 0,76 (2.600 ± 0.030)

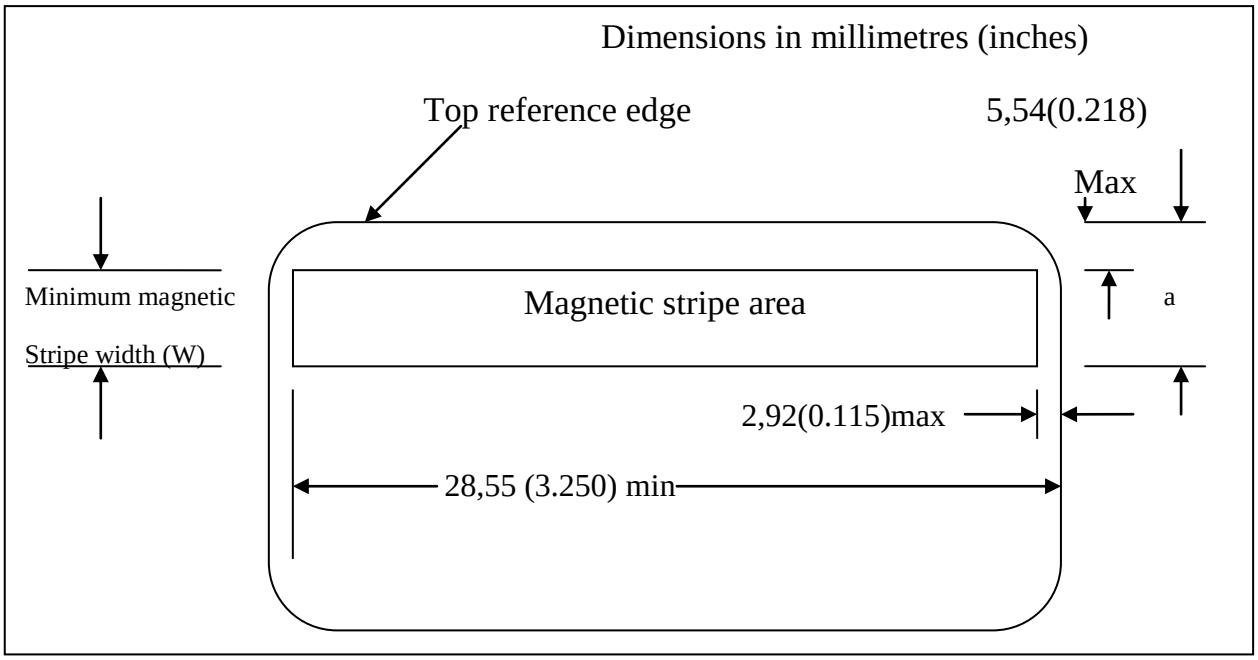
Trên thẻ có 2 khu vực dập nổi

- Khu vực 1: số định dạng thẻ PAN, được dập nổi trên một dòng đơn, tối đa là 19 ký tự.
- Khu vực 2: tên, ngày phát hành, ngày hết hạn và các thông tin liên quan đến chủ thẻ, được dập nổi trên 2 dòng với tối đa là 27 ký tự.

2.1.3. Thông tin lưu trên vạch từ của thẻ

Các thông tin lưu trên vạch từ và cấu trúc các trường thông tin của thẻ tuân theo chuẩn ISO 7811- 2, ISO 7811- 6 và ISO 7813.

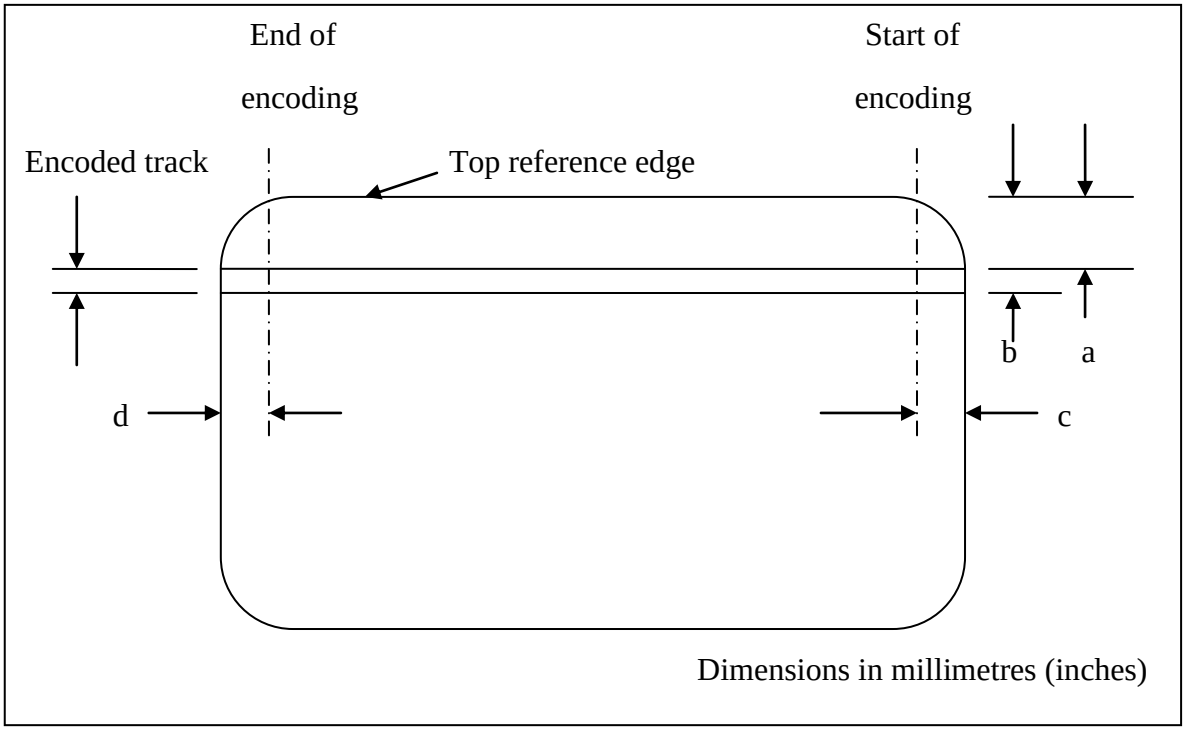
Đơn vị milimet (inches)



Hình 2.2 Vị trí dải từ (Mặt sau thẻ).

a = 11,89 (0.468): Khi sử dụng cho các tracks 1 và 2

a = 15,95 (0.628): Khi sử dụng cho các track 1, 2 và 3.



Hình 2.3 Vị trí của các rãnh trong dải từ.

Bảng 2.2: Bảng định nghĩa kích thước vị trí rãnh từ, đơn vị milimet (Inches)

Term	**Track 1**	**Track 2**	**Track 3**
a	5,79 (0.228) maximum	8,33 (0.328) minimum 9,09 (0.358) maximum	11,63 (0.458) minimum 12,65 (0.498) maximum
b	8,33 (0.328) minimum 9,09 (0.358) maximum	11,63 (0.458) minimum 12,65 (0.498) maximum	15,19 (0.598) minimum 15,82 (0.623) maximum
c	7,44 ± 1,00 (0.293 ± 0.039)	7,44 ± 0,50 (0.293 ± 0.020)	7,44 ± 1,00 (0.293 ± 0.039)
d	6,93 (0.252) minimum	6,93 (0.252) minimum	6,93 (0.252) minimum

Các chuẩn này quy định trên thẻ gồm có 3 tracks, nhưng thường chỉ sử dụng thông tin trên track 1 và 2.

- Track 1 là track tuân theo chuẩn IATA (International Air Bansport Associantion).Đây là track chỉ đọc, được ghi với mật độ cao và có thể chứa cả số lẫn ký tự chữ cái.

- Track 2 là track tuân theo chuẩn ABA (America Banker Association). Đây là Track chỉ đọc với mật độ ghi thấp và chỉ chứa ký tự số.
- Track 3 là track tuân theo chuẩn TTS (Thift Third) với mật độ ghi cao, chỉ chứa ký tự số nhưng có khả năng ghi đè (rewrite) lên thành phần dữ liệu đã có.

Thông tin về các tính chất, mật độ ghi … trên từng Track của thẻ có thể được tóm lược như sau:

Bảng 2.3: Bảng mô tả định nghĩa các Track

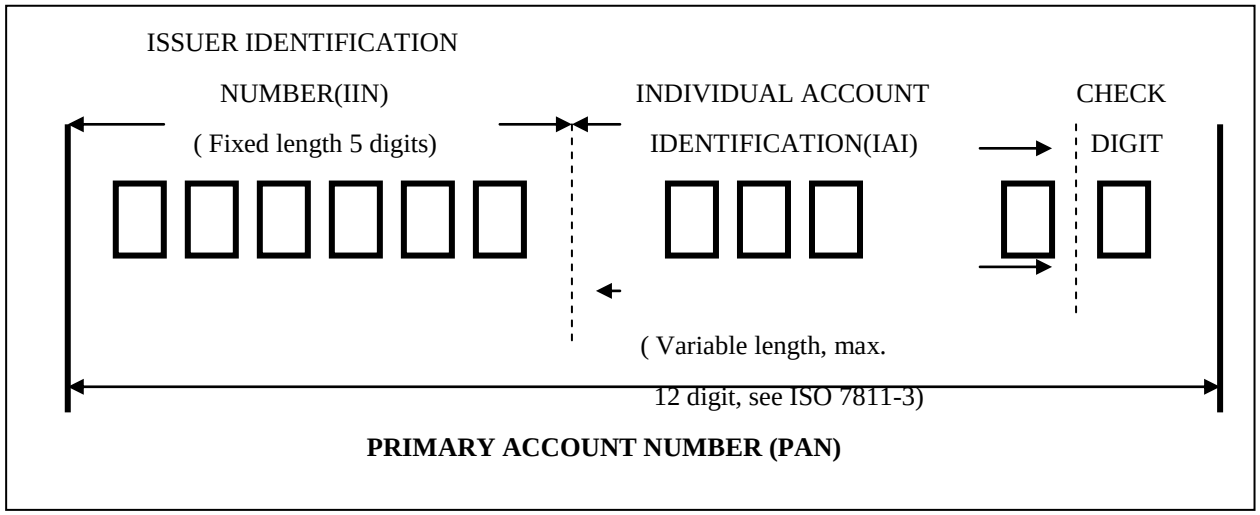
Track	**Tính chất**	**Mật độ ghi**	**Thể hiện**	**Độ dài**	**Định dạng mã**	**Số lượng ký tự**
Track1	Chỉ đọc	210 bits/inch	Chữ và số	Tối đa 79 ký tự	Mỗi ký tự được tạo bởi 7 bit (6 bit dữ liệu + 1 bit kiểm tra chăn lẻ)	2^6=64
Track2	Chỉ đọc	75 bits/inch	Số (0→9)	Tối đa 40 ký tự	Mỗi ký tự được tạo bởi 5 bit (4 bit dữ liệu + 1 bit kiểm tra chăn lẻ)	2^4=16
Track3	Đọc, ghi đè	210 bits/inch	Số (0→9)	Tối đa 107 ký tự	Mỗi ký tự được tạo bởi 5 bit (4 bit dữ liệu + 1 bit kiểm tra chăn lẻ)	2^4=16

2.1.4. Cấu trúc của số thẻ

Đối với mỗi thẻ khi được lưu hành đều có một dãy số xác định đó là số PAN – Primarry Accounr Number. Số PAN còn có thể được gọi với các tên khác như số thẻ hoặc số tài khoản chính.

2.1.4.1. Số PAN (Primary Account Number)

Số PAN là số định danh duy nhất đối với từng thẻ. Tuân theo chuẩn ISO 7812



Hình 2.4: Cấu trúc số PAN

Số PAN có thể lên tới 19 số, hiện tại hầu hết thẻ từ của các Ngân hàng Việt Nam đều có 16 chữ số. Số PAN gồm 3 thành phần như sau:

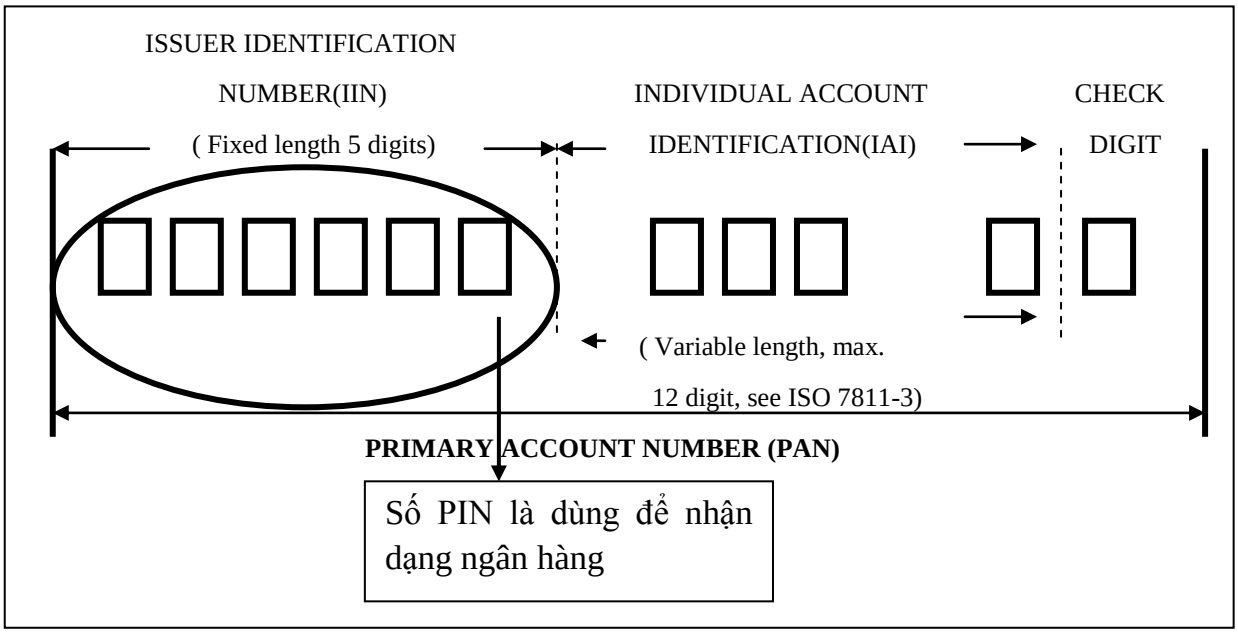
1/**.** IIN – Issuer Identification Number: số định danh đối với nhà phát hành thẻ, IIN cũng được gọi là số BIN – Bank Indentification Number.

2/. IAI – Individual Account Identification: Số nhận dạng tài khoản chủ thẻ. Các ngân hàng có thể quy định cấu trúc trong trường thông tin này.

3/. CD- Check Digit: Số với ý nghĩa mang tính chất kiểm tra số thẻ này có hợp lệ hay không. Số này được tạo ra từ việc sử dụng giải thuật Luhn.

2.1.4.2. Số IIN (số BIN)

IIN (Issuer Identification Number) là số nhận dạng đối với nhà phát hành thẻ hay BIN – Bank Indentification Number là số dùng để nhận dạng ngân hàng. Số BIN có độ dài là 6 chữ số, là một thành phần trong số PAN.



Hình 2.5 Vị trí số PIN

Minh họa cách đánh số BIN của mốt số ngân hàng của Việt Nam.

Tên các ngân hàng	Số BIN	Số thẻ - PAN
Ngân hàng Nông nghiệp và phát triển Nông thôn (VBARD)	**272728**	272728000000000-272728999999999
Ngân hàng Đầu tư và phát triển (BIDV)	**668899**	**668899**000000000-**668899**999999999
Ngân hàng Công thương (ICB)	**621060**	**621060**000000000-**621060**999999999

Hình 2.6: Vị trí các Số BIN

2.1.5. Định dạng thông điệp (message) của máy ATM

Định dạng thông điệp là cấu trúc thông điệp để ATM có thể trao đổi thông tin với Switch.

Thông điệp trong giao dịch tài chính được sử dụng trong máy ATM thường gồm các loại sau: 91x, NDx và ISOx. Do hiện nay có hai hãng chính về sản xuất máy ATM lớn trên thế giới là diebold và NCR nên chuẩn 91x, NDx là hai loại định dạng chính được sử dụng.

- Thông điệp chuẩn của hãng Diebold:

+ 911

+ 912+

- Thông điệp chuẩn của hãng NCR:

+ NDC

+ NDC+

Cấu trúc chung của thông điệp như sau:

STX	**Header**	**Body**	**ETX**

***Trong đó*:** STX – Start of text : Trường khởi đầu của thông điệp.

Header : Phần đầu của thông điệp.

Body : phần thân của thông điệp.

ETX – End of text : Trường kết thúc của thông điệp.

2.1.5.1. Thông điệp từ ATM đến Switch

Giới thiệu mốt số định dạng thông điệp từ ATM đến Switch.

(1) Xác thực PIN – PIN Verification (PNV)

(2) Rút tiền – Cash Withdrawal (CWD)

(3) Đổi PIN – PIN Change (PIN)

(4) Vấn tin và in sao kê – Balance Inquiry and Mini Sratement (INQ)

(5) Chuyển khoản – Funds Transfer (TFR)

(6) Yêu cầu đổi khóa – Request Transmission Key (RQK)

1/. Đầu mục thông điệp Massage header

Đầu mục nay sẽ xuất hiện trong tất cả các thông điệp được gửi từ ATM đến Switch.

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX-Start Of text		1	02	Hex
2	Transaction Code	Mã giao dịch	3	xxx	
3	Type 1 Note Status	Trạng thái 1	1	0 - 2	Note 1
4	Type 2 Note Status	Trạng thái 2	1	0 - 2	Note 1
5	Type 3 Note Status	Trạng thái 3	1	0 - 2	Note 1
6	Type 4 Note Status	Trạng thái 4	1	0 - 2	Note 1
7	Journal status	Trạng thái nhật ký	1	0 - 2	Note 1
8	Receipt Status	Trạng thái in hóa đơn	1	0 - 2	Note 1
9	Dispenser Status	Trạng thái thiết bị trả tiền	1	0 - 2	Note 2
10	Encryptor status	Trạng thái thiết bị mã hóa	1	0 - 2	Note 2
11	Card reader status	Trạng thái đầu đọc thẻ	1	0 - 2	Note 2
12	Transaction Sequence No	Số tuần tự giao dịch	6	[999999]	Kiểu số
13	ATM Status	Trạng thái ATM	1	O-Open C-Close	
14	ATM Identification	Số nhận dạng ATM	8	[999999999]	Kiểu số
Tổng độ dài			24		Byte

Chú ý:

1. Các trạng thái được định nghĩa

0 – good

1 – low

2 – out

2. Các trạng thái được định nghĩa

0- Normal

1- Missing

2- Inoperative

2./ Thông điệp xác thực PIN (PNV)

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1 - 14	Message Header		24		Mã xử lý:'PNV'
15	Track 2	Track 2 của thẻ từ	104		
16	Encrypted PIN Block	PIN block đã mã hóa	16		
17	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		145		Byte

3./ Thông điệp rút tiền CWD

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1 - 14	Message Header		24		Mã xử lý:'CWD'
15	Track 2	Track 2 của thẻ từ	104		
16	Transaction A/C No.	Số tài khoản giao dịch	16		
17	Transaction Amount	Khối lượng giao dịch	8	[99999999]	Kiểu số
18	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		153		Byte

4./ Thông điệp Đổi PIN

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1 - 14	Message Header		24		Mã xử lý:'PIN'
15	Track 2	Track 2 của thẻ từ	104		
16	Old PIN Block (Encrypted)	PIN cũ (đã được mã hóa)	16		
17	New PIN Block (Encrypted)	PIN mới (đã được mã hóa)	8	[99999999]	
18	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		163		Byte

5./ Thông điệp vấn tin - INQ

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1 - 14	Message Header		24		Mã xử lý:'INQ'
15	Track 2	Track 2 của thẻ từ	104		
16	Transaction A/C No.	Số tài khoản giao dịch	16		
17	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		145		Byte

6./ Thông điệp Chuyển khoản –TFR

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1 - 14	Message Header		24		Mã xử lý:'INQ'
15	Track 2	Track 2 của thẻ từ	104		
16	Source Transaction A/C No.	Số tài khoản nguồn	16		
17	Distination Transaction A/C No	Số tài khoản đích	16	[99999999]	
18	Transaction Amount	Khối lượng giao dịch	8	03	Số Hex
17	ETX	Kí hiệu kết thúc	1	03	Số Hex
Tổng độ dài			169		Byte

7/. Thông điệp yêu cầu truyền khóa (RQK)

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1 - 14	Message Header		24		Mã xử lý:'RQK'
15	ATM status	Trạng thái ATM	1	C-Cold Strt S-Supervisor	
16	ETX	Kí hiệu kết thúc	1	03	Số Hex
Tổng độ dài			26		Byte

2.1.5.2 Thông điệp từ Switch đến ATM

Giới thiệu một số định dạng thông điệp từ Switch đến ATM.

(1) Phản hồi chấp nhận xác thực PIN – Accepted Response to PIN Verification (PNV)

(2) Phản hồi từ chối xác thực PIN – Rejected Response to PIN Verification (PNV)

(3) Phản hồi chấp nhận rút tiền – Accepted Response to Cash Withdrawal (CWD)

(4) Phản hồi từ chối rút tiền – Rejected Response to Cash Withdrawal (CWD)

(5) Accepted Response to PIN Change (PIN)

(6) Accepted Response to Balance Inquiry & Mini Statement (INQ)

(7) Accepted Response to Funds Transfer (TFR)

1/. Phản hồi chấp nhận xác thực PIN

Trường	**Miêu tả**		**Độ dài**	**Giá trị**	**Ghi chú**
1	STX	Kí hiệu bắt đầu	1	02	Số Hex
2	TPC		1	66	Số Hex
3	Operating Mode		1		P- Production T- Testing
4	Transaction Date		12		YYYYMMDD HHMM
5	Status		2		00-Good 01- Bad 02- Retained 03- Rorce change PIN
6	A/C Ditails		100		
7	Transaction sequence No		6	[999999]	Kiểu số
8	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		124		Byte

2./ Phản hồi không chấp nhận xác thực PIN

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Kí hiệu bắt đầu	1	02	Số Hex
2	TPC		1	47 hoặc 54	Số Hex
3	Operating Mode		1		P- Production T- Testing
4	Transaction Date		12		YYYYMMDD HHMM
5	Reject Code		4		
6	Transaction sequence No		6	[000000-999999]	
7	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài	26			Byte

3/. Phản hồi chấp nhận giao dịch rút tiền

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Kí hiệu bắt đầu	1	02	Số Hex
2	TPC		1	66	Số Hex
3	Operating	Chế độ hoạt động	1		P- Production T- Testing
4	Transaction Date	Ngày giao dịch	12		YYYYMMDD HHMM
5	Transaction A/C No	Số tài khoản	16		
6	Accepted		1		1-Online
7	Fund Available	Giá trị hiện có	15		
8	Transaction Amount	Khối lượng giao dịch	8		
9	Transaction sequence No	Số thứ tự giao dịch	6	[000000-999999]	
10	ETX	Kí hiệu kết thúc	1	03	Số Hex
	Tổng độ dài		62		Byte

4./ Trả lời từ chối giao dịch rút tiền

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Kí hiệu bắt đầu	1	02	Số Hex
2	TPC		1	54	Số Hex
3	Operating Mode	Chế độ hoạt động	1		P- Production T- Testing
4	Transaction Date	Ngày giao dịch	12		YYYYMMDD HHMM
5	Reject Code		4		
6	Transaction sequence No		6	[999999]	
7	ETX	Kí hiệu kết thúc	1	03	Số Hex
Tổng độ dài			24		Byte

5./ Trả lời từ chối giao dịch rút tiền do không đủ tiền

Trường	Miêu tả		Độ dài	Giá trị	Ghi chú
1	STX	Kí hiệu bắt đầu	1	02	Số Hex
2	TPC		1	55	Số Hex
3	Operating Mode	Chế độ hoạt động	1		P- Production T- Testing
4	Transaction Date	Ngày giao dịch	12		YYYYMMDD HHMM
5	Reject Code		4		
6	Fund Available		15		
7	Transaction sequence No	Số thứ tự giao dịch	6	[999999]	
8	ETX	Kí hiệu kết thúc	1	03	Số Hex
Tổng độ dài			24		Byte

2.2. HỆ THỐNG THANH TOÁN BẰNG MÁY ATM CHO THẺ CHÍP

2.2.1. Thẻ chíp

Thẻ chíp hay còn được gọi là thẻ thông minh – SmartCard. Là loại thẻ nhựa cứng, thông tin về thẻ được lưu trên chíp nhớ. Thẻ có thể thực hiện được các giao dịch tự động như kiểm tra số dư, rút tiền chuyển khoản v.v từ máy rút tiền tự động ATM.

2.2.2. Sự phát triển của thẻ chíp

Giữa những năm 80, Châu Âu đã triển khai những chiếc thẻ thông minh đầu tiên, giờ đây phạm vi sử dụng của thẻ thông minh đã được mở rộng ra trên toàn thế giới.

Thẻ thông minh cung cấp rất nhiều tính năng vượt trội so với thẻ từ truyền thống như khả năng lưu trữ lớn, khả năng bảo mật an toàn thông tin, hỗ trợ nhiều ứng dụng.

Hiện nay, các tổ chức thẻ quốc tế như Europay, MasteCard, Visa – EMV đang thúc đẩy việc chuyển đổi từ thẻ từ sang thẻ SmartCard trên phạm vi toàn cầu. Theo EMV từ ngày 1/1/2006, khi tham gia vào hệ thống của các tổ chức này các ngân hàng sẽ phải chuyển đổi sang sử dụng thẻ thông minh đạt chuẩn EMV. Nếu không các ngân hàng sẽ phải chịu toàn bộ rủi ro do gian lận thẻ gây ra.

Vai trò của thẻ từ chỉ đến 1 ngưỡng nhất định. Khi hệ thống an toàn không còn đảm bảo nữa việc chuyển sang thẻ thông minh là việc làm tất yếu, hợp xu thế.

Chuyển đổi sang thẻ chip nhằm bảo vệ chính ngân hàng, bảo vệ khách hàng và tạo nên ưu thế cạnh tranh cho ngân hàng.

Thay đổi từ thẻ sang thẻ thông minh không thể diễn ra trong chốc nát. Quá trình chuyển dịch đòi hỏi các ngân hàng phải thực hiện những thay đổi mang tính toàn hệ thống vì công nghệ phát hành và thanh toán thẻ thông minh có sự khác biệt lớn so với công nghệ thẻ từ truyện thống.

Sự đầu tư là lớn, vì vậy lý giải tại sao tại các nước các ngân hàng chưa thể chuyển từ sử dụng thẻ từ sang thẻ thông minh một cách nhanh chóng được.

Thẻ chíp ra đời dựa trên hai nhân tố chính, các thuật toán mã hóa mạnh: mã hóa khóa công khai RSA, mã hóa khóa đối xứng 3DES, hàm băm SHA-1.

Chip trên thẻ có thể thực hiện các tinh toán mã hóa trên dữ liệu. Thuật toán mã hóa PIN và thuật toán dành cho chữ ký số là RSA, hàm băm là SHA -1, MACing và việc mã hóa các thông điệp theo từng phiên thì sử dụng 3DES.

Thẻ chip có thể được cập nhật hay lập trình lại một cách an toàn khi đang sử dụng. Ngân hàng phát hành thẻ có thể cập nhật tham số quan lý rủi ro chứa trong một ứng dụng ngân hàng từ xa trong một giao dịch trực tuyến tại terminal.

Một số loại thẻ đa ứng dụng hỗ trợ việc tải xuống các ứng dụng mới và xóa đi các ứng dụng cũ từ xa tại terminals chuyên dụng hay qua Internet.

Các thông tin lưu trong thẻ chip gồm:

+ Dữ liệu công khai: thông tin về CA, chứng chỉ khóa công khai của nhà phát hành thẻ, chứng chỉ thẻ công khai của thẻ, chứng chỉ thẻ công khai để mã hóa PIN…

+ Dữ liệu bí mật: khóa riêng của thẻ, khóa riêng mã hóa PIN, khóa chủ (Master Key), PIN.

Chương 3. CƠ CHẾ AN TOÀN THÔNG TIN TRONG HỆ THỐNG ATM

3.1. MÃ HÓA TRONG HỆ THỐNG ATM

ATM là một phần trong hệ thống mạng không tập trung nằm phân bố ở các địa điểm khác nhau, do đó việc bảo đảm an toàn thông tin được đặt nên rất cao. Không những đảm bảo an toan trên từng máy ATM mà còn bảo đảm an toàn trong toàn bộ hệ thống mạng.

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 Switch, hệ thống sử dụng thiết bị mã hóa cứng để mã hóa và giải mã thông tin. Máy ATM có thiết bị EPP (Encrypting PIN Pad), hệ thống Switch có thiết bị HSM (hardware Security Module).

3.1.1. Thuật toán mã hóa

Trong hệ thống ATM hiện nay thường dùng thuật toán DES và 3DES để mã hóa và giải mã dữ liệu.

Khóa được sử dụng trong thuật toán có độ dài 64 bit, 128 bit hoặc 192bit tùy theo cách sử dụng mã khóa hoặc chọn mã hóa DES hay 3DES.

3.1.1.1. Thuật toán mã hóa 3DES – Triple DES

Thuật toán 3DES chính là DES, gọi là 3DES bởi vì người ta dùng liên tiếp 3 lần DES với ba mã khóa K1, K2, K3. Khóa K được xây dựng từ bộ ba khóa 64bit (K1, K2, K3) có độ dài 3*64=192bit.

1) Khi mã hóa sử dụng K1 mã hóa, K2 giải mã, K3 mã hóa.
2) Khi giải mã sử dụng K3 giải mã, K2 mã hóa, K1 giải mã

3.1.1.2. Xây dựng khóa K1, K2, K3

1) Key single length (Bộ một khóa 64bit)
   K1=K2=K3, độ dài khóa 64bit
2) Key double length (Bộ hai khóa 64bit)
   K1#K2 và K3=K1, độ dài khóa 128 bit

3) Key triple length (Bộ ba khóa 64bit)

K1#K2#K3#K1, độ dài khóa 192bit

Trường hợp này không gian khóa 3*56=168bit là 2^{168}

3.1.1.3 Ví dụ

Xây dựng khóa Key Triple length

K=0123456789ABCDEFFEDCBA987654321089ABCDEF01234567

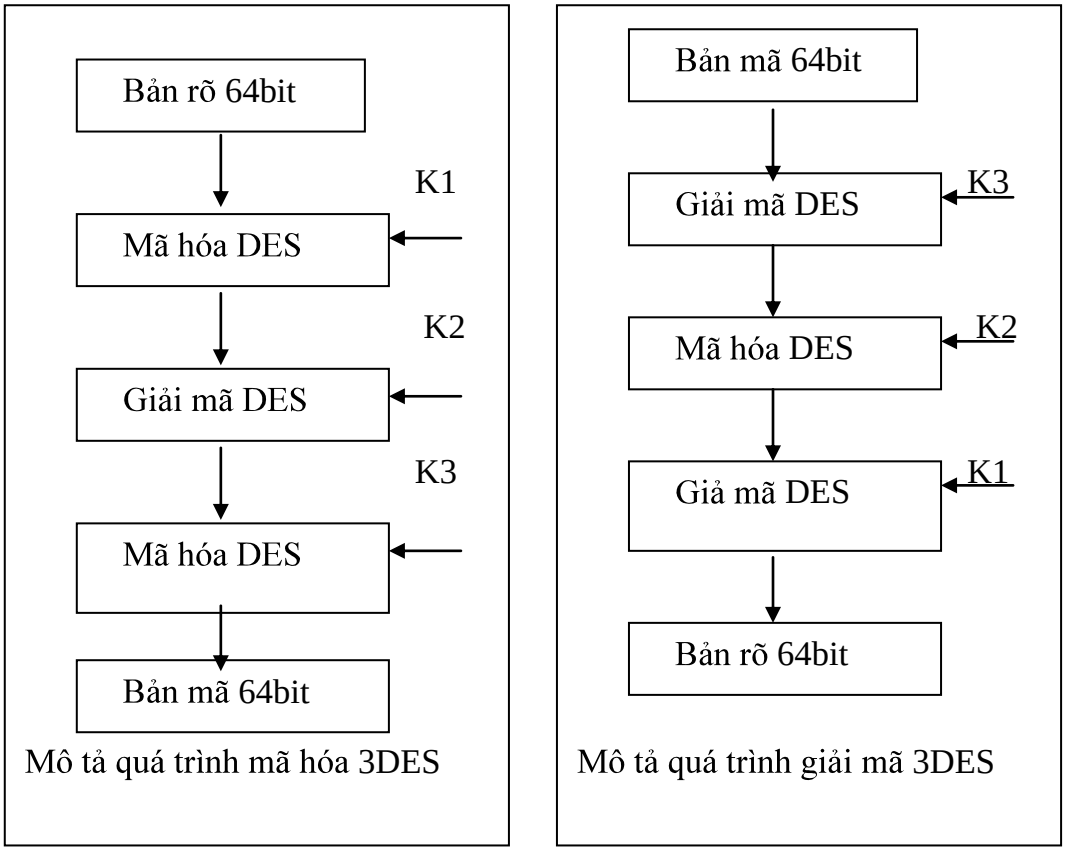
Khi đó các khóa con K1, K2, K3 được tách như sau:

0123456789ABCDEF|FEDCBA9876543210|89ABCDEF01234567

|<----------K1------->|<----------K2------->|<----------K3---------->|

3.1.1.4. Quá trình mã hóa và giải mã

Quá trình mã hóa và giải mã của DES được thực hiện như hình vẽ.



Hình 3.1 Các bước thực hiện trong quá trình mã hóa và giải mã theo 3DES.

1/. Mô tả quá trình mã hóa theo 3DES

Bản rõ 64bit được mã hóa theo DES với khóa K1 ta được bản mã 64bit.

Bản mã 64bit được giải mã theo DES với khóa K2 ta được bản "rõ" 64bit.

Bản "rõ" 64bit được mã hóa theo DES với khóa K3 ta được bản mã 64bit.

Kết quả là bản rõ được mã hóa theo 3DES.

2/. Quá trình giải mã theo 3DES

Bản mã 64bit được giải mã theo DES với khóa K3 ta được bản "rõ".

Bản "rõ" được mã hóa theo DES với khóa K2 ta được bản mã.

Bản mã được giải mã theo DES với khóa K3 ta được bản rõ.

Kết quả là bản mã đã được giải mã theo 3DES.

3.1.2. Khóa bí mật trong hệ thống ATM

Khóa được sử dụng trong hệ thống ATM gồm có CVK, PVK, WK, LMK, TMK và được đảm bảo một số tính chất sau:

- Với các khóa được lưu trữ trong EPP và HSM, khi bị xâm nhập một cách bất hợp pháp, khóa bí mật sẽ tự bị hủy.
- Khóa có độ dài 64bit, 128bit, hoặc 192bit tùy theo cách sử dụng của khóa hoặc chọn mã hóa DES hay 3DES.

Tất cả các khóa trên đều được tạo ra trong thiết bị HSM và khóa LMK phải được tạo trước tiên còn các khóa CVK, PVK, WK, TMK tạo ra sau.

Khóa chia làm hai loại khi lưu: Lưu dưới dạng bản rõ, lưu dưới dạng bản mã:

- Khóa LMK và TMK được lưu dưới dạng bản rõ trong HSM và EPP.
- Khóa CVK, PVK, WK, TMK được lưu dưới dạng bản mã trong CSDL của Switch và của máy ATM.

3.1.2.1. Định nghĩa các khóa trong hệ thống ATM

1/. Khoá LMK-Local Master Keys

LMK được tạo trước tiên trong HSM sau đó được lưu trong HSM và một bản sao được lưu trong Smartcard. Nếu HSM bị mở ra vì bất cứ lý do gì hay xâm nhập trái phép, thì LMK sẽ bị xóa và phải được nhập lại vào HSM.

Để sinh khóa LMK và tải vào HSM thì phải có ít nhất 3 thành phần khác nhau dưới dạng bản rõ (3 clear LMK component khác nhau, trong HSM ta có thể cấu

hình khóa LMK được sinh ra từ 3 đến 9 thành phần clear LMK component). Để đảm bảo an toàn thì mỗi thành phần khóa bản rõ sẽ do mỗi người giữ.

Để tạo ra LMK thì người ta sử dụng phép XOR từ các clear LMK component

Khóa LMK có các thông tin sau:

Khóa được lưu trong HSM dưới dạng bản rõ (Từ các clear LMK component)

Khóa được dùng để mã hóa và giải mã các khóa CVK, PVK, WK và TMK.

Khóa này chỉ được thay đổi khi có yêu cầu.

Khóa có độ dài 64bit, 128bit và 192bit.

2/. Khóa CVK- card Verification Keys

Khóa CVK được sinh ngẫu nhiên trong HSM và được mã hóa bởi khóa LMK.

Khóa dùng để sinh số CVV/CVC, để đảm bảo thẻ không bị làm giả, khi phát hành người ta dựa trên thông tin về thẻ để sinh số CVV/CVC, được lưu trên thẻ.

Bản mã của khóa CVK sẽ được lưu vào hệ thống Switch. Không lưu bản rõ khóa có độ dài 64bit, 128bit hoặc 192bit

3/. Khóa PVK-PIN Verification Keys

Khóa PVK được sinh ngẫu nhiên trong HSM và được mã hóa bởi khóa LMK.

Khóa được dùng để mã hóa và giải mã số PIN của chủ thẻ, số PIN này được mã hóa và lưu trong CSDL của CoreBank

Bản mã của khóa PVK sẽ được lưu vào hệ thống Switch. Không lưu bản rõ nếu thay đổi khóa này, thì phải thay đổi toàn bộ số PIN cho chủ thẻ.

Khóa có độ dài 64bit, 128bit hoặc 192bit.

4/. Khóa WK-Working Keys(hay PIN Encryption Key)

Khóa WK được sinh ngẫu nhiên trong HSM và được lưu dưới hai bản mã tại Switch và ATM.

- Bản mã thứ nhất được mã bởi khóa LMK và lưu trong CSDL của Switch.
- Bản mã thứ hai được mã bởi khóa TMK và lưu trong CSDL của ATM.

Sự đồng bộ khóa giữa ATM và Switch thông qua quá trình trao đổi khóa.

Khóa được dùng để mã hóa và giải mã số PIN trong quá trình trao đổi thông điệp giữa ATM và Switch.

Khóa được thay đổi thường xuyên tùy theo yêu cầu của NH, để đảm bảo an toàn thông tin giao dịch, sai mỗi lần giao dịch, khóa này sẽ được thay đổi.

Khóa có độ dài 64bit, 128bit hoặc 192bit.

5/. Khóa TMK- Terminal master keys

Khóa TMK được sinh ngẫu nhiên trong HSM và được mã hóa bởi khóa LMK.

Khóa được sử dụng để giải mã khóa WK.

Khóa được lưu lại hai nơi là EPP và Switch:

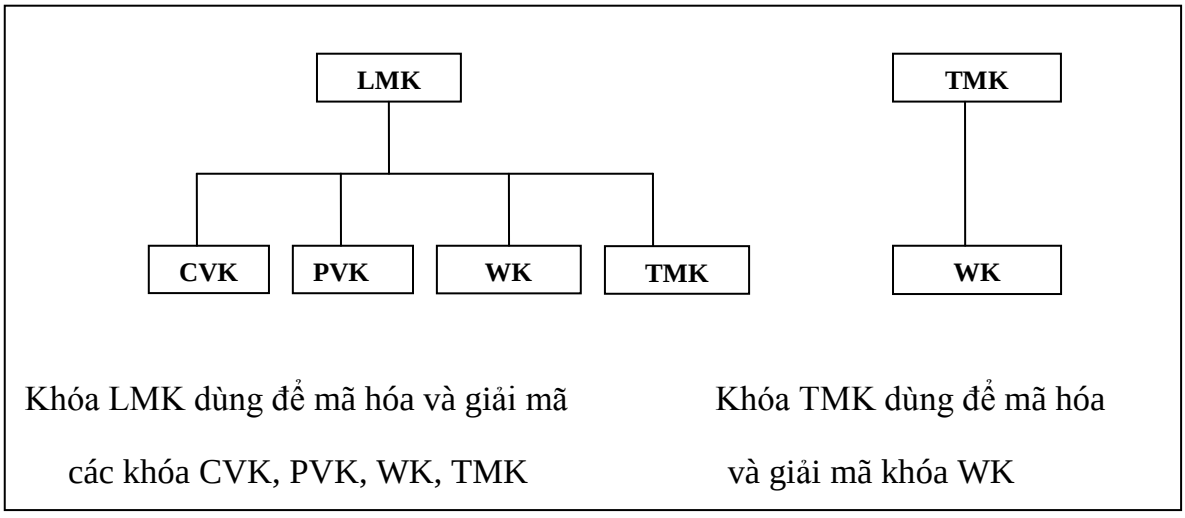
- Tại EPP khóa được lưu dưới dạng bản rõ.
- Tại Switch khóa được lưu trong CSDL dưới dạng bản mã, mã hóa bởi LMK.

Khóa chỉ thay đổi khi có yêu cầu, khi thay đổi thì nhân viên kỹ thuật sẽ thực hiên.

Khóa có độ dài 64bit, 128bit hoặc 192bit.

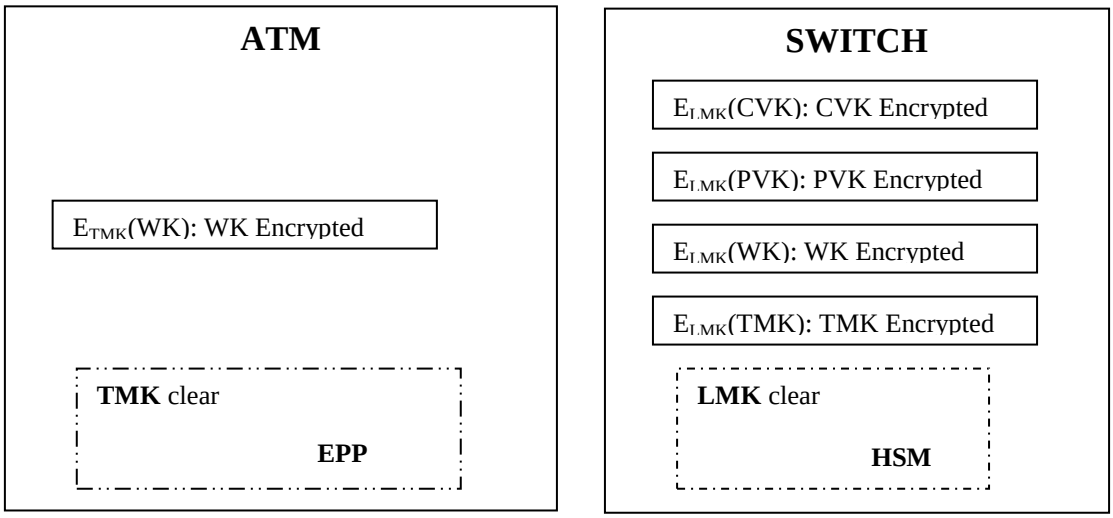
3.1.2.2. Sơ đồ phân cấp khóa trong hệ thống ATM

Các khóa trên đươc phân cấp như sau:



Hình 3.2 Phân lớp các khóa sử dụng trong hệ thống ATM

Mô tả vị trí các khóa trong hệ thống ATM:



Hình 3.3 Mô tả các vị trí kóa trong hệ thống ATM

* Tại ATM

+ TMK được lưu dưới dạng bản rõ trong thiết bị EPP.

+ WK được mã hóa bởi TMK và lưu trong CSDL của máy ATM.

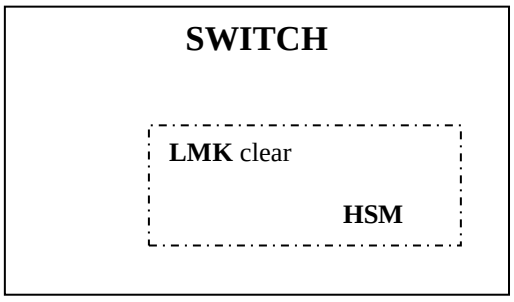
* Tại SWITCH

+ LMK được lưu dưới dạng bản rõ trong thiết bị HSM.

+ CVK, PVK, WK, TMK được mã hóa bởi LMK và lưu trong CSDL của Switch.

3.1.2.3. Trao đổi khóa giữa ATM và Switch

1/. Thiết lập khóa LMK cho HSM

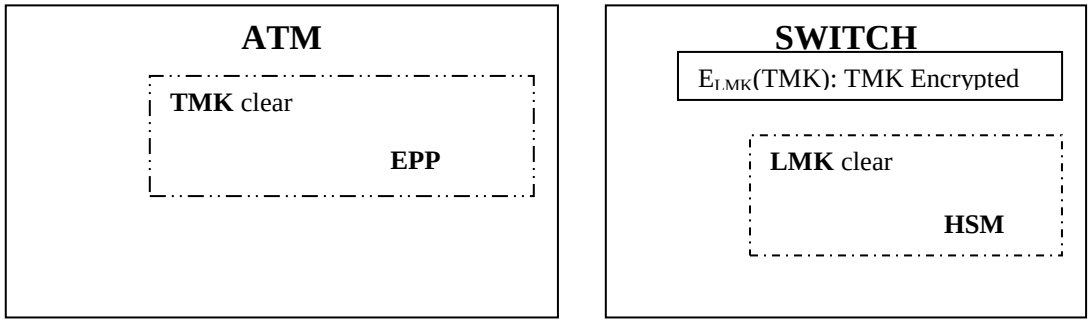


Hình3.4 Thiết lập khóa LMK trong HSM

(a) Tạo khóa LMK ngay trong HSM

(b) Lưu LMK dưới dạng bản "rõ" trong HSM và một bản dự phòng được lưu trong Smartcard (Smartcard cũng được bảo mật).

2/. Thiết lập khóa TMK cho EPP



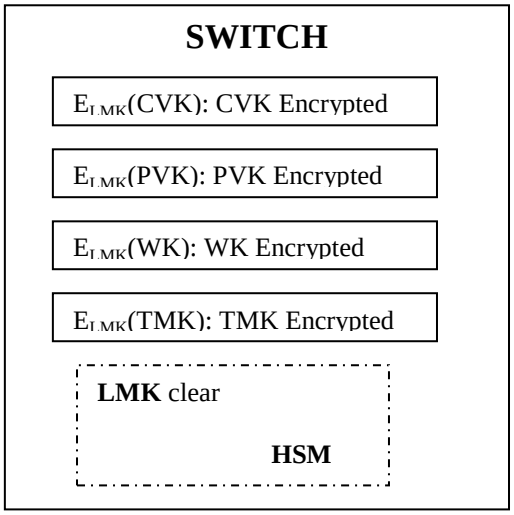
Hình3.5 Thiết lập khóa TMK cho EPP.

(a) Khóa TMK được tạo trong HSM.

(b) Một bản rõ được lưu lại EPP

(c) Một bản mã lưu lại Switch (được mã hóa bởi khóa LMK)

3/. Thiết lập các khóa khác tại Switch



Hình 3.6 Thiết lập khóa khác tại Switch.

(a) Các khóa trên đều được sinh trong HSM và được mã hóa bởi khóa LMK

(b) Bản mã của các khóa trên được lưu trong CSDL của Switch không lưu bản rõ

3.1.3. Thiết bị mã hóa trong hệ thống ATM

Hệ thống ATM sử dụng hai thiết bị mã hóa cứng là EPP và HSM. EPP dùng trên máy ATM, còn HSM dùng trên hệ thống Switch.

Thiết bị này là một "hộp đen", toàn bộ quá trình được thực hiện bên trong ta chỉ cần quan tâm đến giá trị đầu vào và kết quả đầu ra.

EPP dùng để mã hóa số PIN.

HSM dùng để sinh và mã hóa các khóa bí mật, dùng giải mã và so sánh số PIN.

Các thiết bị này đều lưu trữ các khóa bí mật và đảm bảo các tính chất sau:

- Không truy cập hoặc xác định được bản rõ của bất kỳ khóa bí mật nào được lưu trữ trong thiết bị EPP, HSM một cách bất hợp pháp.
- Khi xâm nhập một cách bất hợp pháp, khóa bí mật sẽ tự bị hủy.
- Với các thiết bị mã hóa này sẽ hạn chế được những sơ hở ở phía hai đầu (tiền mã hóa và hẩ mã dịch), đây là những sơ hở mà hackers chuyên nghiệp có thể mọi thông tin ngay từ đó mà không cần "thám mã".

3.1.3.1. Thiết bị EPP (Encrypt PIN Pad)

Bàn phím để nhập PIN của máy ATM chính là thiết bị mã hóa EPP. Đây là thiết bị chuyên dụng , dùng mã hóa trực tiếp số PIN khi được nhập vào.

Số PIN được mã hóa ngay khi chủ thẻ nhập đủ độ dài số PIN hoặc gõ enter để kết thúc nhập PIN. Không lưu bất kỳ bản nào của số PIN chỉ lưu bản mã.

3.1.3.2. Thiết bị HSM (Hardware Security Module)

HSM thiết bị mã hóa cứng dùng để mã hóa và giải mã, đây là một phần của hệ thống phần mềm Switch.

Toàn bộ quá trình mã hóa và giải mã ở hệ thống Switch đều được thực hiện tại HSM.

3.2. MÃ HÓA VÀ GIẢI MÃ SỐ PIN

3.2.1. Khái niệm số PIN (Personal Identification Number)

Số PIN – số nhận dạng cá nhân hay còn gọi là mã số bí mật của chủ thẻ. Số PIN được dùng để xác định định danh tài khoản của chủ thẻ.

Độ dài tối thiểu của số PIN là 4 chữ số và tối đa là 12 chữ số , hiện nay các ngân hàng ở Việt Nam số PIN có độ dài không quá 6 chữ số.

Hệ thống sử dụng thiết bị phần cứng để mã hóa và giải số PIN. Đây cũng là một trong những giải pháp nhằm nâng đảm bảo an toàn tuyệt đối khi sử dụng kỹ thuật mã hóa (không sử dụng mã hóa bằng phần mềm).

Các thiết bị được sử dụng bao gồm EPP dùng trong máy ATM và HSM dùng trong hệ thống Switch. Bản rõ của PIN không bao giờ xuất hiện ngoài EPP hay HSM.

3.2.2. Mã hóa PIN và ATM

Để đảm bảo độ an toàn của số PIN trong quá trình truyền trên mạng, số PIN sẽ được chuyển thành khối PIN (PIN Block) và khối PIN này sẽ được mã hóa trước khi chuyển từ ATM tới hệ thống Switch.

Khối PIN được mã hóa bằng khóa được cấu hình (thỏa thuận) trước giữa ATM và hệ thống Switch.

Thuật toán DES (3DES) chỉ làm việc với khối dữ liệu đầu vào có độ dài là 64 bit, nên PIN Block được xây dựng bằng cách module-2 (XOR) hai trường 64 bit theo chuẩn ISO 9564-1 gồm:

+ Trường số PIN theo khuôn dạng 64 bit.

+ Trường số PAN theo khuôn dang 64 bit.

Điều kiện đầu vào và kết quả đầu ra của quá trình mã hóa số PIN:

Đầu vào : + Số thẻ - PAN

+ Số PIN.

Đầu ra: Khối PIN Block được mã hóa bằng thuật toán DES (3DES) có độ dài 64 bit.

Quá trình xác thực PIN sẽ được làm ở HSM (không làm trong phần mềm Switch), giá trị trả về của HSM sẽ cho biết số PIN nhập là đúng hay sai.

3.2.2.1. Khuôn dạng PIN Block

Khuôn dạng trường số PIN được định nghĩa như sau:

Vị trí bit	1-4	5-8	9-12	13-16	17-20	21-24	25-28	29-32	33-36	37-40	41-44	45-48	49-52	53-56	57-60	61-64
Giá trị	C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

Trong đó:

Kí hiệu	Miêu tả	Giá trị
C	Trương điều khiển	0000
N	Chiều dài PIN (4 -12)	4 bit với giá trị từ 0100 (4) đến 1100 (12)
P	Chữ số trong số BIN	4 bit với giá trị từ 0000 (0)đến 1001 (9)
P/F	Số PIN/Số lấy đầy	Trường này được xác định bởi giá trị N
F	Số mặc định (Hex)15	Trường 4 bit 1111 (15)

Khuôn dạng trường số PAN được định nghĩa như sau:

Vị trí bit	1-4	5-8	9-12	13-16	17-20	21-24	25-28	29-32	33-36	37-40	41-44	45-48	49-52	53-56	57-60	61-64
Giá trị	0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12

<u>Trong đó:</u>

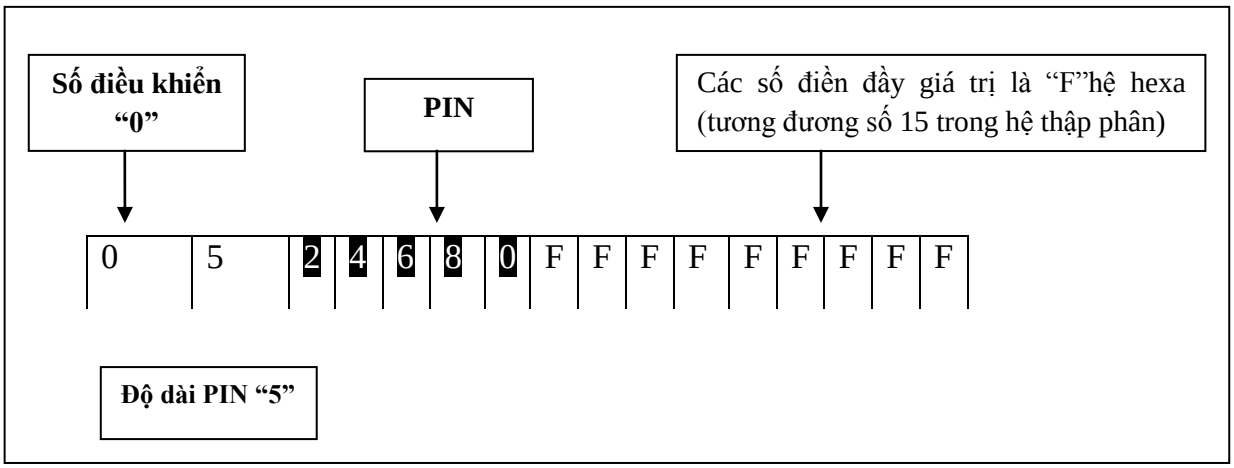
0 = Pad digit	Trường 4 bit có giá trị là 0 (thể hiện dạng nhị phân 0000)
A1.... A12 =account number A1 đến A12 thuộc [0,..,9]	12 số bên phải của số PAN ngoại trừ CD (bỏ số cuối cùng bên phải). A12 là số đứng trước số CD. Nếu số PAN không tính CD mà nhỏ hơn 12 số thì được sắp dần vào từ bên phải và được điền ở bên trái bằng các số Pad digit

- Ví dụ cho số PIN và số PAN của một thẻ ATM như sau:

Số PIN = 24680 có độ dài là 5 chữ sô.

Số PAN = 6688997312456719831 có độ dài là 19 chữ số.

+ Khuôn dạng trường số PIN:



+ Khuôn dạng trường số PAN:

+ Khối PIN Block được tính như sau:

PIN	0	5	2	4	6	8	0	F	F	F	F	F	F	F	F	F	
PAN	0	0	0	0	7	3	1	2	4	5	6	7	1	9	8	3	
	0	5	2	4	1	B	1	D	B	A	9	8	E	6	7	C	XOR

Hình 3.7 Minh họa cách tính khối PIN Block.

+ Khối PIN Block là: 05241B1DBA98E67C

3.2.2.2. Mã hóa khối PIN Block

Khối này được mã hóa bởi 3DES trước khi truyền đi, ví dụ với một khóa bộ hai (128 bit) sẽ được dùng để mã hóa như sau:

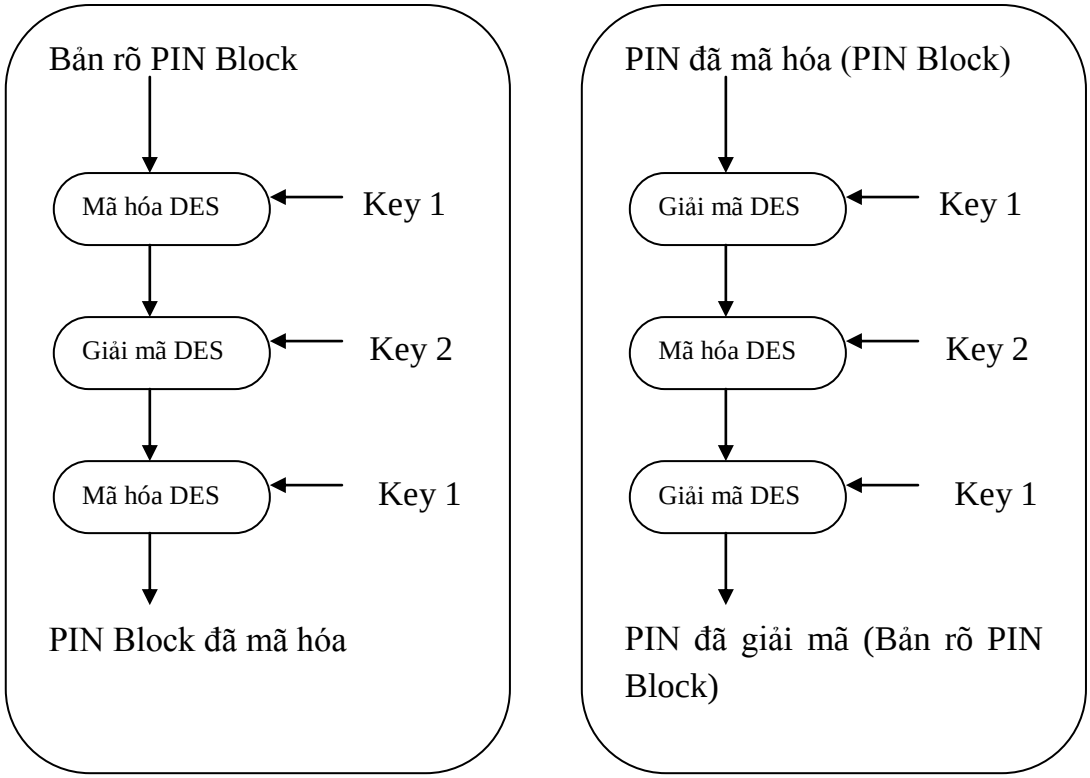
AAEEAA75BDFDB57F 66AAEEAA66AAEEAA

Với 64bit bên trái (key 1) và 64 bit bên phải (key 2) ta có 2 nhau sau:

AAEEAA75BDFDB57F **66AAEEAA66AAEEAA**

Key 1 **Key 2**

Sơ đồ dưới đây mô tả việc dùng khóa 3DES bộ hai để mã hóa và giải mã PIN block:



Hình 3.8 Các bước mã hóa và giải mã PIN Block

3.2.3. Xác thực PIN tai HSM

Tại HSM để xác thực PIN gồm các quá trình sau:

- Giải mã PIN được nhập vào từ máy ATM đã được mã hóa.
- Giải mã PIN lưu trong CSDL của Corebanhk đã được mã hóa.
- So sánh số PIN được nhập vào và số PIN được lưu trong CSDL.
- Quá trình xác thực đều thực hiện trong thiết bị HSM.

Kết quả đầu ra sẽ là số PIN nhập vào đúng hay sai.

Các bước thực hiện xác thực PIN:

(1) Người dùng cho thẻ vào ATM và nhập số PIN.

(2) Thiết bị EPP sẽ tạo ra PIN block.

(3) Giải mã khóa WK bởi khóa LMK.

(4) Mã hóa PIN block theo khóa WK, khối PIN này được gắn vào thông điệp và gửi cho Switch.

(5) Bản mã WK tại Switch được giải mã bởi khóa LMK trong HSM.

(6) Khối PIN block được giải mã bởi WK.

(7) Bản của PVK tại Switch được giải bởi khóa LMK trong HSM.

(8) Khối PIN được lưu trong CSDL của khách hàng được giải mã bởi khóa PVK, sau đó được so sánh với khối PIN block rong Module PIN Verification.

(9) Kết quả so sánh sẽ được gửi lại cho ATM.

3.3. CƠ CHẾ AN TOÀN THÔNG TIN TRONG HỆ THỐNG ATM.

1/. Bảo đảm an toàn thông tin trong hệ thống có thể chia ra làm 3 lĩnh vực sau:

a/. Đảm bảo an toàn phía Ngân hàng.

b/. Đảm bảo an toàn phía người dùng.

c/. Đảm bảo an toàn cơ sở hạ tầng hệ thống: phần cứng, phần mềm, mạng truyền thông.

2/. Các giải pháp nhằm đảm bảo an toàn thông tin trong hệ thống:

a/. Kiểm tra số thẻ phát hành.

b/. Kiểm tra tính hợp lệ của thẻ.

c/. Bảo đảm an toàn các khóa bí mật.

d/. Mã hóa số PIN của chủ thẻ trong CSDL Corebanhk.

e/. Mã hóa số PIN của chủ thẻ khi thực hiện giao dịch.

f/. Bảo đảm an toàn Phần mềm.

g/. Bảo đảm an toàn hệ điều hành.

h/. Bảo đảm an toàn trên đường truyền.

i/. Bảo đảm an toàn chống tấn công vật lý.

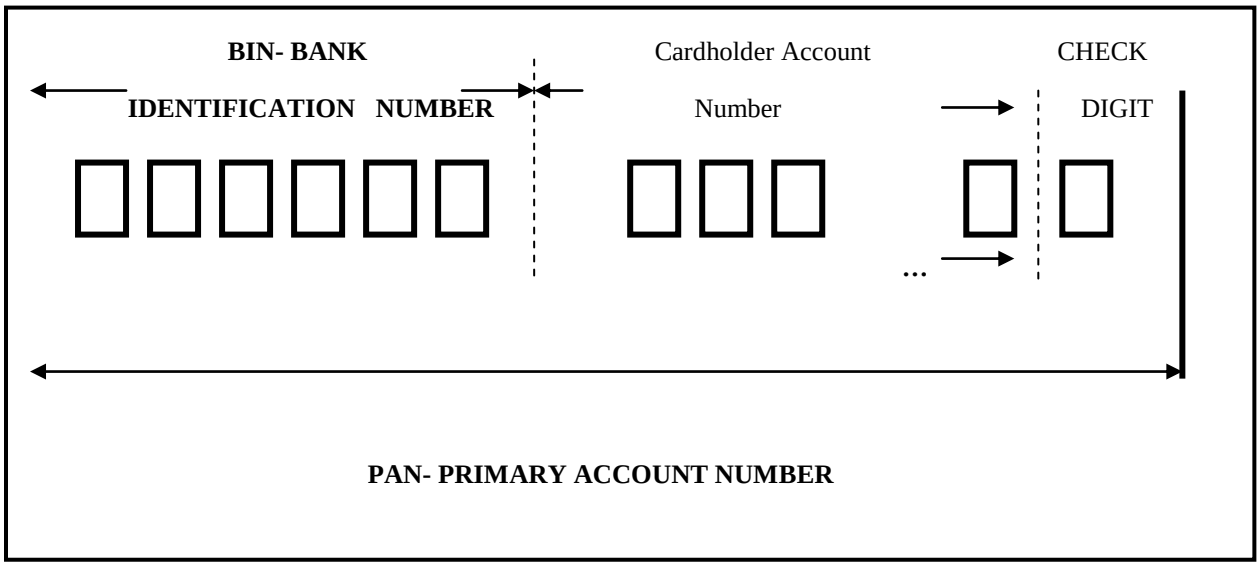
j/. Bảo đảm an toàn từ phía ngân hàng.

k/. Bảo đảm an toàn từ phía người dùng.

3.3.1. Kiểm tra tính đúng đắn số thẻ (Card number Check Digit)

3.3.1.1. Khái niệm số CD (Check Digit)

Trong quá trình phát hành thẻ, modul quản lý thẻ CMS (Card Management System) của hệ thống Switch sẽ tính toán ra một con số (nằm trong khoảng từ 0 đến 9) và gắn vào cuối thẻ, số này được gọi là Check Digit CD, chữ số này để kiểm tra số thẻ này là đúng hay sai.



Chữ số này nằm trong khoảng [0, 9], nên có thể dễ dàng tìm ra được bằng cách thay đổi chữ số cuối của thẻ với các giá trị lần lượt từ 0 đến 9.

3.3.1.2. Giải thuật tính số CD

Sử dụng giải thuật Luhn để sinh số CD. Giải thuật Luhn là cách thức kết hợp các chữ số của một mã số thẻ tín dụng (các chữ số xen kẽ nhau) và kiểm tra tổng cuối cùng có chia hết cho 10 hay không. Nếu đúng thì thẻ này hợp lệ.

Khi kiểm tra PIN nhập vào của chủ thẻ thì hệ thống Switch sẽ kiểm tra đồng thời số CD. Căn cứ vào thông tin thẻ, hệ thống tính số CD nếu so khớp thì thẻ hợp lệ.

Giải thuật này thực hiện như sau:

a) Từ các số thẻ cho trước ta làm từ trái qua phải

b) Các số nằm ở dòng chẵn thì nhân với 1 (để bình thường)

c) Các số nằm ở dòng lẻ thì nhân với 2.

d) Kiểm tra kết quả tính được, nếu số nào lớn hơn 9 thì trừ đi 9.

e) Cộng các kết quả tính được lại với nhau ta được một số.

f) Thực hiện phép tính lấy số đơn vị của số đó cộng với số cần tính để thành 10, khi đó giải phép toán ta được số CD.

1/. Quy trình tạo số CD

Ví dụ: có số thẻ 668899123456789Y, ta cần sinh số Y sao cho hợp lệ.

Bảng 3.1: Cách sinh số CD

	BIN															**CD**
PAN	6	6	8	8	9	9	1	2	3	4	5	6	7	8	9	Y
Nhân 2 (cột lẻ)	x2		x2		x2		x2		x2		x2		x2		x 2	Y
Kết quả	12	6	16	8	19	9	2	2	6	4	10	6	14	8	1 8	Y
Trừ 9 nếu >9	-9		-9		-9						-9		-9		-9	Y
Kết quả	3	6	7	8	9	9	2	2	6	4	1	6	5	8	8	Y
Cộng các chữ số lại	3+6+7+8+9+9+2+2+6+4+1+6+5+8+8+Y= 84+Y ***Giải bài toán:*** Lấy số hàng đơn vị của 84 cộng với Y có tổng bằng 10. 4+Y=10 => Y =6															
Kết quả	6	6	8	8	9	9	1	2	3	4	5	6	7	8	9	6

Y=6 => Số thẻ hợp lệ cho dãy số trên : PAN =6688991234567896

2/. Quy trình kiểm tra số CD

Hoàn toàn tương tự như trên, Sau khi cộng được các chữ số lại gồm cả số CD ta được tổng, nếu tổng này chia hết cho 10 thì số thẻ đó hợp lệ

Bảng 3.2 Cách kiểm tra số CD

	BIN															**Check Digit**
PAN	6	6	8	8	9	9	1	2	3	4	5	6	7	8	9	6
Nhân 2 (cột lẻ)	x2		x2		x2		x2		x2		x2		x2		x2	6
Kết quả	12	6	16	8	19	9	2	2	6	4	10	6	14	8	18	6
Trừ 9 nếu >9	-9		-9		-9						-9		-9		-9	6
Kết quả	3	6	7	8	9	9	2	2	6	4	1	6	5	8	8	6
Cộng các chữ số lại	3+6+7+8+9+9+2+2+6+4+1+6+5+8+8+6= 90 ***Giải bài toán:*** 90 mod 10 = 0															
Kết quả	Số thẻ hợp lệ															

3.3.2. Xác thực tinh hợp lệ của thẻ (Card Authenication values)

3.3.2.1. Khái niệm số CVV/CVC

Khi phát hành thẻ, đảm bảo thẻ không bị làm giả, người ta dùng số CVV/CVC (Card Verification value/ Card Verificatinon Code) để phân biệt thẻ thật thẻ giả.

Mỗi loại thẻ khi phát hành sẽ có một số CVV/CVC được lưu trong rãnh từ để sinh số này người ta sử dụng các điều kiện đầu vào bao gồm các số thẻ PAN, ngày hết hạn thẻ Card expiration date và Mã dịch vụ Service code.

Các giá trị đầu vào là duy nhất do đó mỗi thẻ chỉ có một số CVV/CVC duy nhất.

Khi kiểm tra PIN nhập vào của chủ thẻ thì hệ thông Switch sẽ kiểm tra đồng thời số CVV/CVC được lưu trong thẻ, nếu khớp thì thẻ hợp lệ.

Giải thuật sinh số CVV/CVC: thuật toán DES với độ dài khóa bí mật 64 bit.

Input: chuỗi 64 bit hay 16 ký tự hexa được gọi là Transformed Security Parameter (TSP), TSP tính từ số thẻ PAN, Ngày hết hạn thẻ Card Expiration date (YYMM) và mã dịch Service code.

Output: 16 ký tự hexa (64bit).

1/. Cách tạo số TSP

TSP có định dạng gồm 9 chữ số tính từ bên phải của số PAN loại từ số cuối cùng cộng với 4 số Exp date cộng với 3 số Service code

PAN: 6688991234567896

Exp date: 0909

Service code: 101

TSP= 123456789090910 1

2/. Cách tính số CVV/CVC

Ba số CVV/CVC được tính như sau:

- Từ dãy số 16 ký tự hexa kết quả đầu ra ta đi từ trái qua phải, khi đó CVV/CVC là 3 số thập phân đầu tiên trong dãy số 16 ký tự hexa.
- Nếu không tìm được đủ 3 số thập phân trong đó thì số còn thiếu sẽ sử dụng là các số không phải là thập phân tính từ trái qua và chuyển sang số thập phân theo công thức A->0, B->1, C->2, D->3, E->4, F->5.

Ví dụ: Output from DES: 0FAB9CDEFFEFDCBA

⇨ CVV/CVC là 095

3.3.2.2 Xác thực số CVV/CVC

Quá trình xác thực này diễn ra cùng với quá trình xác thực PIN của chủ thẻ.

a) Khi thực hiện xác thực PIN, thì đồng thời các thông tin của thẻ là Track 2 sẽ được gửi đến Switch. Thông tin để xác thực bao gồm số PAN, ngày hết hạn thẻ Expire date, mã dịch vụ Service và số CVV/CVC.

b) Bản mã của khóa CVK tại Switch được giải mã bởi khóa LMK trong HSM

c) Sử dụng khóa CVK trong thuật toán DES để sinh số CVV/CVC. Kiểm tra số CVK

d) Kết quả kiểm tra được gửi lại cho ATM.

3.3.3. Bảo đảm an toàn thông tin giao dịch

+ Bảo mật số PIN.

+ Bảo đảm an toàn các khóa bí mật trong hệ thống ATM.

Bản rõ của PIN không bao giờ xuất hiện bên ngoài một thiết bị EPP hay HSM.

Để đảm bảo an toàn, số PIN sẽ được mã hóa trước khi thực hiện giao dịch.

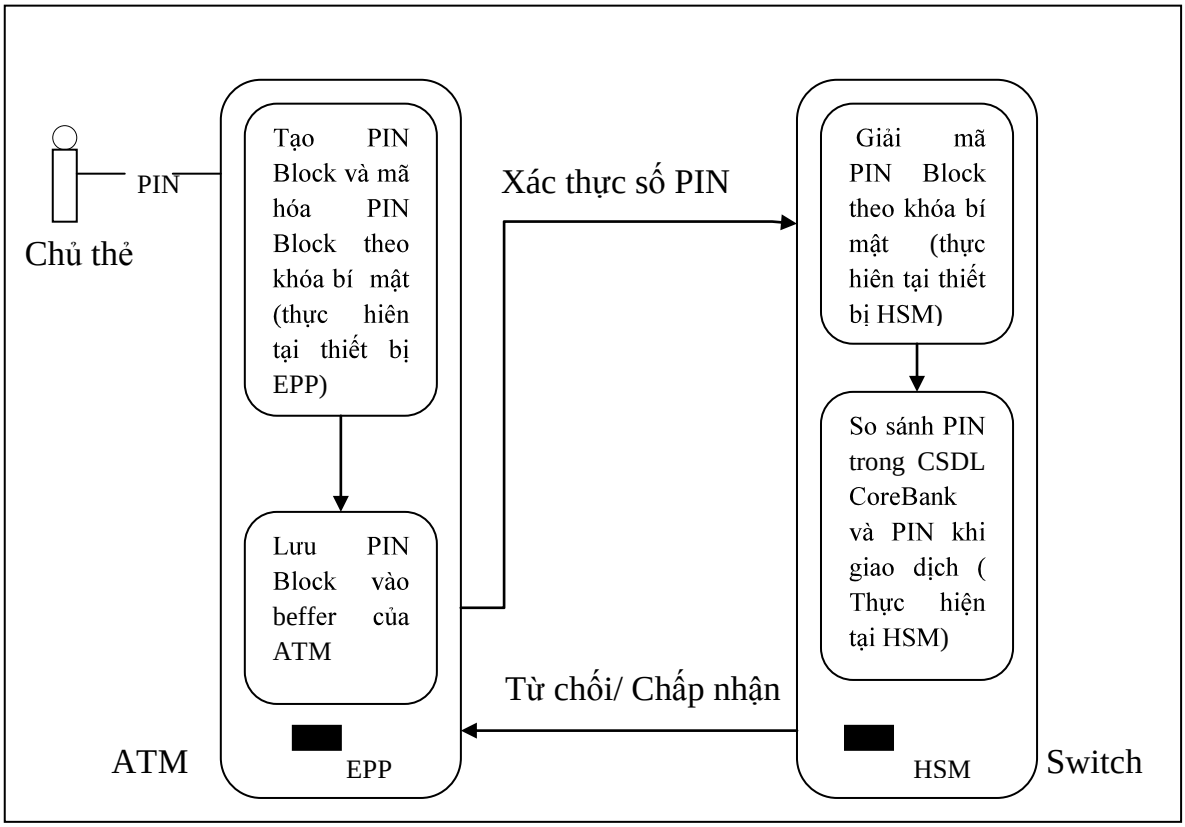
Số PIN của chủ thẻ được lưu trong CSDL Core Bank dưới dạng bản đã mã hóa.

Không truy cập hoặc xác định được bản rõ của bất kỳ khóa bí mật nào được lưu trữ trong thiết bị EPP, HSM một cách bất hợp pháp.

Khi bị xâm nhập một cách bất hợp pháp, khóa bí mật sẽ tự bị hủy.

Khóa có độ dài 64bit, 128bit hoặc 192bit tùy theo cách sử dụng khóa hoặc chọn mã khóa DES hay 3DES.

Quá trình xác thực PIN được thực hiện theo mô hình sau:



Hình 3.19 Quy trình mã hóa và xác thực PIN

Bước 1: Chủ thẻ đưa thẻ và nhập PIN tại máy ATM

Bước 2: Tạo và mã hóa PIN Block bằng thuật toán DES (3DES) tại EPP

Bước 3: Lưu PIN Block vào bộ đệm của ATM

Bước 4: Giải mã PIN Block tại HSM.

Bước 5: So sánh PIN trong CSDL của chủ thẻ và PIN của giao dịch tại HSM.

Bước 6: Kết quả phản hồi cho máy ATM la từ chối hay chấp nhận giao dịch

3.3.4. Đảm bảo an toàn phần mềm ATM

Đảm bảo phần mềm cài đặt có bản quyền và không cài đặt các phần mềm không được phép.

Đảm bảo an toàn mật khẩu truy nhập vào phần mềm.

3.3.5. Bảo đảm an toàn hệ điều hành

Để đảm bảo an toàn cho hệ điều hành ta cần thực hiện một số nội dung sau. Vì hệ điều hành trong máy ATM được sử dụng là hệ điều hành thông thường, nên ta cần đảm bảo sự an toàn theo như khuyến cáo của nhà sản xuất.

- Tắt các service không dùng.
- Đóng các cổng không dùng.
- Thiết lập FireWall cho máy ATM.

3.3.6. Bảo đảm an toàn chống tấn công vật lý

ATM được bảo vệ bằng vỏ thép, các hộp đựng tiền được đặt trong một tủ mà được gọi là két sắt. Két sắt gồm có khóa số và khóa chìa để đảm bảo an toan.

ATM còn sử dụng cơ chế phát hiện rung, khi đó hệ thống chuông sẽ rung để thông báo ATM bị tấn công.

ATM có hệ thông phun mực vào các tờ tiền khi các hộp đựng tiền bị xâm nhập trái phép.

ATM có hệ thống camera giám sát và ghi lại.

3.3.7. Bảo đảm an toàn từ phía ngân hàng

Thiết lập các danh sách thẻ nóng, thẻ đen để hạn chế sự gian lận của tội pham.

Phân quyền và kiểm soát truy cập đến tài nguyên của hệ thống, sao cho thông tin không bị lộ với người không được phép, thông tin sẵn sàng cho người dùng hợp pháp.

3.3.8. Bảo đảm an toàn tư phía người dùng

Một trong những cái khó ở đây chính là bản thân chủ thẻ cũng không biết mình bị mất cắp tài khoản, chỉ đến khi kiểm tra số dư mới thấy nghi ngờ. Còn bản thân NH thì cũng không thể nắm rõ đâu là giao dịch của chủ thẻ, đâu là của tội phạm. Vì thế, sự cảnh giác của các chủ thẻ cũng là vô cùng quan trọng và chính khách hàng là người đảm bảo an toàn cho những thông tin giao dịch của mình.

Khi thông tin về thẻ bị lộ, thì ngay lập tức thông báo cho phía NH để NH khóa thẻ và kiểm tra giao dịch nghi vấn liên quan đến thẻ.

Chủ thẻ cần phải chú ý đến những trò gian lận ATM sau:

3.3.8.1. Lấy cắp thẻ và số PIN

Bước đầu tiên, bọn tội phạm sẽ lắp vào khe đọc thẻ của một máy một miếng nhựa có khả năng giữ thẻ và ngăn máy nhả ra. Khi đó chủ thẻ sẽ nghĩ mình thao tác nhầm và bị máy nuốt thẻ, chứ không chú ý xem khe đọc thẻ có gì bất thường không.

Khi đó kẻ gian lại gần chúng sẽ "tư vấn" chủ thẻ nên nhập lại số PIN để lấy lại thẻ và theo dõi. Tất nhiên việc nhập lại số PIN chả giúp ích gì cho chủ thẻ cả, nhưng lại là cơ hội để kẻ gian biết được mật mã truy cập tài khoản thẻ của nạn nhân.

Khi chủ thẻ thất vọng bỏ đi, kẻ gian sẽ ở lại lấy thẻ ra, rồi dùng PIN vừa nhìn trộm được để truy cập vào tài khoản và rút tiền.

3.3.8.2. Trộm dữ liệu

Đây là cách ăn cắp thông tin tài khoản và PIN mà không cần tiếp cận trực tiếp với chủ thẻ. Thông thường, bon tội phạm cài thêm một thiết bị đọc dữ liệu vào khe đọc của ATM.

Khi chủ thẻ thực hiện giao dịch, toàn bộ thông tin trên thẻ đã được lưu giữ lại trong thiết bị đọc thẻ mà bọn tội phạm cài vào.

Khi nạn nhân ra đi, bọn tội phạm sẽ lấy thiết bị ra, sử dụng các thông tin vừa chôm được đẻ làm thẻ giả hoặc mua hàng qua mạng, qua điện thoại.

3.3.8.3. Trộm dữ liệu bằng camera

Bọn tội phạm vẫn lắp đặt thiết bị đọc thẻ vào máy như trước, nhưng chúng có thể lấy dữ liệu về tài khoản và số PIN từ xa nhờ một chiếc camera mà chúng lắp kín

đáo tại máy ATM. Camera thường đặt kín đáo, một vị trí có thể ghi hình toàn bộ các thao tác của chủ thẻ cũng như lưu giữ số liệu.

3.3.8.4 Nhìn trộm qua vai

Bọn tội phạm có thể đứng gần ATM, theo dõi quá trình bạn thao tác trên máy. Để tránh loại tội phạm này, phần lớn người tiêu dùng đều cảnh giác che bàn phím khi nhập mã số. Việc ăn cắp dữ liệu này rất thô sơ, song đang có xu hướng nở rộ trở lại vì không phải chủ thẻ nào cũng thận trọng mỗi khi giao dịch trên máy.

Cũng với mưu chước "nhìn trộm qua vai" này, bọn tội phạm sẽ đứng nấp gần ATM và theo dõi chủ thẻ khi họ nhập PIN. Sau đó, chúng sẽ tìm cách làm chủ thẻ mất tập trung, chẳng hạn hét lên hoặc đánh rơi tiền và hỏi đó là tiền của ai. Trong lúc chủ thẻ sao nhãng, kẻ gian liền cuỗm toàn bộ thẻ tiền.

Chương 4. THỬ NGHIỆM CHƯƠNG TRÌNH

4.1. MÔ TẢ CHƯƠNG TRÌNH

4.1.1. Giới thiệu

Chương trình mã hóa và giải mã DES, được viết bằng ngôn ngữ lập trình VB.net.

- ***Cấu hình của hệ thống***

* Phần cứng (cấu hình tối thiểu):

Bộ nhớ ổ cứng: 20gb

Bộ nhớ ram: 128 mb

Tốc độ máy tối thiểu: 1 GHz

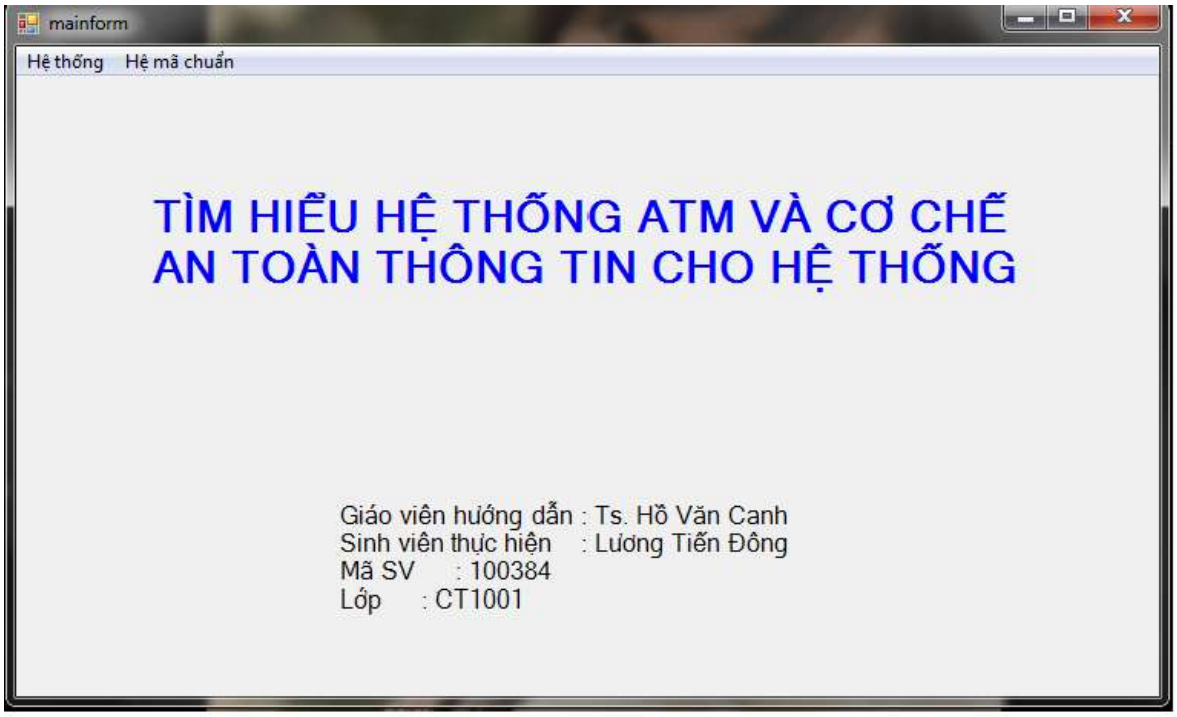
* Phần mềm:

Hệ điều hành:Linux, Window,…

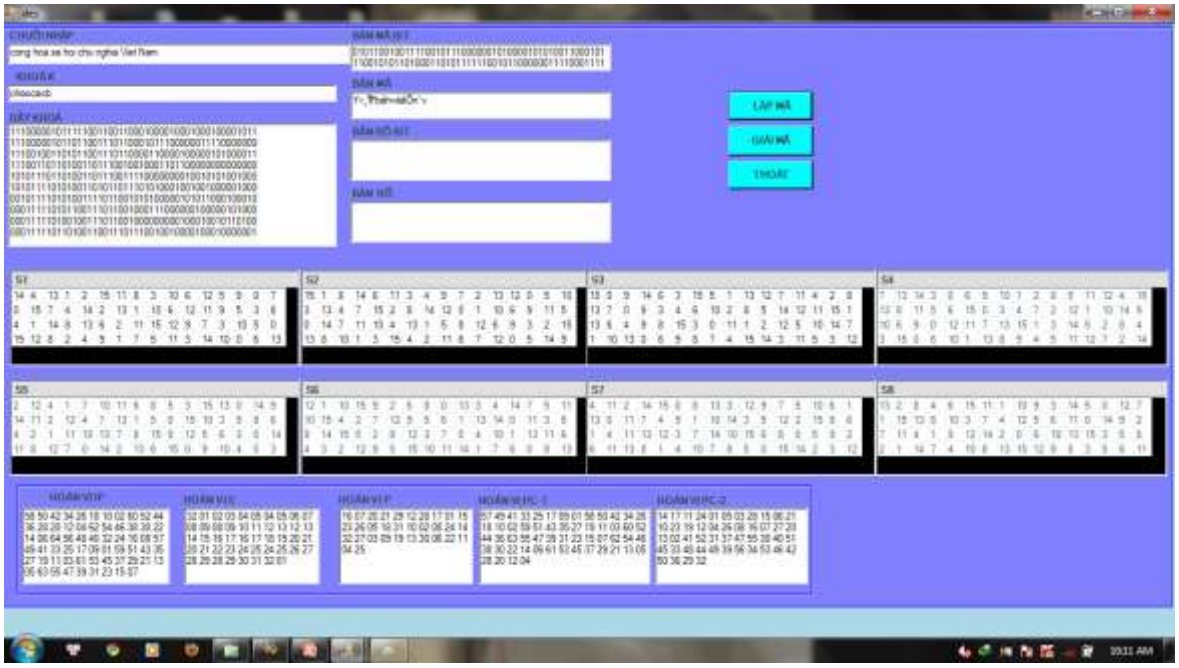
Ngôn ngữ lập trình: VB.net

4.1.2. Các chức năng chính

1). Giao diện chính chương trình



2). Quá trình lập mã



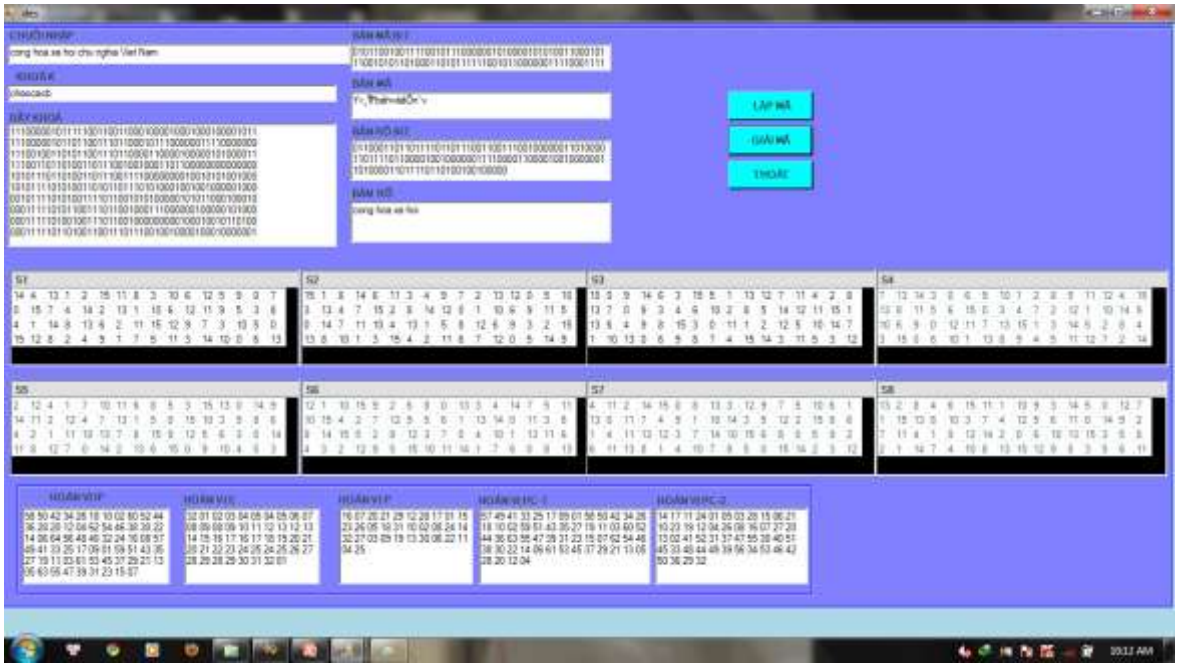
Bước 1: Nhập chuỗi cần mã hóa

Bước 2: Nhập khóa K gồm 8 kí tự

Bước 3: Click vào nút lập mã để bắt đầu quá trình lập mã

Kết quả đạt được là chuỗi kí tự đã được mã hóa.

3). Quá trình giải mã



Bước 1: Nhập chuỗi cần giải mã vào ô text bản mã

Bước 2: Nhập khóa K gồm 8 kí tự

Bước 3: Click vào nút giải mã để bắt đầu quá trình giải mã

Kết quả đạt được là chuỗi kí tự được giải mã

KẾT LUẬN

Trong đề tài đồ án em đã tìm hiểu tổng quan về máy ATM (Automatic Teller Machine), cấu trúc của máy ATM và hệ thống liên kết của chúng. Trong đó em chủ yếu tập trung tìm hiểu thẻ từ, vấn đề an ninh / an toàn thông tin cho hệ thống ATM được đặc biệt lưu ý vì theo em đây là vấn đề cốt lõi để hệ thống ATM được đứng vững và phát triển. Do đó, trong đề tài đồ án em đã tập trung tìm hiểu cơ chế an ninh / an toàn thông tin trong hệ thống ATM: bao gồm mã hóa, giải mã thông tin truyền và lưu trong hệ thống, mã hóa và giải mã số PIN (Personal Identification Number), v.v.

Tuy nhiên, do trình độ hạn chế và các tài liệu tham khảo bằng tiếng Việt 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 các thầy, cô để đồ án của em được hoàn thiện hơn.

Em xin chân thành cảm ơn các thầy, cô và các bạn đồng môn đã tạo điều kiện để em hoàn thành đúng quy định đồ án của mình.

TÀI LIỆU THAM KHẢO

1. Báo tin học và Tài chính – Bộ tài chính (4/2008), Sự hình thành và phát triển của máy ATM, (số 58)

2. Banknetvn (2006), tài liệu tiêu chuẩn kỹ thuật về hệ thống Switch.

3. Bach khoa toàn thư mở Wikipedia ,Hệ mã hóa DES, được lấy về tại: http://vi.wikipedia.org/wiki/DES_(m%C3%A3_h%C3%B3a).

4. DIEBOLD (2007), Tài liệu giới thiệu hệ thống ATM.

5. Hiệp hội ngân hàng việt nam, 10 năm phát triển của thị trường thẻ, được lấy về tại:

http://www.vnba.org.vn/index.php?option=com_content&task=view&id=374&Itemid=92.

6. Hồ Văn Canh TS (2003), Tài liệu giảng dạy hệ mã hóa DES.

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

8. Trịnh Nhật Tiến PGS. TS (2007), Bài giảng môn An toàn và bảo mật dữ liệu