Tạp chí Tin học và Điều khiển học, T.21, S.2 (2005), 184–190

MỘT GIẢI PHÁP TRIỂN KHAI MÔ HÌNH KÝ VĂN BẢN ĐIỆN TỬ

PHẠM HUY ĐIỂN, ĐINH HỮU TOÀN

Viện Toán học, VAST

Abstract. The paper presents a method for implementation of a Digital Signature Scheme which is based on the combination of the RSA algorithm and the SHA-256 hashing function. The obtained software package possesses high processing speed and user-friendly (Vietnamese) interface.

Tóm tắt. Trong xu thế hiện nay, mọi loại hình dịch vụ trong lĩnh vực công nghệ thông tin phải được đơn giản hóa ở mức cao nhất để tạo thuận lợi tối đa cho người dùng. Chính vì vậy, quy trình ký điện tử với các tính toán phức tạp và thủ tục nghiêm ngặt chỉ có thể khả thi nếu được triển khai một cách khéo léo, với các giao diện thân thiện và đơn giản. Mục tiêu của công trình này là đưa ra một giải pháp cho vấn đề đó.

1. BẢN CHẤT CỦA CHỮ KÝ VÀ VẤN ĐỀ ĐIỆN TỬ HÓA QUY TRÌNH KÝ

1.1. Chữ ký trong đời sống

Trong đời sống thường ngày, chữ ký (viết tay) trên một văn bản là một minh chứng về "bản quyền" hoặc ít nhất cũng là sự "tán đồng, thừa nhận" nội dung của văn bản. Những yếu tố nào làm lên "sức thuyết phục" của nó? Một cách lý tưởng thì:

• Chữ ký là bằng chứng thể hiện người ký có chủ định khi ký văn bản, và cũng là thể hiện chủ quyền của người ký, nó làm cho người ta nhận biết rằng ai đích thị là người đã ký văn bản.

• Chữ ký *không thể được tái sử dụng*, tức là nó là phần của văn bản mà không thể "gắp" sang các văn bản khác. Nói cách khác, nó chỉ có giá trị ở trong văn bản được ký và trở thành vô giá trị nếu ở ngoài văn bản đó.

• Văn bản sau khi ký thì không thể thay đổi được nội dung.

• Chữ ký không thể chối bỏ được và cũng không thể giả mạo được. Người đã ký văn bản không thể phủ định việc mình đã ký, còn người khác không thể tạo ra chữ ký đó.

Trong cuộc sống đời thường, mọi cái không phải lúc nào cũng diễn ra theo đúng như mô hình "lý tưởng" nêu trên, nhưng đây luôn là điều người ta mong muốn.

Trong trào lưu "tin học hóa" các hoạt động xã hội ngày càng rộng rãi, các loại hình văn bản điện tử đang ngày càng trở nên phổ biến và các giao dịch thông tin điện tử ngày càng trở lên lấn át các giao dịch giấy tờ truyền thống. Một vấn đề cấp bách đang được đặt ra là: liệu chúng ta có thể mang được những nét "đặc trưng lý tưởng" của chữ ký viết tay (nêu trên) vào "thế giới điện tử hóa" hay không? Nói cách khác, liệu ta có thể tạo ra cho mỗi văn

bản điện tử một cái gì đó mang các thuộc tính tương tự như chữ ký hay không?

Ta thấy ngay những khó khăn hiển nhiên sẽ gặp trong thế giới các văn bản điện tử, đó là: các dòng thông tin trên máy tính được sao chép một cách quá dễ dàng, việc thay đổi nội dung một văn bản điện tử chẳng để lại dấu vết gì về phương diện "tẩy xoá", hình ảnh của chữ ký tay của một người (dù khó bắt chước đến đâu) cũng dễ dàng cho "sao chép" từ văn bản này sang văn bản khác,... Tóm lại, văn bản điện tử không có được thuộc tính "bút sa gà chết" như văn bản giấy, và do đó không phù hợp với cung cách ký thông thường xưa nay. Để tạo ra cho mỗi văn bản điện tử một "chữ ký" với các thuộc tính tương tự như chữ ký trên văn bản giấy, ta cần có một cách tiếp cận hoàn toàn mới. Một trong những cách tiếp cận đó là dựa trên các thành tựu công nghệ mã hóa thông tin hiện đại.

1.2. Hệ mã khoá công khai và việc tạo chữ ký điện tử

Nguyên lý hoạt động của hệ mã khoá công khai:

Hệ mã khoá công khai là hệ mật mã được phát minh ra trong những thập kỷ cuối của thế kỷ 20. Nét khác biệt cơ bản của các hệ mã này so với các hệ mã truyền thống trước đây là nó sử dụng 2 chìa khoá riêng biệt cho việc lập mã và giải mã văn bản. Chìa dùng cho việc lập mã có thể được công bố cho mọi người biết (thường được gọi là chìa công khai), còn chìa dùng cho việc giải mã thì được giữ bí mật tuyệt đối. Việc biết được chìa khoá lập mã (công khai) không cho phép tính ra được chìa khoá giải mã (bí mật). Mỗi cá thể k tham gia vào hệ thống được cấp riêng một cặp chìa khoá (E_k, D_k), trong đó E_k là chìa khoá lập mã, còn D_k là chìa khoá giải mã. Khi mã hóa một văn bản P (bằng chìa khoá lập mã E_k) ta sẽ được một văn bản mã ký hiệu là $C = E_k(P)$. Văn bản này chỉ có thể được giải mã bằng chìa khoá D_k (cùng cặp với E_k), nghĩa là $D_k(C) = D_k(E_k(P)) = P$.

Khi một cá thể i nào đó muốn gửi thông điệp M cho đối tác k thì anh ta dùng chìa khoá lập mã E_k của đối tác k (đã được biết công khai) để mã hóa văn bản và gửi đi dưới dạng thông điệp mã $C = E_k(M)$. Khi đối tác k nhận được thông điệp này thì dùng chìa khoá giải mã của mình (là D_k) để giải mã ra theo nguyên lý đã nêu:

$$D_k(C) = D_k(E_k(M)) = M.$$

Các cá thể khác trong hệ thống, nếu nhận được văn bản mã C thì cũng không thể nào giải ra M, vì họ không có chìa khoá giải mã D_k của cá thể k.

Các nguyên lý vừa trình bày trên đã được cụ thể hoá trong một số hệ mã khoá công khai được phát minh gần đây, điển hình hơn cả là hệ mã RSA được phát minh vào năm 1978 bởi Rivest, Shamir và Adleman [2], và hệ mã đường cong elliptic do Miller và Koblitz tìm ra (một cách độc lập) vào khoảng cuối những năm tám mươi vừa qua [3,4], đã được trình bày chi tiết trong [5].

Nguyên lý tạo chữ ký điện tử trong hệ mã khoá công khai

Với hệ mã khoá công khai, một quy trình ký văn bản điện tử được thiết lập dựa trên ý tưởng của hai nhà khoa học Diffie và Hellman [1]:

(1) Người gửi (chủ nhân văn bản) ký văn bản bằng cách mã hoá nó với khoá bí mật của mình, rồi gửi cho người nhận.

(2) Người nhận văn bản (sau khi ký) tiến hành kiểm tra chữ ký bằng cách sử dụng chìa khoá công khai của người gửi để giải mã văn bản. Nếu giải mã thành công thì văn bản ký là đúng của người gửi.

Giao thức này mang đầy đủ các thuộc tính của thủ tục ký tá thông thường, đã mô tả ở trên. Thật vậy, chữ ký là sản phẩm của người đã chủ động tạo ra nó, và cũng thể hiện chủ nhân của nó chính là người sở hữu chiếc chìa khoá bí mật đã được dùng để mã văn bản (kiểm tra bằng cách cho giải mã bằng chìa khoá công khai của người đó). Không ai làm giả được "chữ ký" vì rằng chỉ có duy nhất một người có chìa khoá bí mật đã dùng để "ký" (mã hoá). Chữ ký cho văn bản này không thể "tái sử dụng" cho văn bản khác, vì việc biết chữ ký (văn bản mã) không cho phép tìm ra được chìa khoá bí mật của người gửi (để có thể mã một văn bản khác). Văn bản đã ký không thể thay đổi (xuyên tạc) được nội dung, vì nếu đã "mở văn bản ra" (giải mã) để thay đổi thì không thể "ký lại" (mã lại) được nữa, vì không có chiếc chìa khoá bí mật của "người đã ký" (như đã nói ở trên). Người ký văn bản không thể thoái thác việc mình "đã ký", vì ngoài ông ta ra không còn ai có cái chìa khoá đã được dùng để "ký" văn bản.

Rõ ràng, về mặt logic thì quy trình ký như trên là rất hợp lý. Mọi thành viên tham gia vào hệ mã khoá công khai đều có được khả năng ký văn bản điện tử (bằng chìa khoá bí mật của riêng mình) và kiểm tra chữ ký của những người khác (bằng chìa khoá công khai mà họ đã công bố).

Tuy nhiên, trong thực tiễn triển khai, có một vấn đề nan giải là tốc độ mã hoá của các hệ mã khoá công khai là vô cùng chậm. Cho nên, việc mã toàn bộ một văn bản dài (như thông tư, nghị định, văn kiện,...) là không khả thi trên thực tiễn. Để khắc phục khó khăn này, người ta không "ký" trực tiếp cả văn bản mà chỉ ký lên cái "đặc trưng" của nó, là xâu số vẻn vẹn vài trăm bit, được sinh ra nhờ một hàm "chiết xuất" đặc biệt. Hàm này có tên gọi là hàm băm mật mã, nhận giá trị đầu vào là văn bản (độ dài tùy ý) và cho đầu ra là một dãy số có độ dài xác định (khoảng vài trăm bit), gọi là mã băm (message digest). Hai thuộc tính quan trọng của hàm chiết xuất là tính một chiều và tốc độ nhanh. Tính một chiều thể hiện ở chỗ không thể tạo ra được một văn bản có mã băm (đặc trưng) là một xâu số cho trước, và dó đó không thể mạo ra một "văn bản giả" có cùng đặc trưng với một văn bản cho trước. Tốc độ nhanh có nghĩa là thời gian "chiết xuất" đặc trưng cho văn bản là không đáng kể.

Hàm băm mật mã còn có thuộc tính quan trọng là rất "nhậy" đối với các thay đổi của văn bản, theo đó chỉ cần một thay đổi cực nhỏ trong văn bản (như thay dấu chấm, dấu phảy,...) cũng sẽ kéo theo sự thay đổi rõ rệt trong giá trị mã băm của nó. Để nhận biết sự toàn vẹn của một văn bản người ta chỉ cần xem đặc trưng của nó có bị thay đổi hay không. Rõ ràng, việc đặc trưng văn bản không bị thay đổi cũng đồng nghĩa với việc bản thân văn bản không bị thay đổi. Từ đây ta có một quy trình ký các văn bản dựa vào đặc trưng của nó.

Quy trình tạo ra và kiểm tra chữ ký điện tử

Khi một cá thể A muốn ký một văn bản thì cần phải thực hiện các bước sau đây:

1. Tính đặc trưng của văn bản P (bằng hàm chiết xuất có sẵn trên hệ thống);

2. Dùng chìa khoá bí mật của mình để mã hoá dãy số đặc trưng văn bản thu được ở bước trên. Đặc trưng văn bản sau khi được mã (bằng chìa bí mật của A) thì được gọi là chữ ký điện tử (của ông A đối với văn bản P);

Một người nào đó, nhận được văn bản cùng với chữ ký điện tử đi kèm, muốn tiến hành kiểm tra thì cần tiến hành các bước sau:

1. Tính đặc trưng của văn bản (bằng hàm chiết xuất có sẵn trên hệ thống);

2. Giải mã chữ ký điện tử (bằng chìa khoá công khai của ông A) để có một đặc trưng

nữa của P, rồi so sánh nó với đặc trưng thu được ở bước trên. Nếu chúng khớp nhau thì chứng tỏ văn bản nhận được chính là văn bản đã được ông A ký và nội dung của nó không bị thay đổi so với khi ký.

Dễ dàng thấy rằng chữ ký điện tử được tạo ra trong quy trình trên có đầy đủ các thuộc tính đã nêu trong mục đầu. Thời gian tạo chữ ký được giảm đi rất nhiều và gần như không phụ thuộc vào độ dài của văn bản (vì thời gian tính mã băm là không đáng kể).

Như vậy, chữ ký điện tử không phải là một nét vẽ ngoằn ngoèo khó bắt chước (như chữ ký thông thường) mà là một dãy số thu được từ việc mã hóa dãy số đặc trưng văn bản với chìa khoá bí mật của người ký. Do bản chất này, chữ ký điện tử còn được gọi là chữ ký số (digital signature). Các công cụ cơ bản của giải pháp ký điện tử là hàm băm mật mã và thuật toán mã hóa khoá công khai. Các tác vụ ký điện tử và kiểm tra chữ ký, được thực hiện trên cơ sở phối hợp các công cụ này theo các quy trình nghiêm ngặt như đã mô tả. Thiết lập một chương trình ký điện tử cũng chính là việc tạo ra các công cụ cơ bản và thực hiện các quy trình phối hợp này một cách tự động.

2. MỘT GIẢI PHÁP TRIỂN KHAI

2.1. Nhu cầu và mục tiêu

Trong tương lai gần, đối tượng phục vụ của chương trình ký điện tử sẽ là tất cả mọi người trong xã hội. Phần lớn trong số họ là những người không được đào tạo về công nghệ thông tin. Chính vì vậy, quy trình ký điện tử với các thủ tục nghiêm ngặt và không đơn giản (như được mô tả trong phần trên) chỉ có thể khả thi nếu được triển khai một cách khéo léo, dưới dạng các phần mềm tiện ích, với các giao diện thân thiện và đơn giản. Mục tiêu của chúng ta là đưa ra một giải pháp cho vấn đề đó. Để có được sự tinh giản tối đa, chúng tôi đã tránh việc thiết lập chương trình trong mô hình tổng quát, mà hướng vào một số tác vụ quan trọng nhất, với thao tác vận hành thật đơn giản. Trong mô hình triển khai này, các thủ tục nghiêm ngặt của quy trình tạo chữ ký điện tử và xác minh chữ ký được thực hiện một cách tự động (và là "trong suốt" đối với người sử dụng). Thao tác chính để thực hiện tác vụ ký chỉ là khai báo mật khẩu mở chìa khoá bí mật; còn thao tác chính để thực hiện tác vụ kiểm tra chữ ký chỉ là chọn chìa khoá công khai (của người đã ký văn bản). Giao diện tiếng Việt đơn giản giúp người dùng có thể nắm bắt được công việc chỉ trong vòng vài phút.

2.2. Lựa chọn hệ mã khóa công khai: RSA

Nguyên lý thực hiện

Hệ RSA được xây dựng trên cơ sở phép toán nâng lên lũy thừa rồi rút gọn theo môđun. Chìa khoá lập mã là một bộ hai số (e, n), trong đó số n là tích của hai số nguyên tố rất lớn, $n = pq$, còn e là một số tự nhiên nguyên tố cùng nhau với số $\phi(n) = (p-1)(q-1)$. Để mã hoá một khối P trong văn bản, người ta tính:

$$C = P^e (\text{mod } n).$$

Việc giải mã trực tiếp theo theo quy trình ngược lại (tức là, khai căn bậc e theo môđun) là không thể thực hiện được (vì đòi hỏi thời gian tính toán vô cùng lớn). Nhờ áp dụng định lý Euler, ta có thể giải mã theo cách khác: chỉ cần biết được số d thỏa mãn $ed \equiv 1 (\text{mod} \phi(n))$, tồn tại do điều kiện nguyên tố cùng nhau đã nói ở trên, ta sẽ có đẳng thức sau

$$C^d(\mathrm{mod}n) = P.$$

Nghĩa là, để "giải mã" ta không cần phải làm phép khai căn "bậc e" mà chỉ cần làm phép nâng lên lũy thừa "bậc d" (môđun n). Bộ số (d, n) vì vậy được gọi là chìa khoá giải mã.

Độ an toàn của RSA

Hệ mã thỏa mãn các nguyên tắc của hệ mã khoá công khai nói ở mục trên. Việc biết chìa khoá lập mã (e, n) không cho phép tìm ra được chìa khoá giải mã (d, n), nếu như không biết được $\phi(n)$. Có thể chỉ ra rằng việc tìm ra $\phi(n)$ là tương đương với việc phân tích n ra các thừa số nguyên tố p, q, một vấn đề không thể thực hiện được trong thời gian hàng trăm năm nữa (với năng lực máy tính mạnh nhất hiện có), nếu ta chọn các số p và q khoảng 150 chữ số thập phân. Do tính đơn giản trong thiết kế và triển khai, RSA đang được sử dụng rộng rãi và có lẽ là được dùng nhiều nhất trong số các thuật toán với khoá công khai. Cũng chính vì vậy, nó đã trải qua nhiều cuộc thử thách, xem xét, khảo cứu kỹ lưỡng của cộng đồng và đã có được nhiều bằng chứng kiểm nghiệm về tính an toàn của nó.

Những vấn đề trong kỹ thuật triển khai

Khó khăn cơ bản trong việc triển khai hệ mã RSA chuẩn mực là phải làm việc với các số nguyên cực lớn (với độ dài cỡ ba trăm chữ số thập phân). Tính toán với những số lớn thường có tốc độ vô cùng chậm, cho nên nếu không có những giải pháp khéo léo thì không thể khả thi trong thực tiễn. Để vượt qua được trở ngại này, cần có các giải pháp hiệu quả hơn, trên cở sở khai thác những nét đặc thù của phép toán mã (nâng lên lũy thừa và lấy môđun theo số cực lớn). Một giải pháp đã được chúng tôi sử dụng là nâng cao tốc độ phép toán lũy thừa bằng cách phân tích số mũ theo "xích cộng ngắn nhất". Một giải pháp khác làm tăng tốc độ phép tính theo môđun là sử dụng định lý Trung Quốc để quy phép tính theo môđun số lớn qua các phép tính theo môđun các số nhỏ hơn. Nhờ áp dụng các giải pháp này, chúng tôi đã làm tăng được tốc độ tính toán lên nhiều lần, giảm thời gian ký một văn bản xuống dưới 1 giây.

Tham số của hệ thống

Chương trình được thiết lập với các tham số được ấn định như sau:

• Hệ mã khoá công khai RSA sử dụng chìa khoá với độ dài 1024 bit. Các số nguyên tố dùng làm chìa đều được trải qua kiểm tra không có phân tích "mịn".

• Hàm băm mật mã được sử dụng là SHA-256 với chiều dài mã băm là 256 bit.

Với các tham số trên, chương trình là "miễn dịch" trước khả năng tấn công của các phương tiện "thám mã" đương thời, như cộng đồng khoa học mật mã quốc tế đã khẳng định.

2.3. Cơ chế hoạt động và giao diện làm việc

Cài đặt và khai báo tham số cho chương trình

Chương trình được cài đặt dễ dàng bằng việc cho chạy file install.exe trong đĩa cài cặt. Ngay sau khi cài đặt cần tiến hành khai báo chìa khoá bí mật (cùng với khẩu lệnh mở chìa). Để làm điều này, ta khởi động chương trình và chọn Tab "Nhập khoá bí mật". Chìa khoá bí mật có thể được cung cấp bởi một số nguồn khác nhau, thí dụ:

• Do người dùng tự sinh cho mình (theo quy trình được hướng dẫn riêng);

• Được cung cấp bởi một cơ quan cung cấp chứng thực điện tử có thẩm quyền (CA);

Chìa khoá bí mật được lưu dưới dạng một file (có đuôi .pvk - private key) và ta cần nhấn chuột vào nút "chọn" để tìm đến thư mục lưu trữ file đó. Sau khi đã khai báo file lưu chìa khoá bí mật, ta cần khai báo mật khẩu mở chìa (đây là một "câu thần chú" mà chỉ duy nhất người sở hữu khoá được biết, và không được phép quên hay nhầm lẫn).

Chìa khoá bí mật được lưu trong chương trình dưới dạng mã và không ai có thể nhìn thấy nó (kể cả khi biết mã nguồn của chương trình). Muốn có được thông tin về nó thì phải biết được mật khẩu mở chìa. Mật khẩu mở chìa khoá bí mật hoàn toàn có thể thay đổi được theo nhu cầu của người chủ sở hữu chìa bí mật đó.

Tiếp theo, cần khai báo danh mục các chìa khoá công khai (của các đối tác cần kiểm tra). Chìa khoá công khai cũng được lưu dưới dạng một file (có đuôi .pbk - public key) và được nhập không hạn định. Chương trình cung cấp các tác vụ như là: xem các thông tin của một khoá công khai như tên người được cấp, ngày cấp,... đổi chìa khoá công khai khác, thêm một khoá công khai của đối tác vào danh sách, xoá 1 khoá khỏi danh sách, xoá tất cả các khoá trong danh sách, ghi thông tin của một khoá công khai ra file (để trao đổi với các đối tác khác).

Sử dụng chương trình

Ký và xác minh chữ ký đối với văn bản word đang mở:

Xuất phát từ thực tế là hiện nay hầu hết các văn bản điện tử của chúng ta được tạo ra trên chương trình MS Word, chúng tôi cố gắng đưa ra một giao diện làm việc đơn giản và thuận tiện tối đa đối với môi trường này. Ngay sau khi chương trình được cài đặt, biểu tượng công cụ "Chữ ký số" được nhúng sẵn vào trong môi trường Word. Văn bản đang mở được ký bằng thao tác nhấn chuột vào biểu tượng "Chữ ký số", sẽ hiện ra giao diện làm việc, chỉ bằng động tác đơn giản là khai báo mật khẩu mở chìa khoá rồi nhấn vào nút "Ký văn bản" là công việc hoàn tất trong giây lát. Việc xác minh chữ ký của một văn bản word (đang được mở) cũng đơn giản tương tự. Điểm khác nhỏ là ta cần phải cho hiển thị Tab "Xác minh chữ ký" và chọn chìa khoá công khai của người đã ký (thay vì khai báo khẩu lệnh mở chìa).

Ký văn bản điện tử bất kỳ

Ta có thể ký và xác minh chữ ký của một file dữ liệu bất kỳ (file âm thanh, file ảnh, file PDF,...) bằng cách kích hoạt chương trình từ Start Menu của Windows và sau đó tiến hành khai báo tên và địa chỉ file cần ký, tên và địa chỉ của file lưu chữ ký vào các ô tương ứng trong giao diện (dựa vào nút "chọn" có sẵn trong giao diện). Sau khi khai báo xong, ta đưa vào mật khẩu mở chìa rồi nhấn vào nút "Ký văn bản" là công việc hoàn tất trong giây lát. Thủ tục kiểm tra chữ ký cũng được tiến hành tương tự.

3. KẾT LUẬN

So với thủ tục ký thông thường (trên văn bản giấy), thủ tục ký điện tử có những ưu thế vượt trội. Nếu như trong môi trường văn bản giấy tờ thông thường các thuộc tính của "chữ ký tay" còn phần nào mang tính "lý tưởng" mà chưa "hiện thực" thì, ngược lại, các thuộc tính này là "hiển nhiên" đối với các "chữ ký số" trên môi trường văn bản điện tử. Hơn thế, trong khi việc kiểm định chữ ký viết tay, con dấu giả,... là không đơn giản (vì thường đòi hỏi phương tiện kỹ thuật đặc biệt) thì chữ ký số có thể được kiểm định một cách dễ dàng và chính xác. Mọi sự giả mạo, gian lận vì thế đều bị phát hiện tức khắc. Tóm lại, bằng việc

triển khai giải pháp ký điện tử ta có thể nói lời kết thúc cho các loại văn bằng chứng chỉ giả, mở đường cho các dịch vụ giao dịch trực tuyến với độ tin cậy cao.

Một mô hình tổng quát hơn, dưới dạng một máy chủ LINUX cung cấp dịch vụ ký điện tử và xác minh chữ ký cho nhiều người làm việc đồng thời trên mạng cũng đã được chúng tôi thiết lập, dành cho đối tượng người dùng nâng cao, và không được đề cập ở đây.

TÀI LIỆU THAM KHẢO

[1] W. Diffie, M. E. Hellman, New directions in cryptography, *IEEE Transaction on Information Theory* Vol. **IT-22** (6) (1976) 644–654.

[2] R. Rivest, A. Sharmir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communication of the ACM* **21** (1978) 120–126.

[3] V. Miller, Uses of elliptic curves in cryptography, *Advances in Cryptology - Crypto '85*, Springer-Verlag, 1986 (417–426).

[4] N. Koblitz, Elliptic curves cryptosystems, *Math. Comp.* **48** (1987) 203–209.

[5] Phạm Huy Điển, Hà Huy Khoái, *Mã hóa thông tin: Cơ sở Toán học và ứng dụng*, NXB Đại học Quốc gia Hà Nội, 2004.

Nhận bài ngày 07 - 3 - 2005
Nhận lại sau sửa ngày 18 - 8 -2005