MỤC LỤC

LỜI NÓI ĐẦU

Ngày nay cùng với sự phát triển vượt bậc về khoa học công nghệ, sự mở rộng và phổ biến của Internet. Từ những nhu cầu thực tế đã thúc đẩy sự phát triển của thương mai điện tử. Từ những hình thức thanh toán đơn giản đến nhu cầu thanh toán hiện đại, đòi hỏi phải có những hình thức thanh toán thông minh, an toàn. Điều đó dẫn đến công nghệ thanh toán điện tử ra đời và một trong những công nghệ đó là thanh toán tiền điện tử.

Trên toàn thế giới, tiền điện tử đã và đang được sử dụng thành công, đem lại lợi ích cho người dùng. Tuy nhiên trong quá trình sử dụng tiền điện tử đã nảy sinh một số vấn đề đáng quan tâm như: người dùng gian lận giá trị đồng tiền, tiêu nhiều lần một đồng tiền hay xác định danh tính người sở hữu đồng tiền.

Đồ án đi vào nghiên cứu một số bài toán trong giai đoạn thanh toán tiền điện tử và trình bày những cách giải quyết phù hợp cho bài toán đề trên

Mục đích của đồ án là nghiên cứu một số giải pháp khoa học cho các bài toán phát sinh trong quá trình thanh toán tiền điện tử, so sánh, đánh giá ưu nhược điểm của các giải pháp và chỉ rõ giải pháp nào phù hợp với từng loại tiền điện tử.

Do thời gian và kiến thức còn nhiều hạn chế, nên quyển đồ án này sẽ còn nhiều thiếu sót. Kính mong nhận được sự hướng dẫn, góp ý thêm của thầy cô và bạn bè.

Em xin chân thành cảm ơn!

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1. TỔNG QUAN VỀ BẢO VỆ THÔNG TIN

1.1.1. Chức năng , Nhiệm vụ của Bảo vệ thông tin

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng , các tiến bộ về điện tử – viễn thông và công nghệ thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới . Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu:

+ Bảo vệ an toàn thông tin bằng các biện pháp hành chính

+ Bảo vệ an toàn thông tin bằng các biện pháp kĩ thuật (phần cứng)

+ Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phầm mềm)

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và quá trình truyền tin.

An toàn thông tin bao gồm các nội dung sau:

+ Bảo mật : Bảo vệ tính riêng tư của thông tin.

+ Bảo toàn : Bảo vệ thông tin , phòng tránh sửa đổi trái phép.

+ Xác thực : Bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.

+ Trách nhiệm : Đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả, thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn , khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với

thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin và cũng như trên mạng.

Có hai loại hành xi xâm phạm thông tin dữ liệu đó là : vi phạm chủ động và vi phạm thụ động. Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được sô lượng, độ dài và tần số trao đổi. Vì vậy vi phạm thụ động không làm sai lệch hoặc hủy hoại nội dung thông tin dữ liệu được trao đổi. Vi phạm thụ động thường khó phát hiện nhưng có thể có những biện pháp ngăn chặn hiệu quả. Vi phạm chủ động là dạng vi phạm có thể làm thay đổi nội dung, xóa bỏ, làm trễ, xắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau đó một thời gian. Vi phạm chủ động có thể them vào một số thông tin ngoại lai để làm sai lệch nội dung thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn hiệu quả thì khó khăn hơn nhiều.

Một thực tế là không có một biện pháp bảo vệ an toàn thông tin dữ liệu nào là an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến đâu cũng không thể đảm bảo là an toàn tuyệt đối.

1.1.2. Các Phương pháp bảo vệ thông tin

1.1.2.1. Các chiến lược chính

***Giới hạn quyền tối thiểu (Last Privilege)**

Đây là chiến lược cơ bản nhất , theo nguyên tắc này bất kỳ một đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên trên mạng, khi thâm nhập vào mạng đối tượng đó chỉ được sử dụng một số tài nguyên nhất định.

***Bảo vệ theo chiều sâu (Defence In Depth)**

Nguyên tắc này nhắc nhở chúng ta : Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh , mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.

***Nút thắt (Choke Point)**

Tạo ra một " cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này, nghĩa là phải tổ chức một cơ cấu kiểm soát và điều khiển thông tin đi qua cửa khẩu này.

***Điểm nối yếu nhất (Weakest Link)**

Chiến lược này dựa trên nguyên tắc: " Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất" Kẻ phá hoại thường tìm những chỗ yếu nhất của hệ thống để tấn công, do dó ta cần phải gia cố các điểm yếu của hệ thống. Thông thường chúng ta chỉ quan tâm đến kẻ tấn công trên mạng hơn là kẻ tiếp cận hệ thống , do đó an toàn vật lý được coi là yếu điểm nhất trong hệ thống của chúng ta.

***Tính toàn cục**

Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có một kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng ra có thể thành công bằng cách tấn công hệ thống tự do của ai đó và sau đó tấn công hệ thống từ nội bộ bên trong.

***Tính đa dạng bảo vệ**

Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

1.1.2.2 Các mức bảo vệ trên mạng

Vì không thể có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều hàng rào chắn đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong máy tính , đặc biệt là các sever trên mạng. Bởi thế ngoài một số biện pháp nhằm chống thất thoát thông tin trên đường truyền mọi cố gắng tập trung vào việc xây dựng các mức rào chắn từ ngoài vào trong cho các hệ thống kết nối vào mạng. Thông thường bao gồm các mức bảo vệ sau:

***Quyền truy nhập**

Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát cac tài nguyên của mạng và quyền hạn trên tài nguyên đó. Dĩ nhiên là kiểm soát được các cấu trúc dữ liệu càng chi tiết càng tốt. Hiện tại việc kiểm soát thường ở mức tệp.

***Đăng ký tên/mật khẩu**

Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không truy nhập ở mức thông thường mà ở mức ở hệ thống. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản ít phí tổn và cũng rất hiệu quả. Mỗi người sử dụng muốn được tham gia vào mạng để sử dụng tài nguyên đều phải có tên đăng ký và mật khẩu trước. Người quản trị mạng có nhiệm vụ quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác theo thời gian và không gian (người sử dụng chị được truy nhập trong một thời gian nào đó tại một vị trí nhất định nào đó).

Về lý thuyết nếu mọi người đều giữ kín được mật khẩu và tên đăng ký của mình thì sẽ không xảy ra các truy nhập trái phép. Song điều đó khó đảm bảo trong thực tế vì nhiều nguyên nhân rất đời thường làm giảm hiệu quả của lớp bảo vệ này. Có thể khắc phục bằng cách người quản trị mạng chịu trách nhiệm đặt mật khẩu hoặc thay đổi mật khẩu theo thời gian.

***Mã hóa dữ liệu**

Để đảm bảo thông tin trên đường truyền người ta thường sử dụng các phương pháp mã hóa. Dữ liệu bị biến đổi từ dạng nhân thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã). Đây là lớp bảo vệ thông tin rất quan trọng.

***Bảo vệ vật lý**

Ngăn cản các truy nhập vật lý vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khóa trên máy tính hoặc các trạm không có ổ lưu trữ ngoài như CD-ROM, USB disk…

***Tường lửa**

Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).

***Quản trị mạng**

Trong thời đại phát triển của công nghệ thông tin, mạng máy tính quyết định toàn bộ hoạt động của một cơ quan, hay một công ty xí nghiệp. Vì vậy việc bảo đảm cho hệ thống mạng máy tính hoạt động một cách an toàn, không xảy ra các sự cố là một công việc cấp thiết hàng đầu.

Mức độ bảo vệ

- *Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.*
- *Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra.*
- *Backup dữ liệu quan trong định kì.*
- *Bảo dưỡng mạng theo định kì.*
- *Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng.*

1.1.2.3 An toàn thông tin bằng mật mã

Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm: lập mã và phá mã. Lập mã bao gồm hai quá trình: mã hóa và giải mã.

Để bảo vệ thông tin trên đường truyền người ta thường biến đổi nó từ dạng nhận thức được sang dạng không nhận thức được trước khi truyền đi trên mạng, quá trình này được gọi là mã hóa thông tin (encryption), ở trạm nhận phải thực hiện quá trình ngược lại, tưc là biến đổi thông tin từ dạng không nhận thức được (dữ liệu đã được mã hóa) về dạng nhận thức được (dạng gốc), quá trình này được gọi là giải mã. Đây là một lớp bảo vệ thông tin rất quan trọng và được sử dụng rộng rãi trong môi trường mạng

Để bảo vệ thông tin bằng mật mã người ta thường tiếp cận theo hai hướng:

- *Theo đường truyền (Link_Oriented_Security).*
- *Từ nút đến nút (End_to_End).*

Theo các thứ nhất thông tin được mã hóa để bảo vệ trên đường truyền giữa hai nút mà không quan tâm đến nguồn và địch của thông tin đó. Ở đây ta lưu ý rằng thông tin chỉ được bảo vệ trên đường truyền, tức là ở mỗi nút đều có quá trình giải mã sau đó mã hóa để truyển đi tiếp, do đó các nút cần được bảo vệ tốt.

Ngược lại theo các thứ hai thông tin trên mạng được bảo vệ trên toàn đường truyền từ nguồn đến đích. Thông tin sẽ được mã hóa ngay sau khi mới tạo ra và chỉ được giải mã khi về đến đích. Cách này mắc phải nhược điểm là chỉ có dữ liệu của người dùng thỳ mới có thể mà hóa được còn dữ liệu điều khiển thỳ giữ nguyên để có thể xử lý tại các nút.

1.2. MỘT SỐ KHÁI NIỆM CƠ BẢN TRONG TOÁN HỌC

1.2.1. Khái niệm trong số học

Số nguyên tố và nguyên tố cùng nhau.

Số nguyên tố là số chỉ chia hết cho 1 và chính nó.

Ví dụ:2, 3, 5, 7, 17,… là những số nguyên tố.

Hai số m và n được gọi là nguyên tố cùng nhau nếu ước số chung lớn nhất của chúng bằng 1.

Ký hiệu : gcd(m,n)=1.

Ví dụ: 9 và 14 là nguyên tố cùng nhau.

Đồng dư thức.

Định nghĩa

Cho a và b là các số nguyên , n là số nguyên dương thì a được gọi là đồng dư với b theo mod n nếu n | (a-b) (tức (a - b) chia hết cho n, hay khi chia a và b cho n được cùng một số dư như nhau). Số nguyên n được gọi là mod của đồng dư.

Ký hiệu

$a \equiv b \pmod{n}$

Ví dụ:

$67 \equiv 11 \pmod 7$, bởi vì $67 \pmod 7 = 4$ và $11 \pmod 7 = 4$

Tính chất của đồng dư

Cho a , a1, b, b1, c € Z. Ta có các tính chất sau:

$a \equiv b \bmod n$ khi và chỉ khi a và b có cùng số dư khi chia cho n.

Tính phản xạ: $a \equiv a \bmod n$.

Tính đối xứng : Nếu $a \equiv b \bmod n$ thì $b \equiv a \bmod n$.

Tính giao hoán: Nếu $a \equiv b \bmod n$ và $b \equiv c \bmod n$ thì $a \equiv c \bmod n$.

$a \equiv a1 \bmod n$, $b \equiv b1 \bmod n$ thì $a + b = a1 + b1 \bmod n$ và $ab = a1b1 \bmod n$.

Lớp tương đương đồng dư

Lớp tương đương của một số nguyên a theo modulo n là tập hợp các số nguyên đồng dư với a theo mod n.

Mỗi lớp tương dương như vậy được đại điện bởi một số duy nhất trong tập hợp Z_n = {0, 1, 2, 3,…,n-1}, là số dư chung khi chia các số đó cho n. Vì vậy, ta có thể đồng nhất Z_n với tập tất cả các lớp tương đương các số nguyên theo mod n, trên tập đó ta có thể xác định các phép tính cộng, trừ và nhân theo mod n.

Tập Z_n = {0, 1, 2, 3,…,n-1} được gọi là tập thặng dư đầy đủ theo mod n , vì mọi số nguyên bất kì đều có thể tìm đc trong Z_n một số đồng dư với mình (theo mod n).

Tập Z_n^* = { a $\in Z_n$: gcd (a, n) = 1}, tức Z_n^* là tập con của Z_n bao gồm tất cả các phần tử nguyên tố với n. Ta gọi tập đó là tập các thặng dư thu gọn theo mod n.

Phần tử nghịch đảo

Định nghĩa

Cho a $\in Z_n$. Nghịch đảo của a theo modulo n là một số nguyên x $\in Z_n$ sao cho ax ≡ 1 (mod n). Nếu tồn tại giá trị x trong khoảng (0,n) thì giá trị đó là duy nhất và kí hiệu là a^{-1}.

Tính chất

Cho a, b $\in Z_n$. Phép chia của a cho b theo mod n là tích của a và b^{-1} theo mod n, và chỉ được xác định khi b có nghịch đảo theo mod n.

Cho a $\in Z_n$, a khả nghịch khi và chỉ khi gcd(a, n) = 1.

Giả sử d = gcd(a, n). Phương trình đồng dư ax ≡ b mod n có nghiệm x khi và chỉ khi d chia hết cho b , trong trường hợp các nghiệm d nằm trong khoảng 0 đến n – 1 thì các nghiệm đồng dư theo modulo n/d.

Ví dụ:

4^{-1} = 7 (mod 9) vì 4.7 ≡ 1 (mod 9)

1.2.2. Khái niệm trong đại số

**** Khái niệm nhóm***

Khái niệm

Nhóm là bộ phận các phần tử (G, *) thỏa mãn các tính chất sau:

Tính chất kết hợp : (x * y) * z = x * (y * z)

Tính chất tồn tại phần tử trung gian:

$e \in G: e * x = x * e = x , \forall x \in G$

Tính chất tồn tại phần tử nghịch đảo:

$x' \in G: x' * x = x * x' = e$

Cấp của nhóm

Ta gọi số các phần tử trong 1 nhóm là *cấp của nhóm đó.*

Ta kí hiệu Ø(n) là các số nguyên dương bé hơn n và nguyên tố cùng với n. Như vậy, nhóm Z_n^* có cấp Ø(n) và nếu p là số nguyên tố thì nhóm Z_p^* có cấp p – 1 .

Cấp của phần tử

Ta nói một phần tử $g \in Z_n^*$ có cấp m, nếu m là số nguyên dương bé nhất sao cho $g^m \equiv 1 \bmod n$.

****Khái niệm nhóm con***

Nhóm con là bộ phận các phần tử (S, *) thỏa mãn các tính chất sau:

$S \in G$, Phần tử trung gian $e \in S$

$x, y \in S \Rightarrow x * y \in S$

****Khái niệm nhóm Cyclic***

Nhóm Cyclic là nhóm mà mọi phần tử x của nó được sinh ra từ một phần tử đặc biệt $g \in G$. Phần tử này được gọi là phần tử sinh (nguyên thủy) , tức là :

Với $\forall x \in G: \exists n \in N$ mà $g^n = x$.

Ví dụ: (Z^+ , +) là một nhóm cyclic có phần tử sinh là 1.

1.3 MÃ HÓA

1.3.1 Khái niệm mã hóa

Mã hóa là phương pháp biến đổi thông tin (phim , ảnh, văn bản,…) từ dạng bình thường sang dạng thông tin "khó" có thể hiểu được, nếu không có phương tiện giải mã. Giải mã là phương pháp chuyển thông tin đã được mã hóa về dạng thông tin ban đầu (quá trình ngược của mã hóa).

Mã hóa tuân theo quy tắc nhất định gọi là hệ mã hóa. Có hai loại:

-*Mã hóa đối xứng*.

-*Mã hóa công khai (phi đối xứng).*

Sau đây là định nghĩa hình thức về sơ đồ mã hóa và cách thức thực hiện để lập mã và giải mã:

Một sơ đồ hệ thống mã hóa là một bộ năm δ = (P, C, K, E, D) thỏa mãn:

P là một tập hữu hạn các ký tự bản rõ,

C là một tập hữu hạn các ký tự bản mã,

K là một tập hữu hạn các khóa,

E là một ánh xạ từ P x K vào C được gọi là phép lập mã

P là một ánh xạ từ K x C vào P, được gọi là phép giải mã

Với mỗi k ∈ K ta định nghĩa $e_k \in$ E; e_k : P $\rightarrow$ C là hàm lập mã và d_k: C $\rightarrow$ P là hàm giải mã sao cho:

$\forall$x ∈ P: e_k(x) = E (K, x)

$\forall$y∈ C: d_k(x) = D (K, y)

e_k và d_k được gọi là hàm lập mã và hàm giải mã ứng với khóa mật mã K. Các hàm đó phải thỏa mãn hệ thức:

$\forall$x ∈ P: d_k(e_k(x)) = x

Hệ mã hóa công khai sử dụng một cặp khóa. Một trong hai khóa được gọi là khóa riêng (Private Key) và phải được giữ bí mật bởi người sở hữu. Khóa còn lại được gọi là công khai (Public Key), nó được phổ biến cho tất cả những ai muốn giao dịch với người riêng tương ứng. Cặp khóa này có liên quan về mặt toán học, và không thể sử dụng các thông tin của khóa công khai để tìm ra khóa riêng.

Theo lý thuyết bất kì ai cũng có thể gửi cho giữ khóa riêng một thông điệp được mã hóa bằng khóa công khai, và như vậy chỉ có người nào sở hữu mã công riêng mới có thể giãi mã được. Đồng thời, người sở hữu khóa riêng cũng chứng minh được tính toàn vẹn của dữ liệu mà anh ta gửi cho người khác bằng chữ kí điện tử thông qua việc sử dụng khóa riêng để mã hóa. Bất kì ai nhận được dữ liệu đó đều có thể sử dụng khóa công khai tương ứng để kiểm tra xem nó do ai gửi và có toàn vẹn hay không.

1.3.2 Hệ mã hóa khóa công khai RSA

RSA là hệ mã hóa công khai, độ an toàn của hệ dựa vào bài toán khó:" Phân tích số nguyên thành thừa số nguyên tố".

Sơ đồ

- Chọn ngẫu nhiên và độc lập hai số nguyên tố lớn p và q với $p \neq q$

- Tính : $n = p.q$

- Tính giá trị hàm số PhiƠle: $\Phi(n) = (p-1)(q-1)$
- Tính chất của hàm $\Phi(n)$:

  1./Nếu n là số nguyên tố thỳ $\Phi(n) = n - 1$

  2./Nếu n=p.q là 2 số nguyên tố thỳ $\Phi(n) = \Phi(p.q)$ =(p-1)(q-1)

  3./Nếu n=m1.m2. Trong đó (m1,m2)=1 thỳ:

  $$\Phi(m1.m2) = \Phi(m1)\ \Phi(m2)$$

- Chọn số tự nhiên *b*, $1 < b < \Phi(n)$ và là số nguyên tố cùng nhau với $\Phi(n)$

- Tính a là nghịch đảo của *b* : $ab \equiv 1 (mod\, \Phi(n))$

Khi đó, *b* là khóa lập mã, công khai ; a là khóa giải mã, bí mật.

Lập mã

Chọn P = C = Z_n với $n = p.q$, $Z_n = \{0, 1, 2, ..., n-1\}$

$x \in Z_n \rightarrow y = x^b \bmod n \in Z_n$

Giải mã

$y \in Z_n \rightarrow x = y^a \bmod n \in Z_n$

1.4 CHỮ KÝ SỐ

Ký số là phương pháp ký một thông điệp lưu dưới dạng "số" (điện tử).Thông điệp được ký và chữ ký cùng truyền trên mạng tới người nhận.

Với chữ ký truyền thống , khi ký lên tài liệu thì chữ kí gắn kết với tài liệu được ký. Chữ ký số không được gắn một cách vật lý với thông điệp được ký.

Đối với chữ ký trên giấy, ta kiểm tra bằng cách so sánh nó với chữ ký gốc đã đăng ký. Tất nhiên, phương pháp này không an toàn vì có thể bị đánh lừa bởi chữ ký của người khác. Trong khi chữ ký số được kiểm tra bằng thuật toán kiểm tra công khai, " người bất kì" có thể kiểm tra chữ ký số. Việc sử dụng lược đồ ký an toàn sẽ ngăn chặn khả năng đánh lừa (giả mạo chữ ký).

Sơ đồ chữ ký số là bộ năm (**P, A, K, S, V)** trong đó:

P: tập hữu hạn các thông điệp **A:** tập hữu hạn các chữ ký.

K: tập hữu hạn các khóa (không gian khóa).

Với mỗi $k \in K$ tồn tại thuật toán kí $sig_k \in \mathbf{S}$ và một thuật toán xác minh $ver_k \in \mathbf{V}$.

Mỗi sig_k:P → A và ver_k : P x A → $\{true, false\}$ là những hàm sao cho mỗi thông điệp x ∈**P** và mỗi chữ ký y thỏa mãn phường trình dưới đây:

$$ver(x.y) = ver(x.y) = \begin{cases} true\ khi\ y = sig\ (x) \\ false\ khi\ y \neq sig(x) \end{cases}$$

1.4.1 Một số sơ đồ ký số

1.4.1.1 Sơ đồ ký số RSA

Sơ đồ ký số RSA được cho bởi bộ năm : S = (**P, A, K, S, V).**

1./Chuẩn bị

P = **A** = Z_n , với n = p.q và q là các số nguyên tố lớn.

Φ(n) = (p – 1)(q – 1) K = (n, p, q, a, b)

Chọn b $\in Z_n$ nguyên tố cùng nhau với Φ(n)

Chọn a $\in Z_n$ là nghịch đảo của b thep module Φ(n)

Các giá trị n và b công khai; các giá trị p, q, a bí mật.

2./Kí

Với mỗi K = (n, p, q, a, b) và x $\in Z_n$ ta định nghĩa chữ ký là:

y = $sig_k(x) = x^a \bmod n, y \in A$

3./Kiểm tra chữ kí

$Ver_k(x, y)$= true $\Leftrightarrow \Leftrightarrow x \equiv y^b \pmod n$

1.4.1.2 Sơ đồ ký số Schnorr

1./Chuẩn bị

Lấy G là nhóm con cấp q của Z_n^* với q là số nguyên tố

Chọn phần tử sinh $g \in$G sao cho bài toán logarit trên G là khó giải .

Chọn $x \neq 0$ làm khóa bít mật Tính $y = g^x$ làm khóa công khai

Lấy H là hàm băm không va chạm.

2./Ký:

Giả sử cần ký trên văn bản m.

Chọn r ngẫu nhiên thuộc Z_q, Tính c = H(m, x^r), Tính s = (r+xc)mod q

Chữ ký Schnorr là cặp (c, s)

3./Kiểm tra chữ ký

Với một văn bản m cho trước, một cặp (c, s) được gọi là một chữ ký Schnorr hợp lệ nếu thỏa mãn phương trình:

c = H(m, $g^s * y^s$)

Hiện nay có 2 hệ thống tiền điện tử chính: Thẻ thông minh (Smart Card) hay phần mềm. Tuy nhiên chúng có chung các đặc điểm cơ bản sau: Tính an toàn, tính riêng tư, tính độc lập, tính chuyển nhượng, tính phân chia.

Khâu quan trọng nhất của Thương mại điện tử là việc thanh toán, bởi vì mục tiêu cuối cùng của cuộc trao đổi thương mại là người mua nhận được những cái gì cần mua và người bán nhận được số tiền thanh toán.

Thanh toán là một trong những vấn đề phức tạp nhất của Thương mại điện tử. Hoạt động Thương mại điện tử chỉ phát huy được tính ưu việt khi áp dụng được hính thức thanh toán điện tử.

Thanh toán điện tử là việc thanh toán tiền thông qua các thông điệp điện tử (Electronic message) thay cho việc thanh toán bằng tiền Sec hay tiền mặt.Bản chất của mô hình thanh toán Thanh toán điện tử cũng là mô phỏng lại mô hình thanh toán truyền thống, nhưng các thủ tục giao dịch, các thao tác xử lý dữ liệu, quá trính chuyển tiền…tất cả đều được thực hiện thông qua mạng máy tính, được bối bằng các giao thức chuyên dụng.

Chương 2. CÁC KHÁI NIỆM CƠ BẢN VỀ DÙNG TIỀN ĐIỆN TỬ

2.1. KHÁI NIỆM THANH TOÁN ĐIỆN TỬ

Khâu quan trọng nhất của Thương mại điện tử (TMĐT) là việc thanh toán, bởi vì mục tiêu cuối cùng của cuộc trao đổi thương mại là người mua nhận được những cái gì cần mua và người bán nhận được số tiền thanh toán.

Thanh toán là một trong những vấn đề phức tạp nhất của TMĐT. Hoạt động TMĐT chỉ phát huy được tính ưu việt của nó khi áp dụng được hình thức thanh toán điện tử (TTĐT).

TTĐT là việc thanh toán tiền thông qua các thông điệp điện tử (Electronic message) thay cho việc thanh toán bằng tiền Sec hay tiền mặt. Bản chất của mô hình TTĐT cũng là mô phỏng lại mô hình thanh toán truyền thống, nhưng các thủ tục giao dịch, các thao tác xử lý dữ liệu, quá trình chuyển tiền… tất cả đều được thực hiện thông qua mạng máy tính, được nối bằng các giao thức chuyên dụng.

2.1.1. Các mô hình thanh toán điện tử.

Hệ thống TTĐT thực hiện thanh toán cho khách hàng theo một số cách, mà tiền mặt và séc thông thường không thể làm được. Hệ thống thanh toán cũng cung cấp khả năng thanh toán hàng hóa và dịch vụ qua thời gian, bằng cách cho phép người mua trả tiền ngay, trả tiền sau hay trả tiền trước.

2.1.1.1. Mô hình trả tiền sau.

Trong mô hình này, thời điểm tiền mặt được rút ra khỏi tài khoản bên mua để chuyển sang bên bán, xảy ra ngay (pay-now) hoặc sau (pay-later) giao dịch mua bán. Hoạt động của hệ thống dựa trên nguyên tắc Tín dụng (Credit crendental). Nó còn được gọi là ***mô hình mô phỏng Séc*** (Cheque-like model).

2.1.1.2. Mô hình trả tiền trước.

Trong mô hình này, khách hàng liên hệ với ngân hàng (hay công ty môi giới – Broker) để có được chứng từ do ngân hàng phát hành. Chứng từ hay Đồng tiền số này mang dấu ấn của ngân hàng, được đảm bảo bởi ngân hàng và do đó có thể dùng ở bất cứ nơi nào đã có xác lập hệ thống thanh toán với ngân hàng này.

Để đổi lấy chứng từ của ngân hàng, tài khoản của khách hàng bị triết khấu đi tương ứng với giá trị của chứng từ đó. Như vậy, khách hàng đã thực sự trả tiềntrước khi sử dụng chứng từ này để mua hàng và thanh toán.Chứng từ ở đây không phải do khách hàng tạo ra, không phải dành cho một cuộc mua bán cụ thể, mà do ngân hàng phát hành và có thể sử dụng vào mọi mục đích thanh toán. Vì nó có thể sử dụng giống như tiền mặt, do đó mô hình này còn được gọi là ***mô hình mô phỏng tiền mặt*** (Cash-like model).

Khi có người mua hàng tại cửa hàng và thanh toán bằng chứng từ như trên, cửa hàng sẽ kiểm tra tính hợp lệ của chúng, dựa trên những thông tin đặc biệt do ngân hàng tạo ra trên đó.

Cửa hàng có thể chọn một trong hai cách: Hoặc là liên hệ với ngân hàng để chuyển vào tài khoản của mình số tiền trước khi giao hàng (deposit-now), hoặc là chấp nhận và liên hệ chuyển tiền sau vào thời gian thích hợp (deposit-later).

Trường hợp riêng của mô hình mô phỏng tiền mặt là mô hình “tiền điện tử” (Electronic Cash).

Hiện tại hầu hết các dịch vụ mua bán hàng hoá trên mạng đều sử dụng hình thức thanh toán bằng thẻ tín dụng (Credit card). Người sử dụng cần nhập vào các thông tin: tên người sử dụng, mã số thẻ, ngày hết hạn của thẻ. Nhưng vì thẻ tín dụng được dùng phổ biến cho các thanh toán khác nhau, nên những thông tin trên có nhiều người biết. Thực tế hiện nay, các gian lận về thẻ trên Internet chiếm 6-7% tổng số các giao dịch thẻ ở các nước châu Âu, tỷ lệ này ở châu Á là 10%. Tại Việt nam, dịch vụ thẻ tín dụng mới sử dụng cuối năm 1996, nhưng đến nay, tỷ lệ các giao dịch gian lận trên tổng số các giao dịch là hơn 10%.

Trên thế giới hiện nay, nhu cầu về thương mại điện tử rất phổ biến, nhưng các vấn đề hạ tầng trong thanh toán điện tử vẫn chưa được giải quyết tương xứng và đáp ứng được các đòi hỏi đặt ra. Việc nghiên cứu xây dựng các hệ thống thanh toán điện tử để đảm bảo an toàn thông tin trong các dịch vụ thương mại điện tử là một hướng nghiên cứu rất cần thiết hiện nay.

Xây dựng các hệ thống thanh toán điện tử về mặt kỹ thuật chính là ứng dụng các thành tựu của lý thuyết mật mã. Các mô hình thanh toán sử dụng các giao thức mật mã được xây dựng để đảm bảo an toàn cho việc giao dịch thông tin giữa các bên tham gia.

2.2. KHÁI NIỆM TIỀN ĐIỆN TỬ

2.2.1. Khái niệm

Tiền điện tử (E-money, E-currency, Internet money, Digital money, Digital cash) là thuật từ vẫn còn mơ hồ và chưa được định nghĩa đầy đủ. Tuy nhiên có thể hiểu Tiền điện tử là loại tiền trao đổi theo phương pháp "điện tử", liên quan đến mạng máy tính và những hệ thống chứa giá trị ở dạng số (Digital stored value Systems).Tiền điện tử cho phép người dùng có thể thanh toán khi mua hàng, hay sử dụng các dịch vụ, nhờ truyền đi các "dãy số" từ máy tính (hay thiết bị lưu trữ như Smart Card) này tới máy tính khác (Smart Card).

Cũng như dãy số (Serial) trên tiền giấy, dãy số của tiền điện tử là duy nhất. Mỗi "đồng tiền điện tử" được phát hành bởi một tổ chức (ngân hàng) và biểu diễn một lượng tiền thật nào đó.Tiền điện tử có loại ẩn danh (identified e-money), có loại định danh (anonymous identified e-money). Tiền ẩn danh không tiết lộ thông tin định danh của người sử dụng. Tính ẩn danh của tiền điện tử tương tự như tiền mặt thông thường. Tiền điện tử ẩn danh được rút từ một tài khoản, có thể được tiêu xài hay chuyển cho người khác mà không để lạidấuvết.Có nhiều loại tiền ẩn danh, có loại ẩn danh đối với người bán, nhưng không ẩn danh với ngân hàng. Có loại ẩn danh hoàn toàn, ẩn danh với tất cả mọi người.Tiền điện tử định danh tiết lộ thông tin định danh của người dùng. Nó tương tự như thẻ tín dụng, cho phép ngân hàng lưu dấu vết của tiền khi luân chuyển.

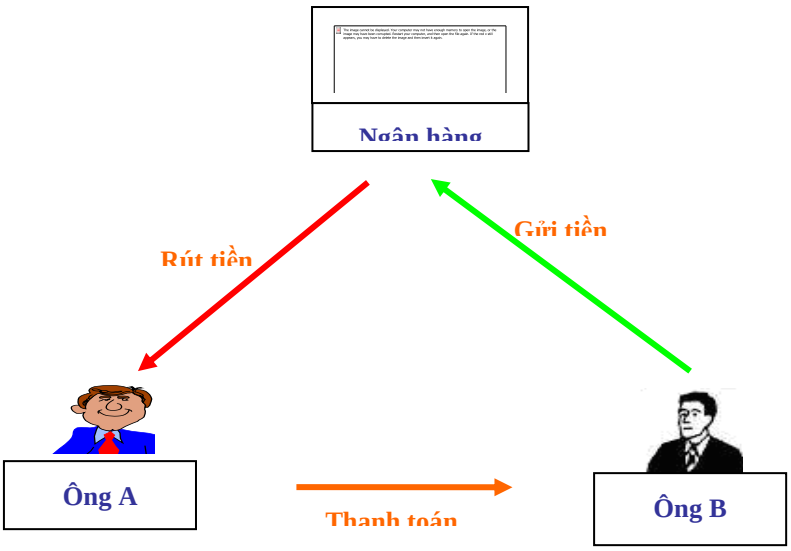
Mỗi loại tiền trên lại chia thành 2 dạng: trực tuyến (online) và không trực tuyến (offline).

Trực tuyến: nghĩa là cần phải tương tác với phía thứ ba để kiểm soát giao dịch.

Không trực tuyến: nghĩa là có thể kiểm soát được giao dịch, mà không cần liên quan trực tiếp đến phía thứ ba (ngân hàng).

Hiện nay có 2 hệ thống tiền điện tử chính: Thẻ thông minh (Smart Card) hay phần mềm. Tuy nhiên chúng có các đặc điểm cơ bản sau: Tính an toàn, tính riêng tư, tính độc lập, tính chuyển nhượng, tính phân chia.chung

2.2.2. Mô hình giao dịch mua bán bằng tiền điện tử



Hình 1: Mô hình giao dịch cơ bản của hệ thống Tiền điện tử.

Mô hình giao dịch mua bán bằng tiền điện tử có 3 giao dịch với 3 đối tượng: Ngân hàng, Người trả tiền A (người mua), Người được trả tiền B (người bán).

* Rút tiền: Ông A chuyển tiền từ tài khoản ở ngân hàng vào 'Túi' của mình ('Túi' có thể là Smart Card hay máy tính) .

* Thanh toán: Ông A chuyển tiền từ 'Túi' của mình đến 'Túi' ông B.

* Gứi tiền: Ông B chuyển tiền nhận được vào tài khoản của mình ở ngân hàng.

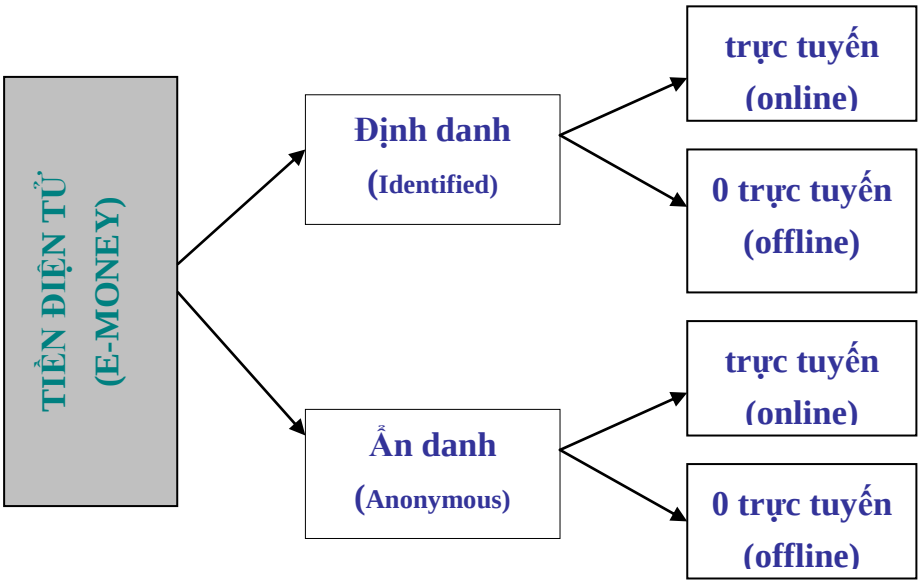
Mô hình này có thể thực hiện bằng 2 cách: trực tuyến, không trực tuyến.

Trực tuyến:

Ông B liên lạc với ngân hàng để kiểm tra tính hợp lệ của đồng tiền trước khi thanh toán và phân phối hàng. Thanh toán và Gửi tiền được tiến hành đồng thời.

Thanh toán trực tuyến cần thiết cho giao dịch có giá trị lớn. Hệ thống yêu cầu phải liên lạc với ngân hàng trong suốt mỗi lần giao dịch, vì thế chi phí nhiều hơn (tiền và thời gian).

Không trực tuyến: ông B liên lạc với ngân hàng để kiểm tra tính hợp lệ của đồng tiền được tiến hành sau quá trình thanh toán. Nó phù hợp cho những giao dịch có giá trị thấp.



Hình 2: Mô hình phương thức thanh toán

2.2.3. Cấu trúc của Tiền điện tử

Với mỗi hệ thống thanh toán điện tử, tiền điện tử có có cấu trúc và định dạng khác nhau nhưng đều bao gồm các thông tin chính như sau.

Số sê-ri của đồng tiền: Giống như tiền mặt, số sê-ri được dùng để phânbiệt các đồng tiền khác nhau. Mỗi đồng tiền điện tử sẽ có một số sê-ri duy nhất. Tuy nhiên, khác với tiền mặt, số sê-ri trên tiền điện tử thường là một dãy số được sinh ngẫu nhiên. Điều này có liên quan tới tính ẩn danh của người sử dụng.

Giá trị của đồng tiền: Mỗi đồng tiền điện tử sẽ có giá trị tương đương với một lượng tiền nào đó. Trong tiền mặt thông thường, mỗi tờ tiền có một giá trị nhất định (1$, 10$,…), trong tiền điện tử, giá trị này có thể là một con số bất kỳ (9$, 17$,…).

Hạn định của đồng tiền: Để đảm bảo tính an toàn của đồng tiền và tính hiệu quả của hệ thống, các hệ thống thường giới hạn ngày hết hạn của đồng tiền. Một đồng tiền điện tử sau khi phát hành sẽ phải gửi lại ngân hàng trước thời điểm hết hạn.

Các thông tin khác: Đây là các thông tin thêm nhằm phục vụ cho mục đích đảm bảo an toàn và tính tin cậy của đồng tiền điện tử, ngăn chặn việc giả mạo tiền điện tử và phát hiện các vi phạm (nếu có). Trong nhiều hệ thống, các thông tin này giúp truy vết định danh người sử dụng có hành vi gian lận trong thanh toán tiền điện tử.

Các thông tin trên tiền điện tử được ngân hàng ký bằng khóa bí mật của mình. Bất kỳ người sử dụng nào cũng có thể kiểm tra tính hợp lệ của đồng tiền bằng cách sử dụng khóa công khai của ngân hàng.

2.2.4. Tính chất của tiền điện tử

Tiền điện tử cũng có một số đặc điểm tương tự như tiền giấy: dùng để biểu diễn một lượng tiền nào đó, có thể chuyển nhượng được, không để lại dấu vết, có tính

ẩn danh, có thể mang đi mang lại và đặc biệt có thể đổi được.

2.2.4.1. Tính an toàn (Security)

* Đảm bảo đồng tiền điện tử không bị sao chép, không bị sử dụng lại.

* Sự giả mạo (forgery).

Các gian lận thường gặp trong hệ thống thanh toán là sự giả mạo. Tương tự như tiền giấy, có hai loại giả mạo đối với tiền điện tử.

+ Giả mạo đồng tiền: tạo ra đồng tiền giả giống như thật, nhưng không có

xác nhận rút tiền của ngân hàng.

+ Tiêu một đồng tiền nhiều lần: là sử dụng cùng một đồng tiền nhiều lần (thuậtngữ tương đương như double spending, hay multiple spending, hay repeat spending)

2.2.4.2. Tính xác thực

Do luôn có sự giả mạo, nên ta cần phải xác lập được các mức khác nhau về cách đánh giá tính xác thực.

+ Nhận dạng người dùng: Người dùng cần phải biết mình đang giao dịch với ai.

+ Xác thực tính toàn vẹn thông điệp: đảm bảo bản copy của thông điệp hoàn toàn giống bản ban đầu.

2.2.4.3. Tính riêng tư (Privacy)

Chưa thể định nghĩa một cách rõ ràng tính chất này của Tiền điện tử. Đối với một số người, tính riêng tư có nghĩa là sự bảo vệ chống lại "eavesdropping". Đối với một số người khác như David Chaum, "tính riêng tư" có nghĩa là trong quá trình thanh toán, người trả tiền phải được ẩn danh, không để lại dấu vết, ngân hàng không nói được tiền giao dịch là của ai.

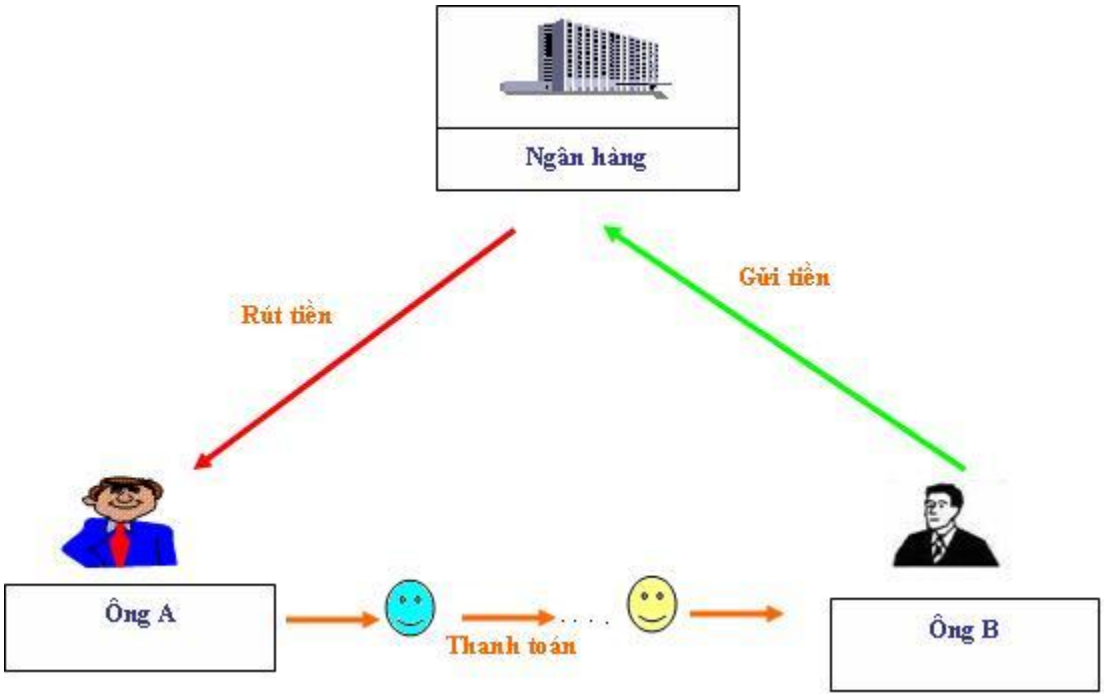
Tính chất này nhằm bảo vệ người dùng, khó có thể truy vết, chấp nối mối quan hệ giữa người dùng với các giao dịch hay chi tiêu mà người đó thực hiện. Tính chất này cũng có thể thấy rõ trong các giao dịch bằng tiền mặt. Sau khi thanh toán, việc chứng minh người nào đã sở hữu số tiền đó trước đây là rất khó.

2.2.4.4. Tính độc lập (Portability)

Tính chất này có nghĩa là sự an toàn của Tiền điện tử không phụ thuộc vào vị trí địa lý. Tiền có thể được chuyển qua mạng máy tính hoặc lưu trữ vào các thiết bị nhớ khác nhau.

2.2.4.5. Tính chuyển nhượng được (Ttransferrability)

Người dùng Tiền điện tử có thể chuyển giao quyền sở hữu đồng tiền điện tử cho nhau. Tính chuyển nhượng được là một tính chất rất quan trọng cho việc tiêu tiền điện tử, thực sự giống với tiêu tiền mặt thông thường.



Hình 3: Mô hình giao dịch có tính chuyển nhượng

Tuy vậy, có một số vấn đề nảy sinh mà hệ thống vẫn cần phải giải quyết:

Kích thước dữ liệu tăng lên sau mỗi lần chuyển nhượng. Vì vậy, cần giới hạn số lần chuyển nhượng tối đa cho phép.Phát hiện giả mạo và tiêu một đồng tiền nhiều lần có thể quá trễ, khi đồng tiền đã được chuyển nhượng nhiều lần.Người dùng có thể nhận ra đồng tiền của mình, nếu nó lại xuất hiện trong một lần giao dịch khác.

2.2.4.6. Tính phân chia được (Divisibility)

Người dùng có thể phân chia đồng tiền của mình thành những mảnh có giá trị nhỏ hơn, với điều kiện tổng giá trị các mảnh nhỏ bằng giá trị đồng tiền ban đầu. Tiền điện tử thực chất là một dãy số bị mã hóa, nên không phải hệ thống nào cũng thực hiện được việc chia dãy số này thành các đồng tiền có giá trị nhỏ hơn

2.3. CÁC GIAI ĐOẠN TRONG DÙNG TIỀN ĐIỆN TỬ

Giai đoạn 1 **:** **RÚT TIỀN TỪ NGÂN HÀNG**

+ Người Rút Tiền gửi Hồ sơ tới Ngân hàng Yêu cầu Rút Tiền.

+ Ngân hàng thẩm định Hồ sơ Yêu cầu Rút Tiền.

+ Nếu Yêu cầu Rút Tiền hợp lý, Ngân hàng và Người Rút Tiền thực hiện Rút Tiền Ẩn danh.

Giai đoạn 2:**THANH TOÁN TIỀN**

+ Người Rút tiền thanh toán (chuyển tiền) cho Người nhận tiền.

+ Người nhận tiền Kiểm tra Tính hợp pháp của Đồng tiền.

Nếu Đồng tiền hợp pháp, họ sẽ nhận tiền.

Giai đoạn 3:**GỬI TIỀN VÀO NGÂN HÀNG**

+Người nhận tiền Gửi tiền vào Ngân hàng.

+Ngân hàng Kiểm tra Tính hợp pháp của Đồng tiền.

Nếu Đồng tiền hợp pháp, Ngân hàng sẽ nhận tiền, và chuyển vào tài khoản của Người nhận tiền.

2.3.1 Một số bài toán trong dùng tiền điện tử

***Giai đoạn 1:*RÚT TIỀN TỪ NGÂN HÀNG**

+ Bài toán bảo vệ Hồ sơ Yêu cầu Rút Tiền.

+ Bài toán Thẩm định Hồ sơ Yêu cầu Rút Tiền.

+ Bài toán thực hiện Ẩn danh Đồng tiền.

+ Bài toán Phòng tránh: Khai man giá trị đồng tiền

+ Bài toán bảo vệ Đồng tiền trên đường truyền tin.

***Giai đoạn 2:*THANH TOÁN TIỀN (CHUYỂN TIỀN)**

+ Bài toán bảo vệ Đồng tiền trên đường truyền tin.

+ Bài toán Kiểm tra Tính hợp pháp của Đồng tiền.

Đồng tiền có chữ ký của Ngân hàng ?

Đồng tiền có chữ ký của Người chuyển tiền ?

+ Bài toán Phòng tránh: Tiêu một đồng tiền nhiều lần.

***Giai đoạn 3*: GỬI TIỀN VÀO NGÂN HÀNG**

+ Bài toán bảo vệ Đồng tiền trên đường truyền tin.

+ Bài toán Kiểm tra Tính hợp pháp của Đồng tiền.

Đồng tiền có chữ ký của Ngân hàng ?

Đồng tiền đã tiêu lần nào chưa ?

Chương 3:MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG GIAO DỊCH THANH TOÁN TIỀN ĐIỆN TỬ

3.1. BÀI TOÁN BẢO VỆ ĐỒNG TIỀN TRÊN ĐƯƠNG TRUYỀN

3.1.1. Giới thiệu bài toán.

Chúng ta thấy rằng trong cả 3 giao dịch sử dụng Tiền điện tử, đều cần giải quyết Bài toán " Bảo vệ đồng tiền trên đường truyền".

Khái niệm " Bảo vệ Đồng tiền" là rộng , trong luận văn này, chúng ta hiểu là "Bảo vệ đồng tiền", để ngoài ông A, ông B, Ngân hàng, không ai có thể nhìn thấy đồng tiền, hay sửa nội dung Đồng tiền.

3.1.2.Giải pháp

* Những người không được phép thỳ không thể nhìn thấy nội dung Đồng tiền. Hiện nay có nhiều phương pháp để giải quyết vấn đề trên, nhưng cách thông dụng nhât là dùng phương pháp Mã hóa , để mã hóa Đồng tiền.

* Những người không được phép thỳ không thể sửa nội dung Đồng tiền.

Hiện nay có nhiều phương pháp để giải quyết vấn đề trên, nhưng cách thông dụng nhất là dùng phương pháp Mã hóa , để mã hóa Đồng tiền.

Người không được phép thỳ không thể sửa nội dung Đồng tiền, vì họ không hiểu nội dung thông tin.

Có thể dùng phương pháp Ký số , để Ký lên Đồng tiền. Sau đó có thể kiểm tra Tính toàn vẹn của Đồng tiền (Kiểm tra đồng tiền có bị sửa đổi không?).

3.2.BÀI TOÁN PHÒNG TRÁNH TIÊU MỘT ĐỒNG TIỀN NHIỀU LẦN

3.2.1. Giới thiệu bài toán

Ông A sau khi nhận được đồng tiền điện tử của Ngân hàng có dạng số hóa, nên dễ dàng tạo bản sao từ bản gốc, hoặc sử dụng đồng tiền đó cho nhiều giao dịch khác nhau. Chúng ta không thể phân biệt được giữa đồng tiền "gốc" và đồng tiền "sao". Kẻ gian có thể tiêu xài đồng tiền "sao" này nhiều lần nếu không bị phát hiện. Bài toán giải quyết vần đề này là bài toán đảm bảo mỗi một đồng tiền điện tử chỉ

được sử dụng cho một giao dịch tại một thời điểm, nếu có gian lận thì xác định danh tính người gian lận.

3.2.2.Giải pháp

Làm thế nào để đảm bảo tính ẩn danh người dùng, mà vẫn truy vết được định danh khi họ vi phạm? Giải pháp là dùng "chữ ký mù có điều kiện" (conditional blind signature), còn gọi là chữ ký mù một phần (partial blind signature).

Chữ ký mù có điều kiện đảm bảo:Nếu không vi phạm xảy ra, nó giống hệt chữ ký mù , tức là đảm bảo tính ẩn danh cho người dùng. Nếu có vi phạm xảy ra, ngân hàng có thể kết hợp với nhà cung cấp để truy vết định danh người đã thực hiện hành vi gian lận.Ý tưởng của chữ ký mù có điều kiện:

Khi người dùng A thực hiện giao thức rút tiền, A truyền cho ngân hàng một số thông tin. Tương tự, khi thực hiện giao thức trả tiền, A gửi cho nhà cung cấp B thêm một số thông tin. Chỉ riêng thông tin mà A cung cấp cho ngân hàng hoặc B, thì không thể suy ra định danh của A, nhưng khi có vi phạm, ngân hàng và B có thể kết hợp với nhau, dưới sự giám sát của pháp luật, để truy vết định danh của A.

Ví dụ, trong trường hợp Alice tiêu xài một đồng tiền hai lần, thì phải cung cấp cho ngân hàng:

Lần 1: c và r_1, r_2, r_3

Lần 2:c' và r'_1, r'_2, r'_3

Với : $r_1 = x_1 + c\,x_2 \mod q$, $r_2 = x_2 + c\,y_2 \mod q$, $r_3 = x_3 + c\,z_2 \mod q$

$r'_1 = x_1 + c'\,x_2 \mod q$, $r'_2 = x_2 + c'\,y_2 \mod q$, $r'_3 = x_3 + c'\,z_2 \mod q$

Từ 2 bộ 3 này ngân hàng sẽ tìm ra được định danh của kẻ gian lận.

Bởi vì từ:

$$\mathbf{AB}^{c} = g_1^{r1}\, g_2^{r2}\, d^{r3}\ ;\ \mathbf{AB}^{c'} = g_1^{r'1}\, g_2^{r'2}\, d^{r'3}$$

Suy ra:

$$\mathbf{A} = g_1^{(c'r_1 - cr_1')/(c'-c)}\ g_2^{(c'r_2 - cr_2')/(c'-c)}\ g_3^{(c'r_3 - cr_3')/(c'-c)}$$

$$\mathrm{B} = g_1^{(r_1 - r_1')/(c'-c)}\ g_2^{(r_2 - r_2')/(c'-c)}\ g_3^{(r_3 - r_3')/(c'-c)}$$

Mà:

A = $g_1^{x_1}\ g_2^{y_2}\ d^{z_1}$

B = $g_1^{x_2}\ g_2^{y_2}\ d^{z_2}$

$\frac{c'r_1 - cr'_1}{(c'-c)} = x_1 \bmod q$ $\frac{c'r_2 - cr'_2}{(c'-c)} = y_2 \bmod q$

$\frac{c'r_3 - cr'_3}{(c'-c)} = z_3 \bmod q$

$\frac{r_1 - r'_1}{(c'-c)} = x_2 \bmod q$ $\frac{r_3 - r'_3}{(c-c')} = z_2 \bmod q$

$\frac{r_2 - r'_2}{(c-c')} = y_2 \bmod q$

Từ công thức, Ngân hàng tính :

$u_1 s = x_1 + x_2$ $u_2 s = y_1 + y_2$ $s = z_1 + z_2$

Tiến hành thay $x_1, y_1, z_1, x_2, y_2, z_2$ theo kết quả trên sẽ được:

$$u_1 s = \frac{c'r_1 - c r_1'}{c'-c} + \frac{r_1 - r_1'}{c-c'} \bmod q$$

$$u_2 s = \frac{c'r_2 - c r_2'}{c'-c} + \frac{r_2 - r_2'}{c-c'} \bmod q$$

$$s = \frac{c'r_3 - c r_3'}{c'-c} + \frac{r_3 - r_3'}{c-c'} \bmod q$$

$$u_1 = \frac{r_1(c'+1) - r_1'(c+1)}{r_3(c'-1) - r'_3(c'+1)} \bmod q$$

$$u_1 = \frac{r_2(c'+1) - r_2'(c+1)}{r_3(c'-1) - r'_3(c'+1)} \bmod q$$

Từ u_1 và u_2 tính được **I** theo công thức **I=** $g_1^{u_1}\ g_2^{u_2}$ **,** Ngân hàng so sánh giá trị **I** trong cơ sở dữ liệu đã lưu trước đó và tìm ra định danh của kẻ gian lận.

3.2BÀI TOÁN KIỂM TRA TÍNH HỢP PHÁP CỦA ĐỒNG TIỀN.

3.2.1.Giới thiệu bài toán

Kiểm tra tính hợp pháp của Đồng tiền là Kiểm tra tính đúng đắn của Nguồn gốc Đồng tiền. Tuy nhiên trong mỗi Giao dịch, người ta dùng phương pháp Kiểm tra khác nhau. Ví dụ:

*Trong Giao dịch rút tiền:

Khi ông A nhận được Đồng tiền từ Ngân hàng , để Kiểm tra tính hợp pháp của Đồng tiền, Ông A phải kiểm tra 2 vấn đề:

+Vấn đề 1: Đồng tiền có phải được gửi từ Ngân hàng hay không?

+Vấn đề 2: Đồng tiền có được quản lý bởi Ngân hàng hay không?

*Trong giao dịch Thanh toán :

Khi ông B nhận được Đồng tiền từ ông A, để kiểm tra tính hợp pháp của Đồng tiền , Ông B phải kiểm tra 2 vấn đề:

+Vấn đề 1: Đồng tiên có phải được gửi từ ông A hay người khác

+Vấn đề 2:Đồng tiền có được quản lý bởi Ngân hàng hay không?

*Trong giao dịch Gửi tiền:

Khi ông B gửi Đồng tiền đến Ngân hàng, để Kiểm tra tính hợp pháp của Đồng tiền, ông B phải kiểm tra 3 vấn đề:

+Vấn đề 1: Đồng tiền có phải được gửi từ ông B hay người khác?

+Vấn đề 2: Đồng tiền có phải được quản lý bởi Ngân hàng hay không?

+Vấn đề 3: Đồng tiền đã được tiêu (sử dụng trong thanh toán) lần nào chưa?

3.2.2.Giải pháp

Các vấn đề của cả 3 Giao dịch trên có thể qui về 3 vấn đề sau:

+Vấn đề 1: Đồng tiền có phải được gửi từ ông A, hay ông B, hay Ngân hàng?

+Vấn đề 2: Đồng tiền có được quản lí bởi Ngân hàng hay không?

+Vấn đề 3: Đồng tiền đã được tiêu (sử dụng trong thanh toán) lần nào chưa?

***Giải quyết Vấn đề 1:**

Người nhận phải kiểm tra chữ ký là của ai, thì Đồng tiền được gửi từ người đó.

***Giải quyết vấn đề 2:**

Người nhận phải kiểm tra chữ ký là của Ngân hàng hay không?

***Giải quyết vấn đề 3:**

Đồng tiền đã được tiêu (sử dụng) lần nào chưa?

Cách giải quyết chung như sau:

+ Khi Đồng tiền được gửi vào Ngân hàng (tức là đã được tiêu) , thì Ngân hàng ghi lại định danh của Đồng tiền này. Sau đó kiểm tra có trùng định danh với Đồng tiền gửi vào trước đó. Nếu 2 định danh trùng nhau, thì kết luận Đồng tiền mới được tiêu lần thứ 2. Kỹ thuật kiểm tra của lược đồ BRAND

Khi Alice muốn mua hàng hay sử dụng dịch vụ của Bob, trước tiên Alice cần phải gửi tiền cho Bob. Quá trình thanh toán được thực hiện theo những bước sau:

Alice gửi tiền (**A**, **B**, Sign (**A**,**B**)) đến Bob.

A = $g_1^{x_1}\ g_2^{y_1}\ d^{z_1}$ **; B** = m' / **A** = $g_1^{x_1}\ g_2^{y_1}\ d^{z_1}$

Sign(**A, B)** = (z', a', b', r')

Đầu tiên, Bob kiểm tra xem **AB** ≠ 1 hay không.

Nếu **AB** = 1 có nghĩa :

$$(g_1^{x_1}\ g_2^{y_1}\ d^{z_1})(g_1^{x_2} g_2^{y_2} d^{z_2}) = 1$$

$$\Rightarrow \quad g_1^{x_1+x_2} g_2^{y_1+y_2} d^{z_1+z_2} = g_1^{u_1 s} g_2^{u_2 s} d^{s} = 1$$

$$\Rightarrow \quad s = 0$$

Điều này là không được phép, vì như vậy Ngân hàng không xác định được u1,u2 trong trường hợp có hành vi "double-spending".

*Sau đó, Bob kiểm tra chữ ký của Ngân hàng sign(**A, B)** có hợp lệ không.

Nếu đúng, Bob thử thách Alice bằng cách gửi $c \in Z'_q$ (nhưng phải đảm bảo c là duy nhất trong mỗi lần thanh toán).

Bob tính c như sau:

c = H0 (**A, B,** Ib , date/time), với I là định danh của Bob, date time là nhãn thời gian của giao dịch, H0 là hàm băm.

Alice phản hồi với:

r1 = x1 + cx2 mod q

r2 = x2 + cy2 mod q

r3 = x3 + cz2 mod q

Bob kiểm tra, nếu $g_1^{r_1} g_2^{r_2} g_2^{r_3} = \mathbf{AB}^c$ thì chấp nhận thanh toán vì:

$$g_1^{r_1} g_2^{r_2} g_2^{r_3} = g_1^{x_1+cx_2}\ g_2^{y_1+cy_2}\ g_3^{z_1+cz_2} = (g_1^{x_1}\ g_2^{y_1}\ g_3^{z_1}) = (g_1^{cx_2}\ g_2^{cy_2}\ g_3^{cz_2}) = \mathbf{AB}^c$$

Alice		**Bob**

	$\xrightarrow{\mathbf{A},\mathbf{B},sign(\mathbf{A},\mathbf{B})}$	
		AB $\neq 1$? Kiểm tra sign(**A, B)** $c \in \mathbf{Z}^*_{\mathbf{q}}$
	$\xleftarrow{c}$	
$r_1 = x_1 + cx_2 \bmod q$ $r_2 = x_2 + cy_2 \bmod q$ $r_3 = x_3 + cz_2 \bmod q$		
	$\xrightarrow{r_1,r_2,r_3}$	
		$g_1^{r_1}\ g_2^{r_2}\ g_2^{r_3} = AB^c$? Nếu đúng Bob chấp nhận thanh toán.

Chương 4. THỬ NGHIỆM ỨNG DỤNG

4.1.VẤN ĐỀ SỬ DỤNG TIỀN ĐIỆN TỬ TẠI VIỆT NAM

4.1.1.Thẻ phone card

Ở việt nam, hệ thống tiền điện tử đầu tiên được triển khai đưa vào sử dụng là thẻ điện thoại công cộng, xuất hiện từ những năm 90, và được sử dụng khá rộng rãi trước trào lưu sử dụng điện thoại di động, và đây cũng chính là hình thức đơn giản nhất của tiền điện tử.

Về cấu trúc, đây là một thiết bị lưu trữ sử dụng một chíp nhớ để ghi lại thông tin về giá trị của thẻ, người sử dụng mua thẻ ở các đại lý, sau đó sử dụng thẻ bằng cách cắm thẻ vào thiết bị đọc thẻ gắn liền với điện thoại, khi hết tiền trong thẻ, người sử dụng phải mua thẻ mới nếu có nhu cầu sử dụng tiếp. Đây là một trong những hạn chế lớn nhất của thẻ điện thoại dùng chíp nhớ vì nó không có khả năng tái sử dụng (nạp thêm tiền vào thẻ), mặc dù vậy khi ra đời nó rất nhanh chóng được xã hội đón nhận.

Hiện nay thì hệ thống này ở Việt Nam gần như đã tê liệt do không còn người sử dụng. Chỉ còn lại một số ít tại các thành phố lớn hoặc trung tâm các dịch vụ chủ yếu phục vụ khách nước ngoài. Còn người dân thì chuyển qua sử dụng thiết bị di động vì mức cước và thiết bị đầu cuối cũng như các sản phẩm gia tăng là vô cùng hấp dẫn.

4.1.2. Thẻ Flexicard

Ngày 13 tháng 10 năm 2009, PG Bank (Ngân hàng dầu khí) cùng với công ty mẹ của mình là Petrolimex đã phát hành loại hình thẻ mới là Flexicard với nhiều tính năng tiện dụng và hiện đại như : Prepaid (trả trước) và Debit (ghi nợ) được sử dụng chủ yếu trong thanh toán , đặc biệt là việc thanh toán xăng dầu của các khách hàng cá nhân. Đây được đánh giá là một trong những bước đi đầu tiên về việc ứng dụng Tiền điện tử vào thực tế tại Việt Nam.

FlexiCard trả trước (prepaid): Là phương tiện thanh toán không dùng tiền mặt dành cho Chủ thẻ để thanh toán hàng hóa dịch vụ tại nhà hàng, siêu thị, đặc biệt là thanh toán xăng dầu tại hơn 2.000 cửa hàng xăng dầu của Petrolimex trên toàn quốc. Chủ thẻ hoàn toàn có thể kiểm soát được kế hoạch chi tiêu bởi vì tính năng trả

trước của Flexicard phát hành dựa trên cơ sở số tiền mà chủ thẻ đã mua hay nạp vào thẻ. Flexicard trả trước gồm 2 loại:

*Flexicard trả trước vô danh có thể mua ngay tại cửa hàng xăng dầu, điểm chấp nhận thẻ của PG Bank mà không cần đăng ký thông tin, tuy nhiên thẻ vô danh không được nạp tiền vào thẻ.

*Flexicard trả trước định danh ; khách hàng không cần mở tài khoản tại ngân hàng nhưng phải đăng ký thông tin và sẽ được nạp tiền vào thẻ cũng như tham gia các chương trình khuyến mại khi thanh toán xăng dầu tại tất cả các cửa hàng xăng dầu của Petrolimex.

FlexiCard ghi nợ nội địa (debit): Là phương tiện thanh toán không dùng tiền mặt tiện lợi và an toàn do PG Bank phát hành trên cơ sở tài khoản tiền gửi không định kì hạn của khách hàng mở tại ngân hàng. Flexicard tích hợp công nghệ thẻ kép (thẻ từ và thẻ chip), Flexicard ghi nợ cho phép chủ thẻ thực hiện rất nhiều tiện ích như Rút tiền mặt tại ATM của PG Bank và hệ thống ATM trong liên minh Banknẻtvn trên toàn quốc ; Nhận lương, thu nhập qua tài khoản thẻ Flexicard; Thanh toán hàng hóa dịch vụ tại hàng nghìn đơn vị chấp nhận thẻ tại các nhà hàng, khách sạn, siêu thị, rạp chiếu phim, các điểm vui chơi giải trí…; Thanh toán chi phí mua xăng dầu tại hơn 2.000 điểm phân phối xăng dầu của Petrolimex trên toàn quốc; Vấn tin số dư tài khoản; Chuyển khoản dễ dàng hơn và đơn giản từ tài khoản thẻ ghi nợ sang tài khoản thẻ ghi nợ; Từ tài khoản thẻ ghi nợ sang tài khoản thẻ trả trước; In sao kê giao dịch…

4.1.3. Tiền điện tử ở Việt Nam, cơ hội và thách thức

Hiện tại, khái niệm Tiền điện tử vẫn là một khái niệm khá mới mẻ tại Việt Nam. Một số doanh nghiệp đã nghiên cứu và đưa ra thị trường loại thẻ thanh toán đa mục đích để chơi game, sử dụng Internet hay mua hàng hóa trên website của

doanh nghiệp. Một vài ngân hàng cũng đã bắt đầu đẩy mạnh cung ứng các sản phẩm, dịch vụ ngân hàng qua kênh điện tử như Internet Banking, Mobile Banking…

Một thực tế không thể phủ nhận là cơ sở hạ tầng kĩ thuật của nước ta còn ở mức thấp, trình độ dân trí của nước ta cũng chưa cao. Nhưng mặt khác, chúng ta rất nhanh chóng tiếp thu được bề nổi của công nghệ. Chúng ta không chế tạo ra các thiết bị thanh toán điện tử, cơ chế vận hàng q uản lý của các ngân hàng cũng chưa thật sự tối ưu, nhưng nhiều hình thức áp dụng đơn giản của Tiền điện tử vẫn đang phát triển.

Cùng với đó, Tiền điện tử đang dần tìm cho mình vị trí trong thương mại, không chỉ là giới hạn trong một quốc gia mà giờ đã mở ra phạm vi toàn cầu. Có cơ sở đúng đắn để tin rằng trong tương lai gần Tiền điện tử sẽ thống trị hệ thống thương mại trên toàn thế giới, đăc biệt là với tốc độ phát triển của công nghệ thông tin hiện nay. Tiền điện tử có những tính năng ưu việt hơn cả tiền giấy. Nhưng thực tế hiện nay, không nhiều quốc gia trên thế giới đã thực sự đưa được Tiền điện tử vào ứng dụng khắp trong nền kinh tế của mình.

Các báo cáo, thống kê gần đây của Ngân hàng Nhà nước phần nào chứng thực được rằng ở Việt Nam Tiền điện tử có chỗ đứng và đang phát triển. Con đường phát triển của nó là rông mở, nhưng nó sẽ phát triển đều đặn theo thời gian, nhưng đa phần chỉ là trong các tình huống nhỏ lẻ, chưa có những bước đại nhảy vọt. Và nguồn gốc sâu xa vẫn lài là do sự yếu kém của cơ sở hạ tầng, hệ thống tài chính, cơ chế quản lý và trình độ sử dụng công nghệ còn hạn chế của dân ta.

4.1.4. Các vấn đề tồn tại ảnh hưởng đến sự phát triển của Tiền điện tử ở Việt Nam

***** Thói quen sử dụng tiền mặt của người dân, tính thuận tiện trong thanh toán đối với các giao dịch hàng ngày, lợi ích của tiền điện tử mang lại đối với người dân chưa đủ lớn…

* Cơ sở hạ tầng đáp ứng chưa phát triển đồng đều, dẫn đến nhiều trường hợp giao dịch điện tử nhưng thanh toán trực tiếp, do các điểm chấp nhận thanh toán còn quá ít, các dịch vụ đi kèm còn hạn chế.

* Các lo ngại về tính bảo mật, riêng tư do phụ thuộc phần lớn vào hệ thống Công nghệ thông tin. Do kinh nghiệm quản lí , năng lực triển khai hệ thống Tiền điện tử còn nhỏ lẻ, chưa hoàn thiện.

* Hành lang pháp lý đối với vấn đề này còn bỏ ngỏ, tuy rằng có điều chỉnh nhưng chưa bám sát với thực tế. Việc phòng chống tội phạm công nghệ cao cần sự phối hợp không chỉ của nhiều ngành, mà còn của nhiều quốc gia khác nhau.

4.1.5.Các biện pháp cở bản và trước mắt

* Tăng cường sử dụng hệ thống bán hàng tự động và thanh toán qua thẻ thông minh tại các trung tâm dịch vụ, siêu thị,…Đầu tư mở rộng hạ tầng cơ sở, mở rộng mạng lưới thanh toán. Tuyên truyền, quảng bá thông tin thường xuyên, chi tiết đến khách hàng về các dịch vụ.

* Các tổ chức cung cấp dịch vụ Tiền điện tử phải liên tục nâng cấp khả năng bảo mật cả về kỹ thuật lần nghiệp vụ. Thường xuyên đầu tư quan tâm đến vấn đề bảo mật, nâng cấp, khắc phục kịp thời các lỗ hổng để giảm thiểu rủi ro. Giải thích hướng dẫn cho khách hàng về quy trình thực hiện cũng như các biện pháp nhằm bảo vệ thông tin.

* Hoàn thiện hệ thống văn bản pháp lí, các luật về tội phạm công nghệ cao. Đồng thời tuyên truyền, giáo dục, phổ biến pháp luật trong lĩnh vực Công nghệ tới nhân dân.

4.2.THỬ NGHIỆM CHƯƠNG TRÌNH BẢO VỆ TIỀN ĐIỆN TỬ

4.2.1. Mô tả bài toán nghiệp vụ

Hệ thống ngân hàng và người dùng đều thực hiện các giao dịch trên mạng Internet. Người dùng (ví dụ như Alice), Bob, các nhà cung cấp) lưu đồng tiền điện tử trên máy tính cá nhân, thẻ thông minh,… để thực hiện các giao dịch.

Hệ thống thanh toán tiền điện tử dựa trên lược đồ Brand cần đạt được các yêu cầu sau: Khách hàng khởi tạo tài khoản, Khách hàng chứng minh mình là người sở hữu hợp pháp tài khoản, rút tiền, thanh toán tiền, gửi tiền, Ngân hàng phát hiện các gian lận (nếu có).

Khởi tạo tài khoản (Open account).

Người dùng (Alice) muốn khởi tạo tài khoản tại một Ngân hàng. Alice tạo ra hai số ngẫu nhiên u_1 và u_2 , sau đó tính giá trị $I=g_1^{u_1}g_2^{u_2}$, gửi đến Ngân hàng. Ngân hàng lưu lại giá trị I trong CSDL.

Chứng minh đại diện tài khoản (Authenticate).

Khi rút tiền, Alice cần chứng minh với Ngân hàng về sở hữu hợp pháp tài khoản. Alice phải chứng minh cho Ngân hàng là mình biết giá trị u_1 và u_2 mà không cần tiết lộ hai giá trị này.

Rút tiền (Withdraw Money).

Sau khi xác thực được chấp nhận, Ngân hàng gửi cho Alice lượng tiền mà Alice yêu cầu. Ngân hàng trừ lượng tiền tương ứng vào tài khoản của Alice. Alice kiểm tra tiền từ Ngân hàng, nếu thấy hợp lệ , thì chấp nhận tiền điện tử này.

Thanh toán (Payment Money).

Khi Alice muốn mua hàng hay sử dụng dịch vụ của Bob, Alice phải gửi tiền cho Bob. Bob kiểm tra đồng tiền, nếu thấy hợp lệ thì chấp nhận.

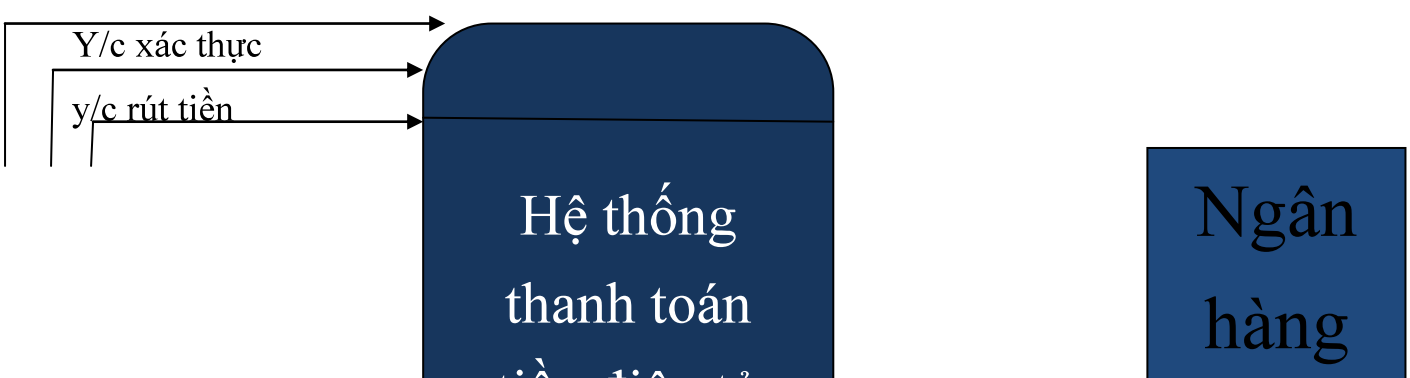
Gửi tiền (Deposit Money).

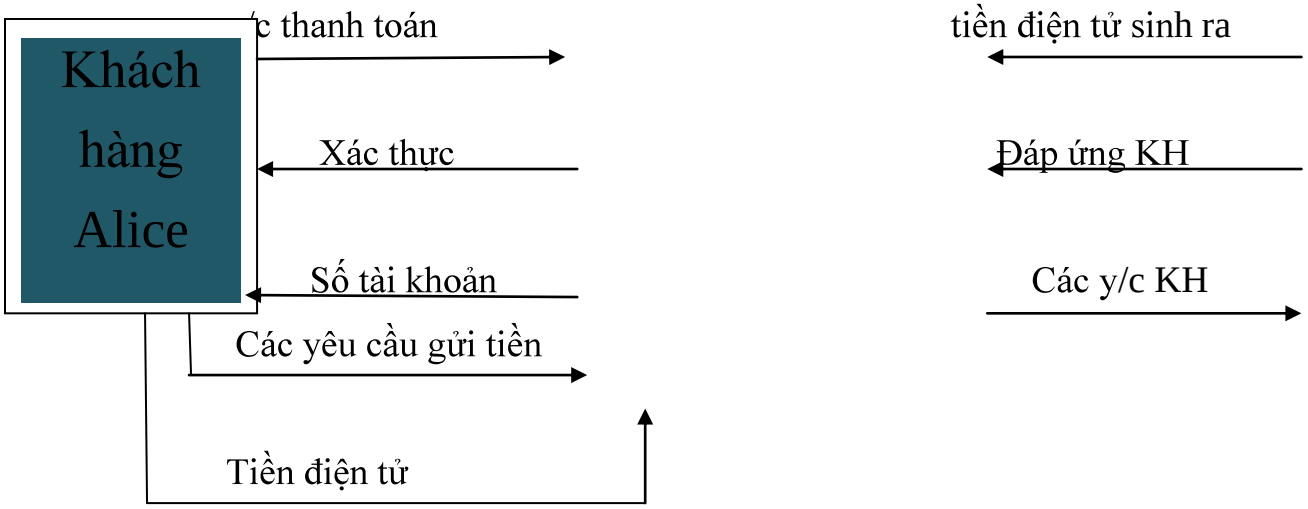
Bob gửi tiền (do Alice trả) đến Ngân hàng và yêu cầu Ngân hàng kiểm tra tính hợp lệ. Ngân hàng kiểm tra chữ kí của mình trên đồng tiền, kiểm tra xem đồng tiền có bị tiêu xài trước đây hay chưa. Đồng thời Bob cũng thử thách lại sự trung thực của Alice. Nếu tất cả đều hợp lệ, Ngân hàng cộng thêm tiền vào tài khoản của Bob.

Phát hiện "double-spending".

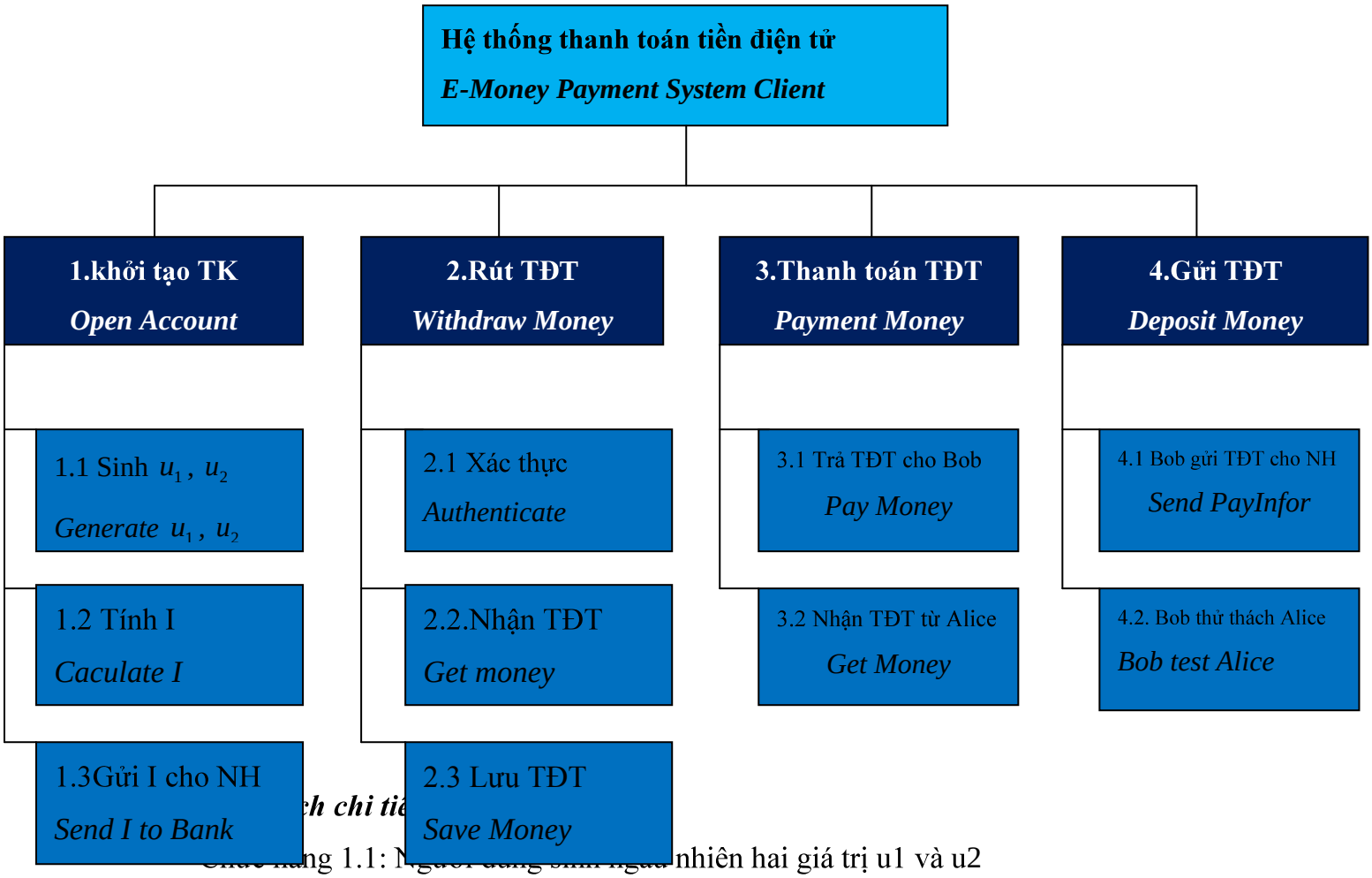
Nếu phát hiện Alice gian lận, Ngân hàng yêu cầu Alice cung cấp một số thông tin cần thiết, kiểm tra định danh I lưu trong CSDL, để truy vết ra Alice.

4.2.2.Biểu đồ ngữ cảnh





4.2.3.Biểu đồ phân rã chức năng.



ch chi tiế

ng 1.1: N nhiên hai giá trị u1 và u2

Chức năng 1.2: Người dùng tính giá trị $I = g_1^{u_1} g_2^{u_2}$

Chức năng1.3 : Người dùng gửi I tới Ngân hàng.

Chức năng 2.1: Ngân hàng yêu cầu người dùng chứng minh về sở hữu tài khoản.

Chức năng 2.2: Sau khi xác thực, người dùng nhận tiền điện tử từ Ngân hàng.

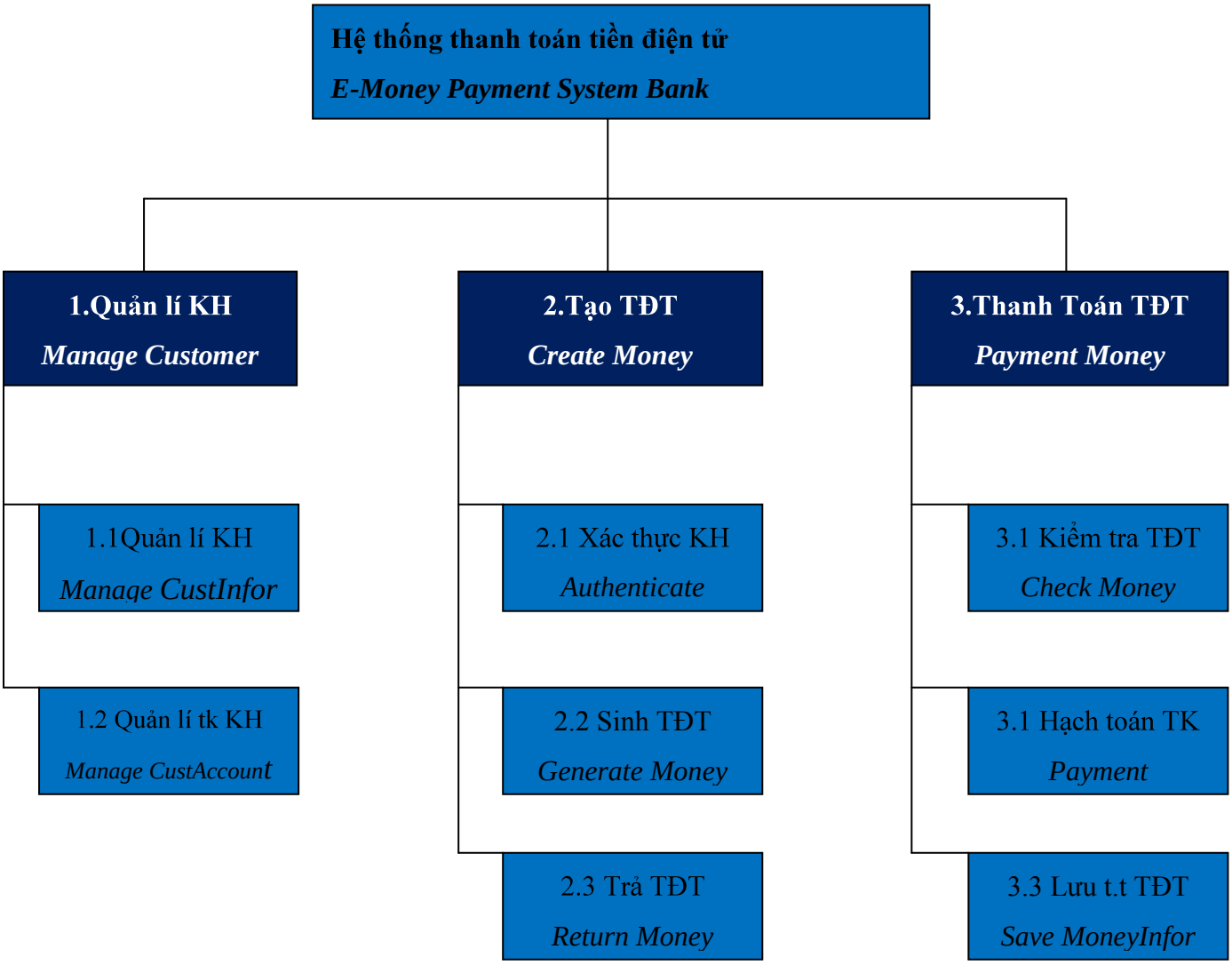
Chức năng 2.3: Người dùng lưu tiền điện tử do Ngân hàng gửi.

Chức năng 3.1: Khi thực hiện các giao dịch, với tư cách là người mua hàng, người dùng (Alice) trả tiền cho người cung cấp hàng hóa (Bob hoặc merchant)

Chức năng 3.2: Đồng thời trong các giao dịch, với tư cách là người bán hàng, Bob nhận tiền từ các người dùng khác trong hệ thống (Alice)

Chức năng 4.1: Sau khi thực hiện các giao dịch, để kiểm tra những đồng tiền mình nhận được có hợp pháp không, Bob gửi các thông tin thanh toán tới Ngân hàng yêu cầu kiểm tra.

Chức năng 4.2 : Đồng thời Bob cũng thử thách lại tính trung thực của Alice.



Biểu đồ phân rã chức năng trong hệ thống Ngân hàng

Giải thích chi tiết các chức năng:

Chức năng 1.1: Ngân hàng quản lí các thông tin về khách hàng (họ tên, địa chỉ, giá trị I tương ứng,..)

Chức năng 1.2: Ngân hàng quản lí thông tin về tài khoản của khách hàng.

Chức năng 2.1: Ngân hàng kiểm tra xem khách hàng có phải chủ sở yếu hợp pháp của tài khoản hay không.

Chức năng 2.2: Sau khi xác thực, Ngân hàng tạo tiền điện tử.

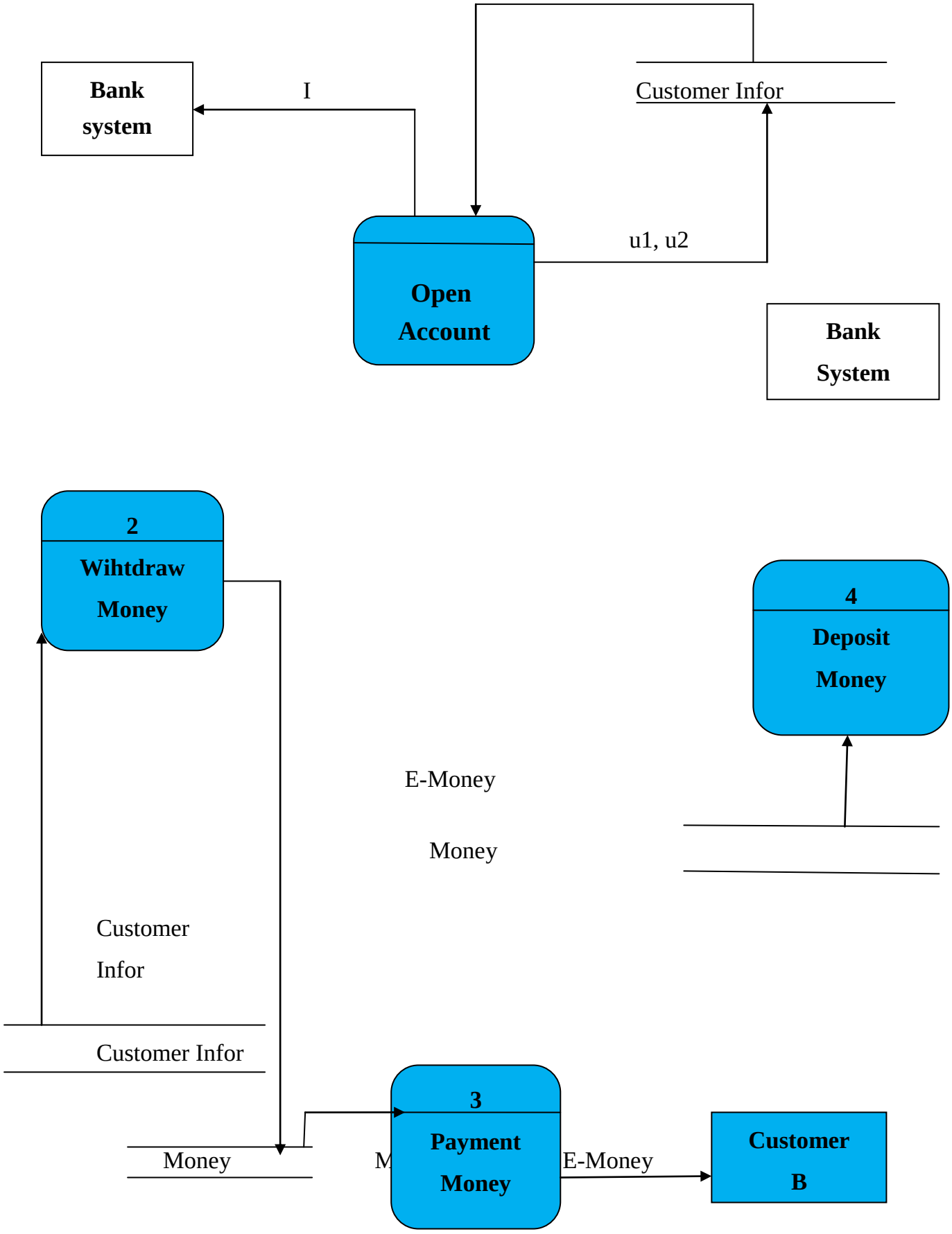
Chức năng 2.3: Ngân hàng trả lại tiền điện tử theo yêu cầu của khách hàng.

Chức năng 3.1: Ngân hàng kiểm tra tính hợp pháp của tiền điện tử theo yêu cầu của khách hàng.

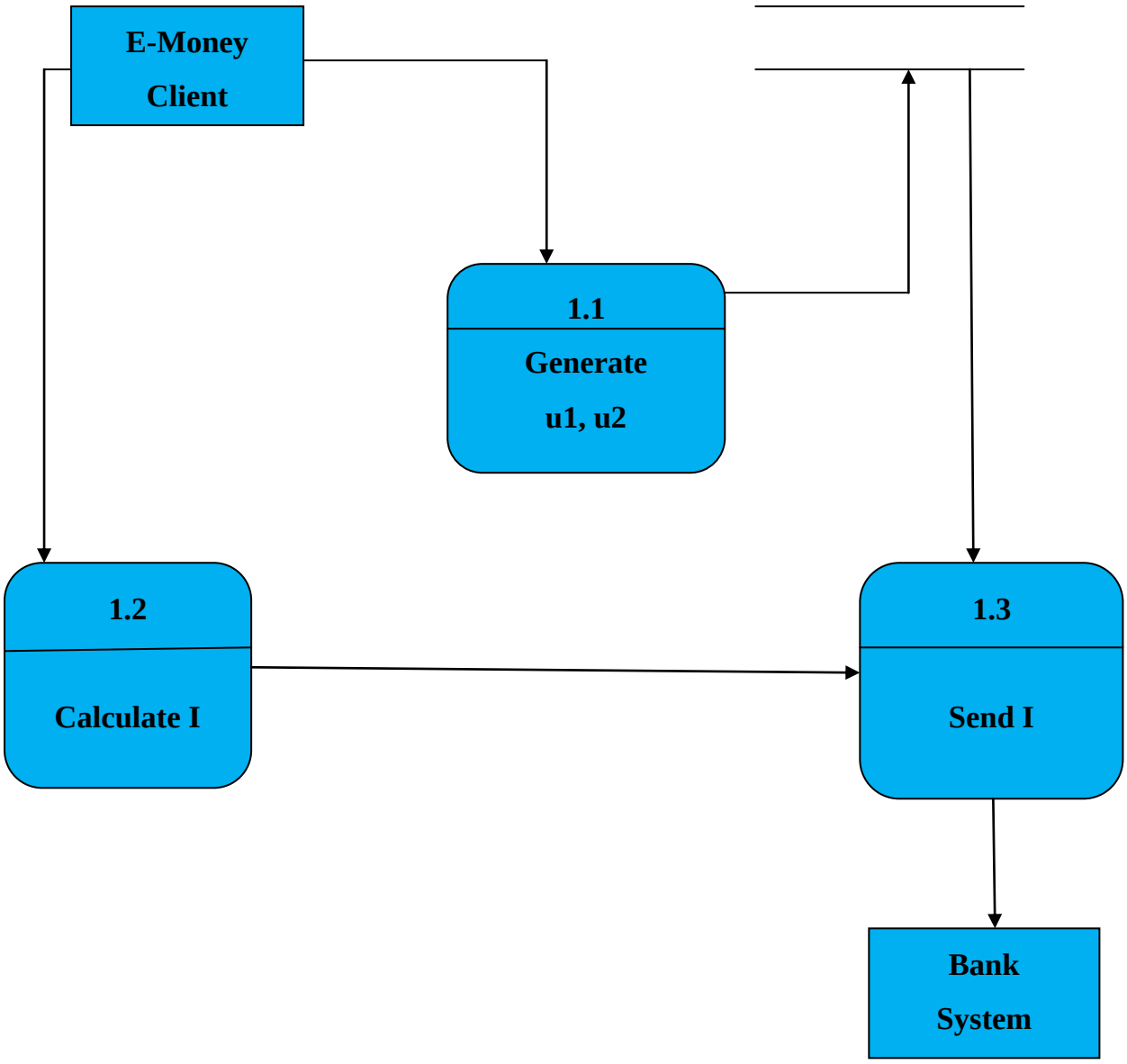
Chức năng 3.2: Ngân hàng cộng thêm (khi khách hàng là người bán hàng) hoặc trừ đi một lượng tiền (khikhách hàng là người mua hàng) trong tài khoản của khách hàng, tùy từng trường hợp cụ thể.

Chức năng 3.3: Các thông tin về tiền điện tử mà khách hàng đã tiêu xài, được Ngân hàng lưu trữ trong CSDL, dùng để truy vết kẻ gian lận.

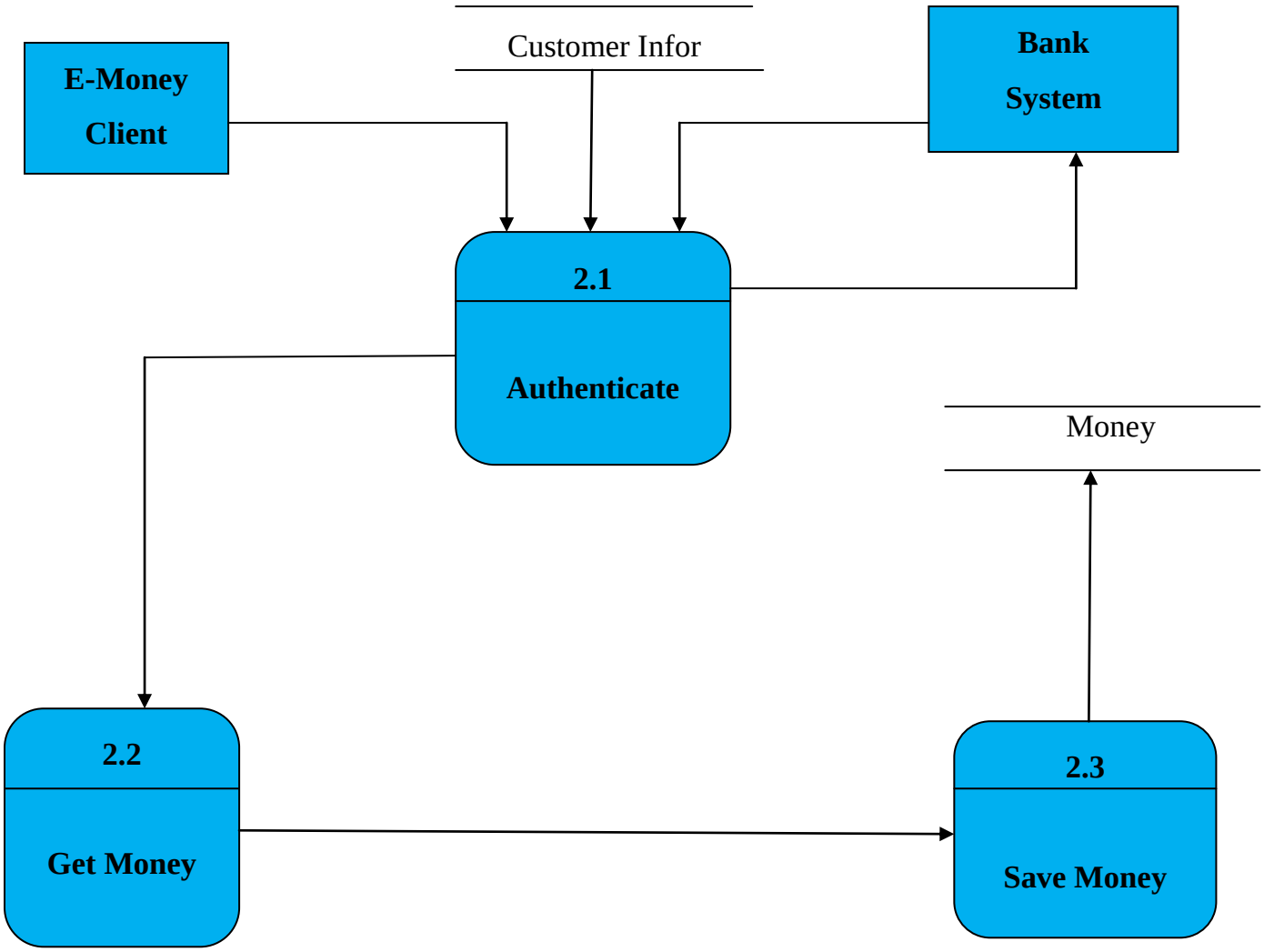
4.2.4.Biểu đồ luồng dữ liêu mức 0



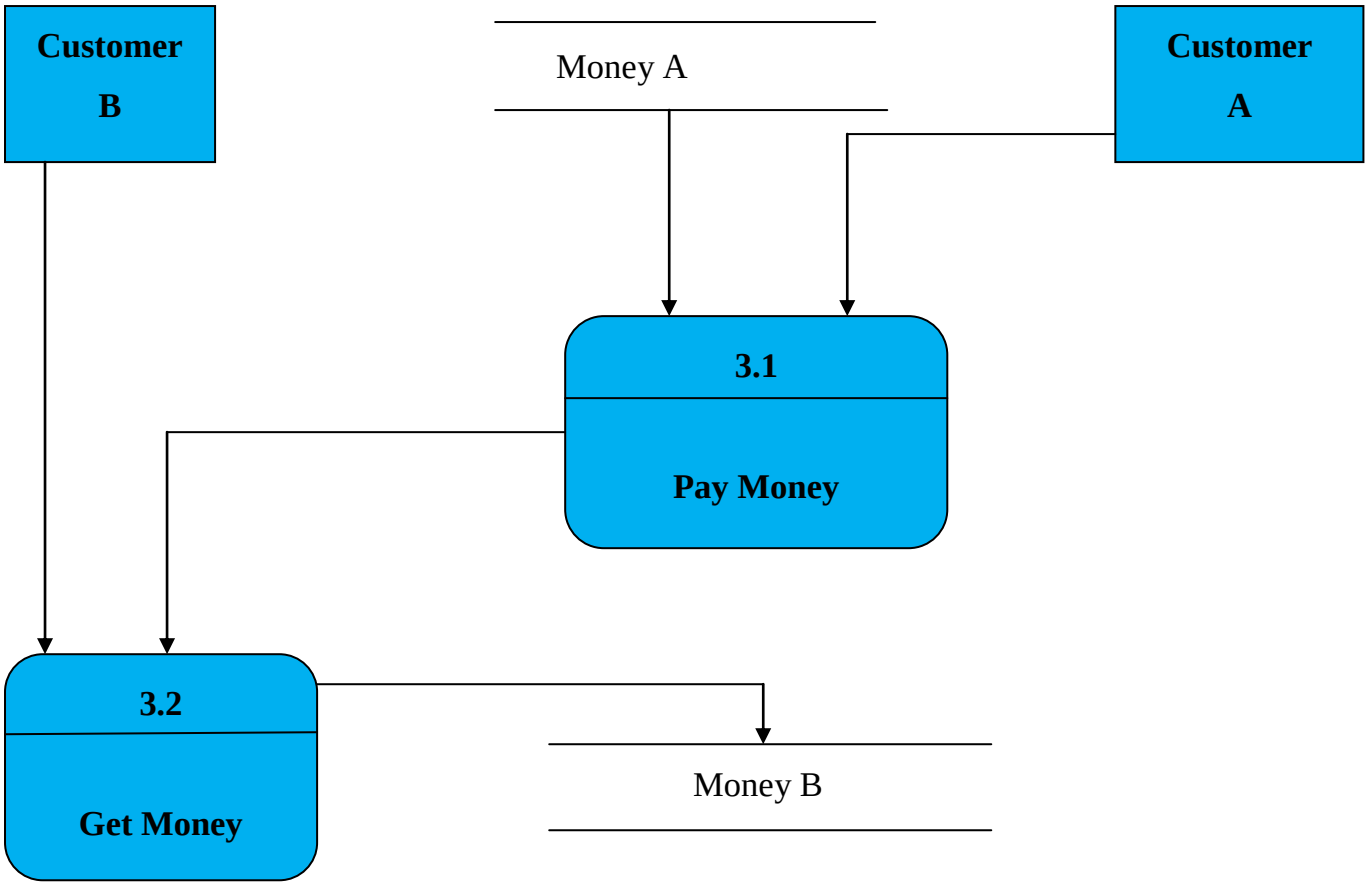
4.2.5 Các biểu đồ luồng dữ liệu mức 1



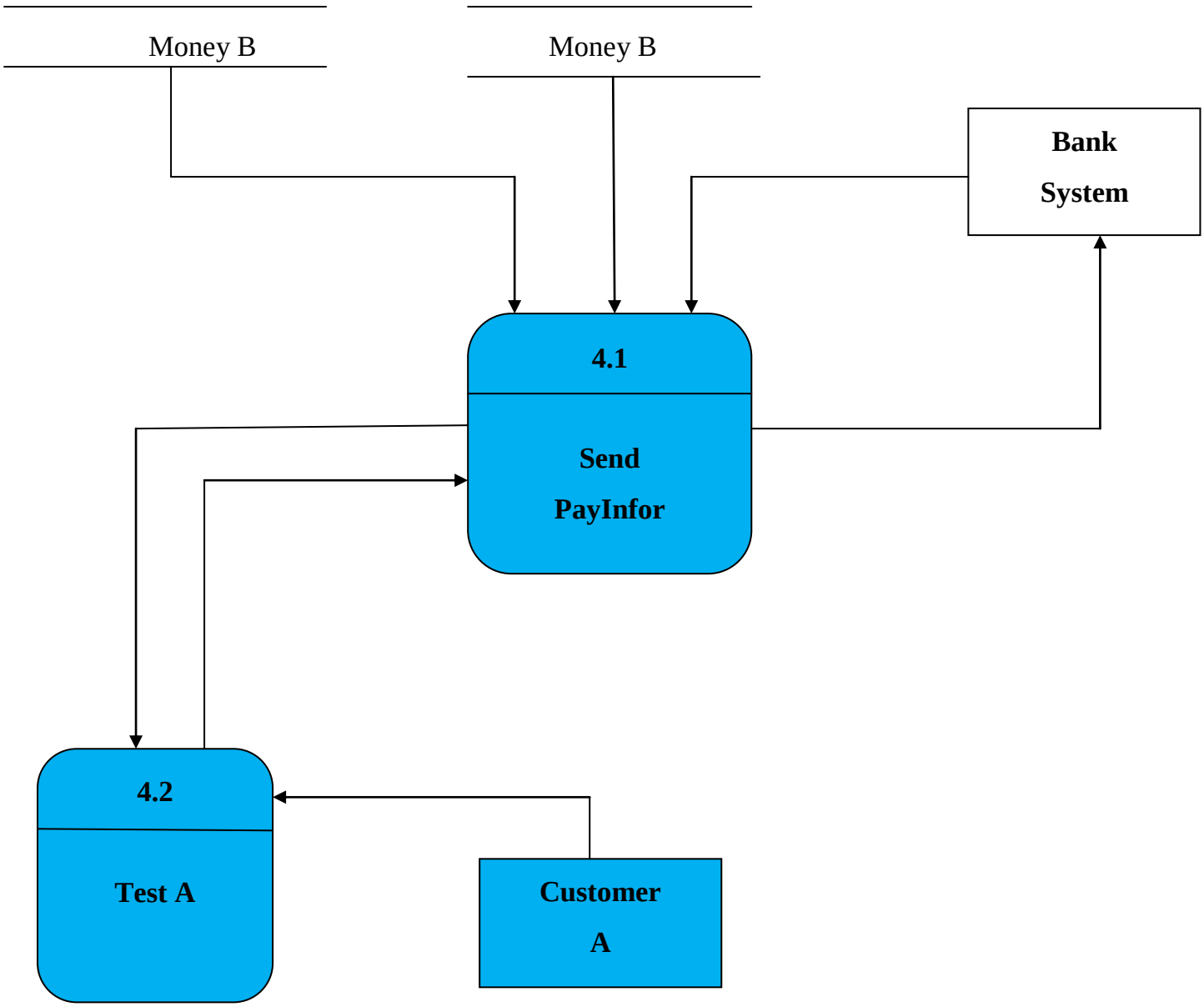
Biểu đồ luồng dữ liệu mức 1 cho chức năng open Account



Biểu đồ luồng dữ liệu mức 1 cho chứng năng Withdraw Money

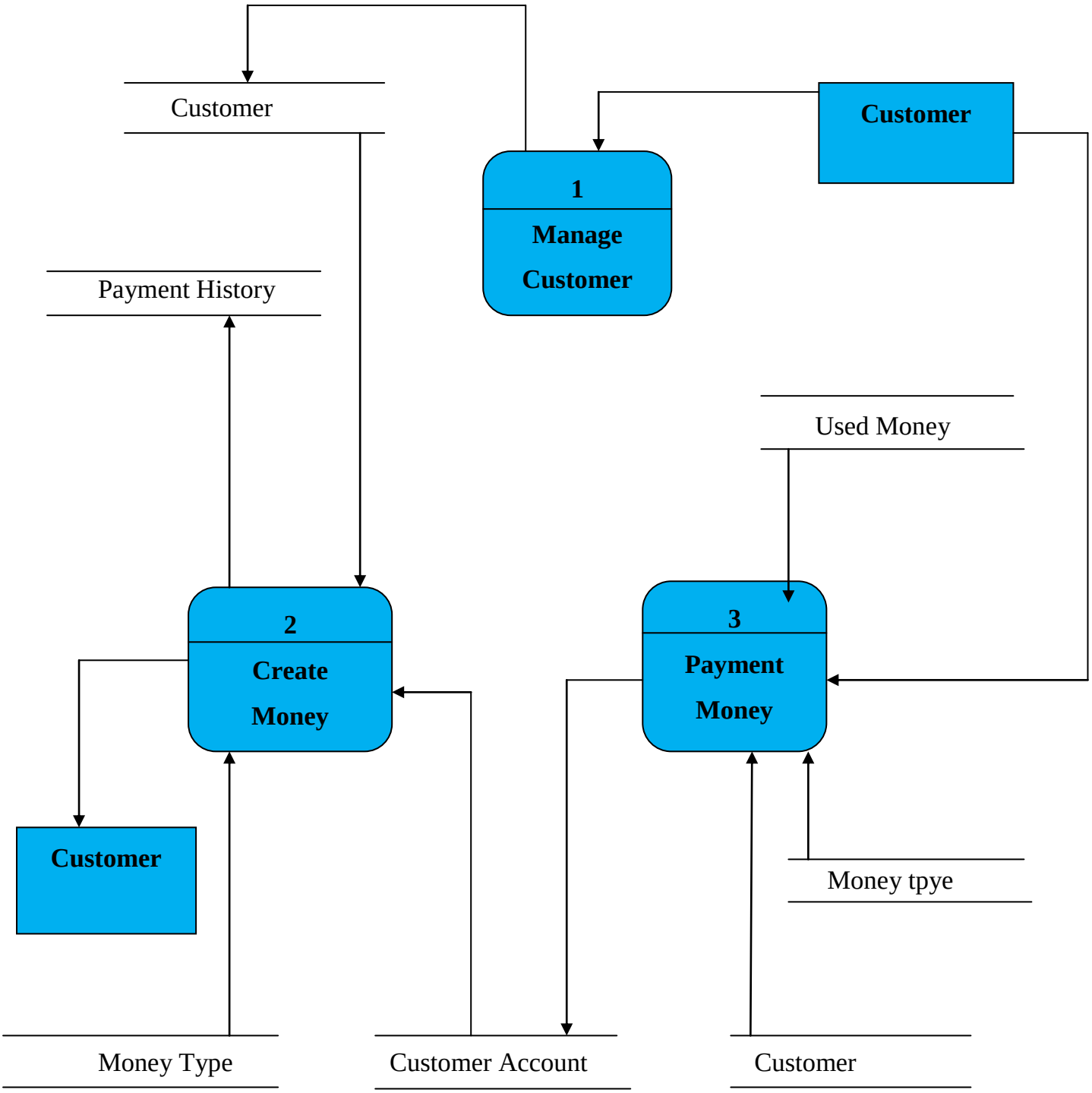


Biểu đồ luồng dữ liệu mức 1 cho chức năng Payment Money

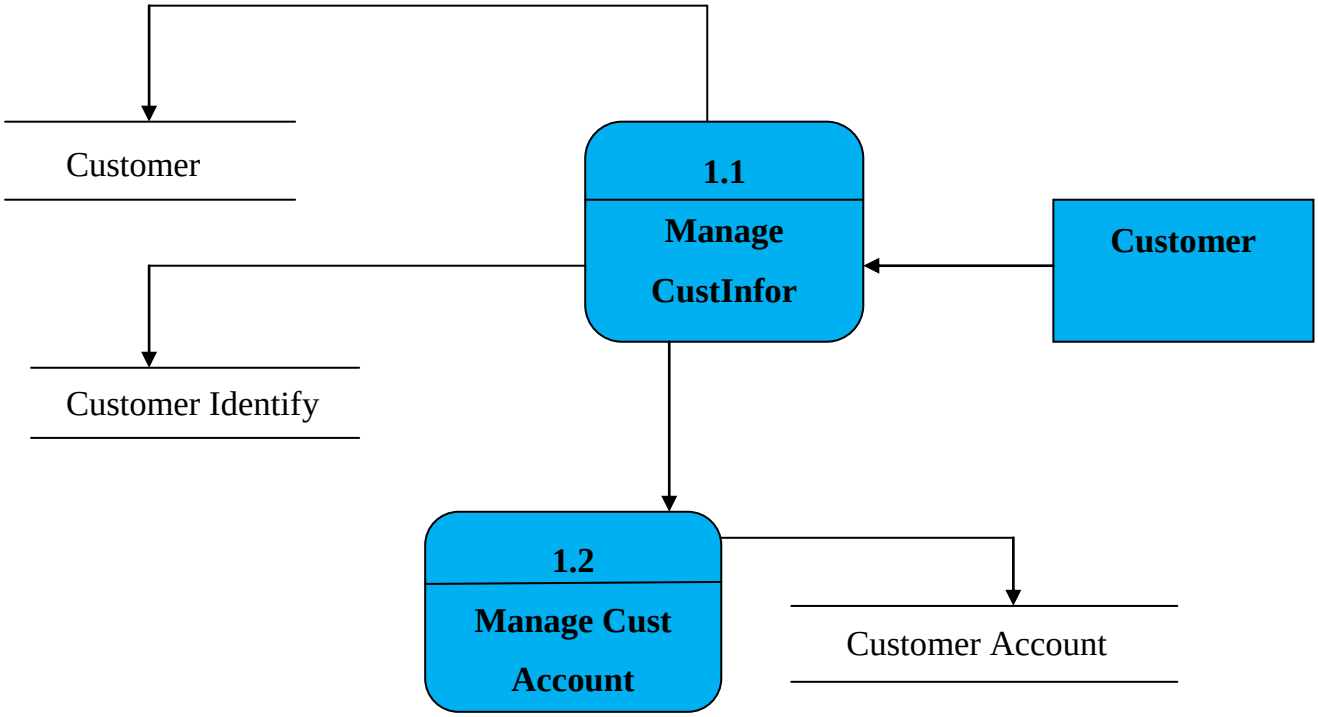


Biểu đồ luồng dữ liệu mức 1 cho chức năng Deposit Money

4.2.6. Hệ thống thanh toán danh cho Ngân hàng

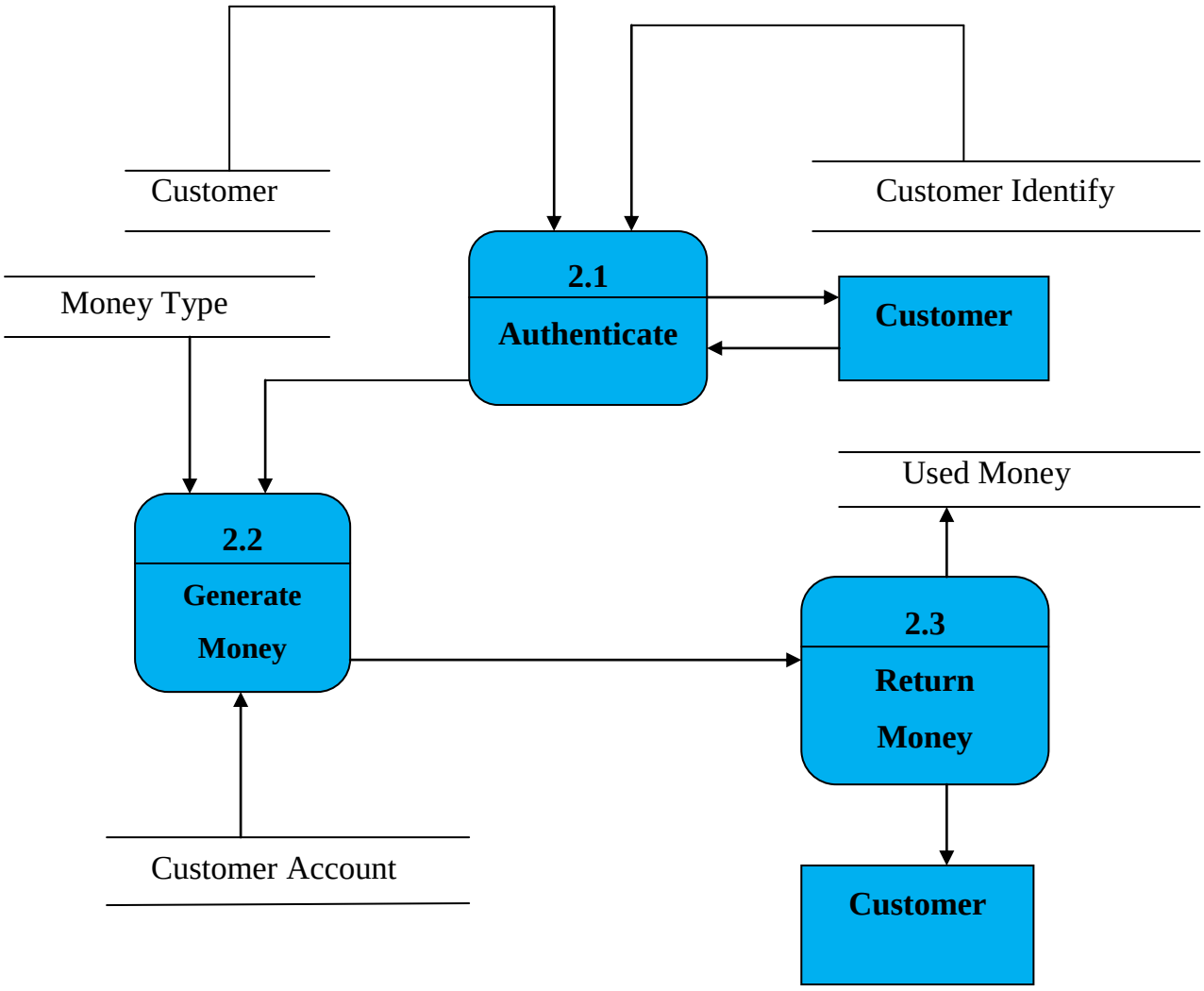


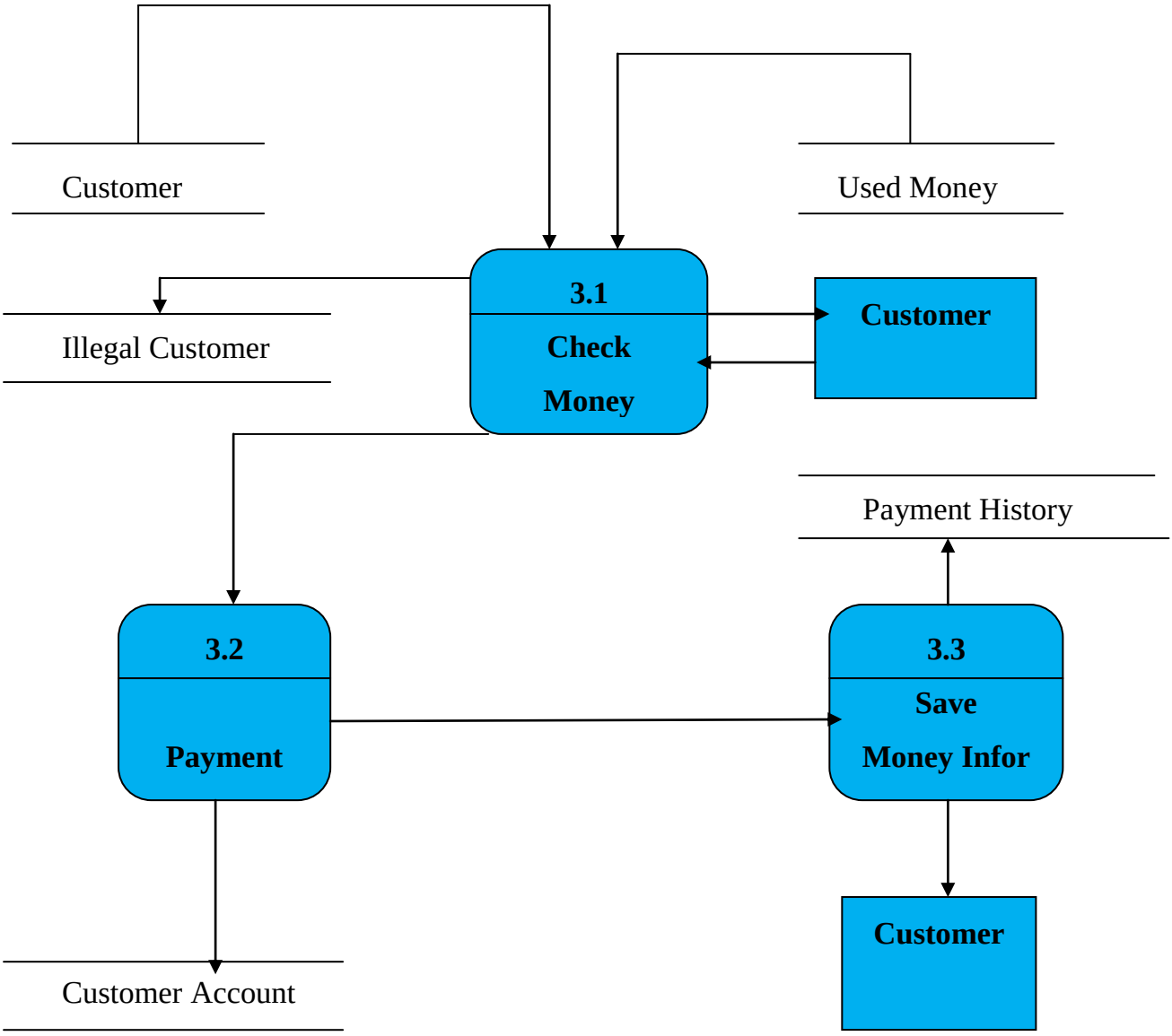
Biểu đồ luồng dữ liệu mức 0 trong hệ thống Ngân hàng



Biểu đồ dữ liệu mức 1 cho chức năng Manage Customer

Biểu đồ luồng dữ liệu mức 1 cho chức năng Create Money





Biểu đồ dữ liệu mức 1 cho chức năng Payment Money

4.3. THỬ NGHIỆM CHƯƠNG TRÌNH CHƯƠNG TRÌNH KÝ " MÙ" RSA

4.3.1. Thử nghiệm chương trình ký "mù" RSA

Bài toán đặt ra là giả sử A muốn lấy chữ ký của B trên x, nhưng không muốn cho B biết x. Quá trình thực hiện được tiến hành như sau:

+Lấy p, q là các số nguyên tố lớn, tính n=p*q

+Tính $\varphi(n)=(p-1)*(q-1)$, $ab \equiv 1 \bmod \varphi(n)$

+r là số ngẫu nhiên $\in Z_n$

(r được chọn sao cho tồn tại phần tử nghịc đảo $r^{-1}(\text{mod } n)$).

-Bước 1: A làm mù x bằng 1 hàm:

Blind(x) = x * r^b mod n = z, và gửi cho B.

-Bước 2: B ký trên Z bằng hàm:

Sign(z) = Sign(Blind(x) = z^a mod n = y, và gửi lại cho A.

-Bước 3: A tiến hành xóa mù y bằng thuật toán:

UnBlind(y) = UnBlind(Sign(Blind(x)))= y/r mod n = sign(x).

Ví dụ:

1./ Sinh khóa:

+Chọn các số nguyên tố p=3, q=5. Tính n = p*q= 15

$\varphi(n)=(q-1)*(q-1)= 2 * 4 = 8$

Đặt P = A = Z_n

+Chọn khóa kiểm tra chữ ký (khóa công khai) b : chọn b = 3

1<b< $\varphi(n)$, b là số nguyên tố cùng nhau với $\varphi(n)$

+Chọn Khóa ký (khóa bí mật) a: Chọn a = 3.

a là phần tử nghịc đảo của b theo φ n, (tl: a*b $\equiv$ 1 (mod $\varphi(n)$).

2./ Ký số:

Chữ ký trên m = 2 $\in$ P là y = Sig(m)= m^a mod n= 2^3 mod 15 = 8

3/. Kiểm tra chữ ký:

Ver(m, y) = đúng $\Leftrightarrow$ m = y^b (mod n)

Vì 2 $\equiv 8^3$ (mod 15), do đó chữ ký y = 8 là chữ ký đúng

4.3.2 . Chương trình ký “ mù” RSA.

- ***Yêu cầu về cấu hình phần cứng:***

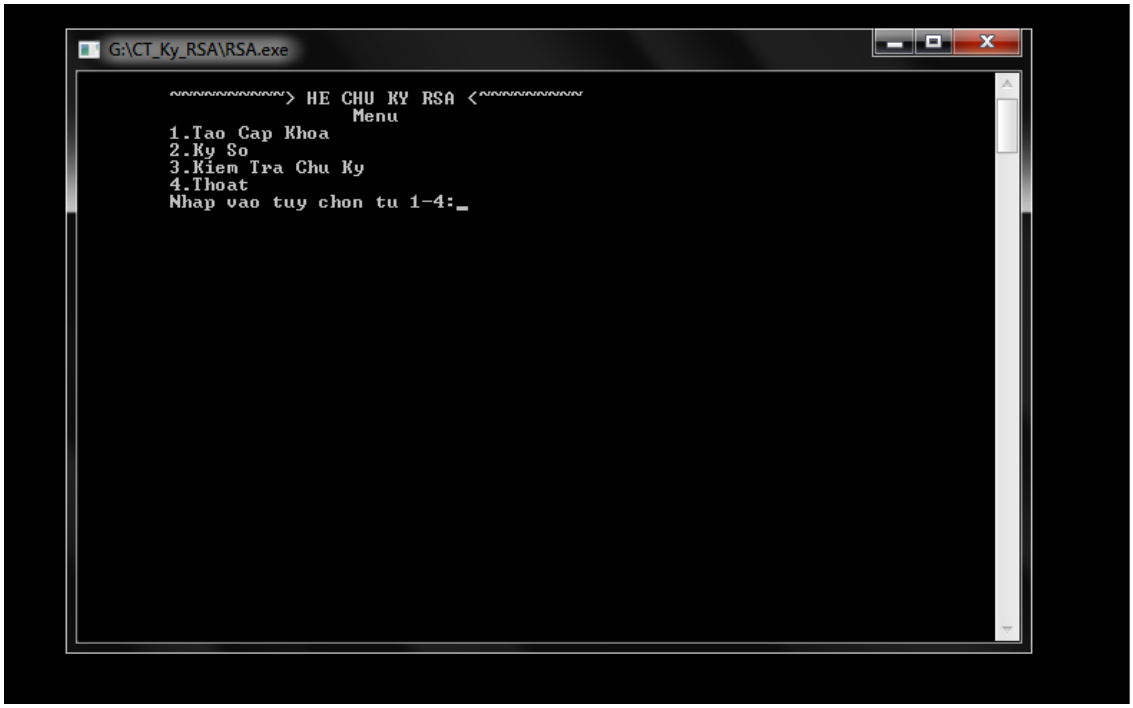
  - Bộ nhớ trong 1G.
  - Cấu hình CPU bình thường.
  - Ram 512 trở lên.
  - Máy tính k có vi rút và hoạt động bình thường.
  -

- ***Yêu cầu về cấu hình phần mềm:***

  -Hệ điều hành MicroSoft Windows.

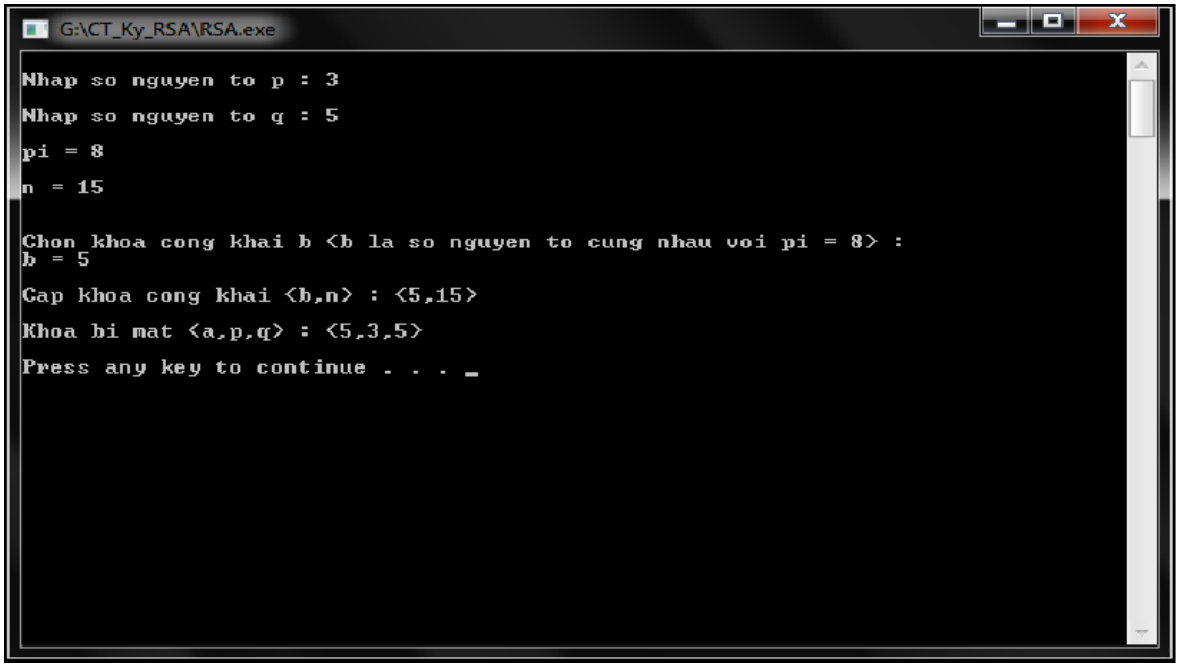
  -Ngôn ngữ lập trình C, C++.

Giao diện chương trình

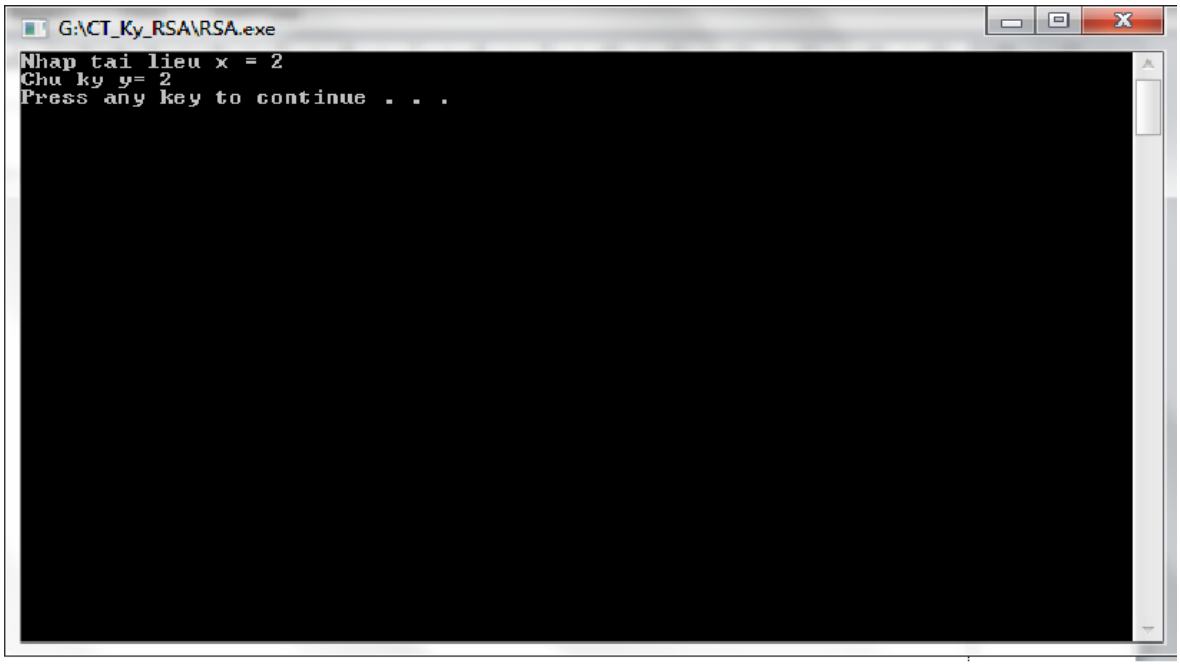


Giao diện chương trình chữ ký "mù" RSA

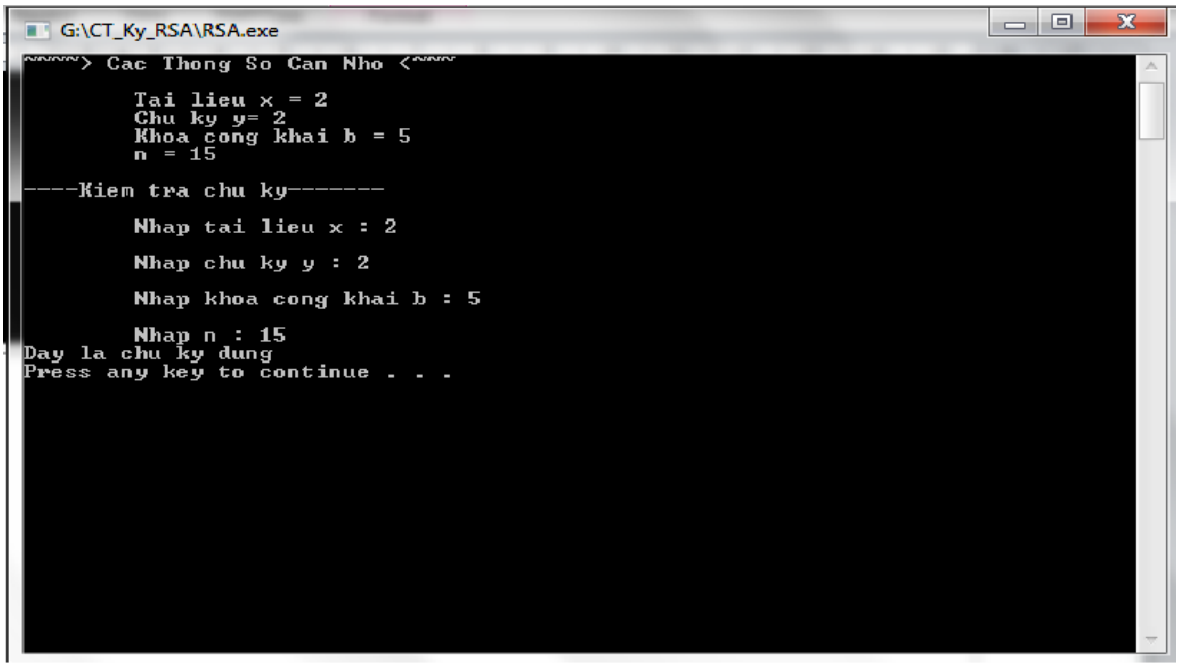
Bươc 1 : Tạo Cặp Khóa



Bước 2 : Ký số


G:\CT_Ky_RSA\RSA.exe
Nhap tai lieu x = 2
Chu ky y= 2
Press any key to continue . . .

Bước 3 : Kiểm tra chữ ký



KẾT LUẬN

Sau thời gian làm việc, với sự nỗ lực của bản thân và sự tận tình chỉ bảo của thầy giáo PGS.TS.Trịnh Nhật Tiến em đã hoàn thành đồ án tốt nghiệp của mình.

Đồ án đã trình bày những kiến thức tổng quát về tiền điện tử, nghiên cứu và phân tích giải pháp cho các bài toán nảy sinh khi thanh toán tiền điện tử

Đồ án tốt nghiệp gồm có hai kết quả chính:

1./Nghiên cứu và hệ thống lại các vấn đề sau:

- Các khái niệm cơ bản về Tiền điện tử
- Một số phương pháp mã hóa, ký số
- Một số bài toán về An toàn thông tin trong hệ thống Tiền điện tử

2./Thử nghiệm một số ứng dụng

- Vấn đề sử dụng tiền điện tử ở Việt Nam
-Thử nghiệm chương trình bảo vệ Tiền điện tử

TÀI LIỆU THAM KHẢO

Tiếng việt.

1.Trịnh Nhật Tiến PGS.TS (2008), *Giáo trình An toàn dữ liệu.*

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

3.Trịnh Nhật Tiến PGS.TS (2007), *Bài giảng môn Phân tích đánh giá thuật toán.*

4.Nguyễn Văn Vỵ PGS.TS (2002), *Phân tích thiết kế Hệ thống thông tin*, Nhà xuất bản thống kê Hà Nội.

Tiếng Anh

6.ByeongKon Kim, School of Enginerring, Information and Communications University (2004).

7.[Ebook- C] *Applied Cryptography Second Edition* – John Wiley & Sons Inc.pdf

8.Pretince Hall – *Modern Cryptography- Theory And Practice* -2003.pdf

9.http://ntrd.cs.tcd.ie/meipeice/Project/Mlists/brands.html