Mục lục

MỞ ĐẦU

1. Tổng quan tình hình nghiên cứu thuộc lĩnh vực đề tài

Mật mã học là một trong những vấn đề quan trọng trong lĩnh vực bảo mật và an toàn thông tin. Trên thế giới, mật mã học đã được ra đời từ thời La Mã cổ đại và ngày càng được phát triển đạt được những thành tựu to lớn. Trong mật mã học, vấn đề bảo mật luôn đi đôi với vấn đề xác thực thông tin, đặc biệt trong hệ thống mã hóa khóa công khai vấn đề xác thực là vô cùng quan trọng. Để giải quyết vấn đề trên người ta đưa ra một cách giải quyết hiệu quả, đó là chữ ký số.

Với sự bùng nổ của mạng Internet hiện nay, mạng máy tính đang ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của toàn xã hội, và khi nó trở thành phương tiện điều hành các hệ thống thì nhu cầu bảo mật thông tin được đặt lên hàng đầu. Việc sử dụng chữ ký số là một giải pháp hữu hiệu, ngày càng được ứng dụng nhiều trong thực tế, không chỉ giới hạn trong ngành công nghệ thông tin, mật mã học mà còn được áp dụng nhiều trong những lĩnh vực khác như ngân hàng, viễn thông…

Mật mã khóa công khai tạo ra chữ ký số và ứng dụng vào các tài liệu. Hệ mã hóa RSA – hệ mã hóa điển hình của mật mã công khai cùng với hàm băm một chiều chính là những công cụ chính trong việc tạo ra chữ ký số điện tử. Trong báo cáo này, chúng em chủ yếu tập trung vào sơ đồ chữ ký số RSA và ứng dụng của nó lên hóa đơn điện tử.

2. Lý do chọn đề tài

Xuất phát từ thực tế ngày 12/9/2018 chính phủ ban hành nghị định số 119/2018/NĐ-CP về "QUY ĐỊNH VỀ HÓA ĐƠN ĐIỆN TỬ KHI BÁN HÀNG HÓA, CUNG CẤP DỊCH VỤ" tại khoản 2 điều 35 của nghị định thì đã quy định lộ trình chuyển toàn bộ từ hóa đơn giấy sang hóa đơn điện tử hạn cuối là đến năm 2020. Căn cứ theo Công văn số 2402/BTC-TCT ngày 23/02/2016, trên hóa đơn điện tử không yêu cầu phải có chữ ký số của người mua hàng nhưng bắt buộc phải có chữ ký số của người bán. Từ thực tiễn nêu trên nhận thấy tính quan trọng, thiết thực nên nhóm tác giả đã muốn làm rõ nội dung, lợi ích mà chữ ký số và hóa đơn điện tử mang lại.

3. Mục tiêu đề tài

Trong nghiên cứu này chúng em muốn làm rõ nội dung, cơ chế hoạt động của chữ ký số . Để từ đó có cái nhìn tổng quan hơn về công nghệ này và ứng dụng nó vào hóa đơn điện tử.

Trong thời kỳ cách mạng công nghiệp 4.0 và các dữ liệu mã nguồn mở rất sẵn có như hiện nay, trang bị cho bản thân kiến thức về chữ ký số là điều nên làm.

4. Phương pháp nghiên cứu

Nghiên cứu lý thuyết kết hợp các ví dụ, các công cụ có sãn để có cách nhìn nhận trực quan hơn.

5. Hướng nghiên cứu:

+ Nghiên cứu lý thuyết về các đặc điểm của chữ ký tay và chữ ký số.

+ Thử nghiệm một số ứng dụng mô tả quá trình mã hóa và giải mã.

6. Cấu trúc báo cáo

Chương 1: Tổng quan về chữ ký số.

Chương 2: Chữ ký số RSA.

Chương 3: Hóa đơn giấy và hóa đơn điện tử.

Chương 4: Sản phẩm thử nghiệm.

Chương 5: Kết luận.

CHƯƠNG 1: TỔNG QUAN VỀ CHỮ KÝ SỐ

1.1. Giới thiệu chung

Trong đời sống hàng 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" các nội dung trong văn bản. Chẳng hạn như trên việc ký vào phiếu nhận tiền từ ngân hàng, hợp đồng mua bán, chuyển nhượng, thừa kế, tố tụng…. Chữ ký viết tay được chính tay người ký nên không thể sao chụp được. Thông thường chữ ký viết tay trên văn bản thì được dùng để xác nhận người ký nó. Những yếu tố nào làm nên "sức thuyết phục của nó" ? Về mặt lý tưởng thì:

- Chữ ký là bằng chứng thể hiện người ký có chủ định khi ký văn bản.

- Chữ ký thể hiện "chủ quyền", nó làm cho người nhận văn bản biết rằng ai đích thị là người đã ký văn bản.

- Chữ ký không thể "tái sử dụng", tức là nó là một phần của văn bản mà không thể sao chép sang các văn bản khác.

- Văn bản đã ký không thể thay đổi được.

- Chữ ký không thể giả mạo và cũng là thứ không thể chối bỏ (người đã ký văn bản không thể phủ định việc mình đã ký văn bản và người khác không thể tạo ra chữ ký đó).

Trong cuộc sống đời thường, việc tạo một mô hình "lý tưởng" như trên là không dễ vì việc ký trên văn bản giấy có thể giả mạo chữ ký, nhưng với khả năng kiểm định sát sao thì việc làm thay đổi không phải dễ. Tuy nhiên trong thế giới máy tính thì vấn đề ký như trong thực tế sẽ gặp phải nhiều khó khăn: các dòng thông tin trên máy tính có thể thay đổi dễ dàng, hình ảnh của chữ ký tay của một người cũng dễ dàng cho "sang – truyền" từ một văn bản này sang một văn bản khác, và việc thay đổi nội dung một văn bản điện tử (sau khi ký) cũng chẳng để lại dấu vết gì về phương diện "tẩy, xóa"…

Để có được những đặc tính như trên, giao thức "ký trong thế giới điện tử" cần phải có sự hỗ trợ của công nghệ mã hóa. Sơ đồ chữ ký số là phương pháp ký một

thông báo được lưu dưới dạng điện tử. Giao thức cơ bản của chữ ký số dựa trên ý tưởng của Diffie và Hellman:

- Người gửi (chủ nhân của văn bản) ký văn bản bằng cách mã hóa nó với khóa bí mật của mình.

- Người gửi chuyển văn bản đã ký cho người nhận.

- Người nhận văn bản kiểm tra chữ ký bằng việc sử dụng chìa khóa công khai của người gửi để giải mã văn bản.

1.2. Khái niệm về chữ ký số

Chữ ký số (khóa công khai) là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật và qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật. Khóa công khai thường được phân phối thông qua chứng chỉ khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký.

Các thuật toán chữ ký số cho phép xác định nguồn gốc, bảo đảm tính toàn vẹn của dữ liệu được truyền đi, đồng thời nó cũng bảo đảm tính không thể phủ nhận của thực thế đã ký thông tin.

1.3. So sánh chữ ký số với chữ ký thông thường (chữ ký viết tay) trên văn bản

Chữ ký số và chữ ký thường có nhiều điểm khác nhau:

- Về tài liệu được ký: Với tài liệu thông thường, nó là một phần vật lý của tài liệu. Ngược lại, chữ ký số không phải theo kiểu vật lý gắn vào thông báo nên không nhìn thấy trên bức điện.

- Về vấn đề kiểm tra chữ ký: Chữ ký thông thường được kiểm tra bằng cách so sánh nó với các chữ ký xác thực khác (chữ ký mẫu). Điểm yếu của chữ ký thông thường là không an toàn, và dễ có thể giả mạo. Ngược lại, chữ ký số lại được kiểm tra nhờ dùng thuật toán kiểm tra công khai, bất kỳ ai cũng có thể kiểm tra được. Việc dùng một sơ đồ chữ ký an toàn có thể ngăn chặn được giả mạo.

1.4. Vị trí, vai trò của chữ ký số

- Xu hướng quốc tế hóa và toàn cầu hóa đã và đang ảnh hưởng đến sự phát triển của thế giới. Việc trao đổi thông tin cũng từ đó yêu cầu nhanh gọn, chính xác và đặc biệt là

phải an toàn. Việc trao đổi thông tin, chứng thực thông tin theo phong cách truyền thông làm giảm tốc độ, cũng như sự chính xác của thông tin. Những công việc đó mang tính chất thủ công gây ra sự chậm chễ và thiếu chính xác trong trao đổi.

- Chính khó khăn đã nảy sinh sự phát triển mạnh mẽ của công nghệ thông tin và công nghệ mã hóa. Hiện nay, ở tất cả các nước phát triển cũng như đang phát triển, mạng máy tính đang ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực hoạt động của toàn xã hội và nhu cầu bảo mật thông tin được đặt lên hàng đầu. Điển hình là việc mã hoá bảo mật các thông tin số của doanh nghiệp, dùng chữ ký số xác thực email trao đổi thông tin, kiểm soát truy cập vào các sàn thương mại điện tử và các đơn đặt hàng, ngân hàng điện tử, mua sắm trực tuyến... mà vai trò chủ yếu là chữ ký số điện tử.

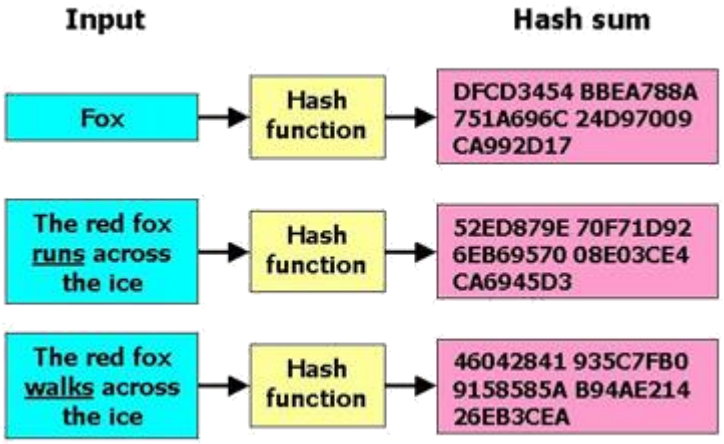
- Trên thực tế, chữ ký số không chỉ được thực hiện cho các giao dịch điện tử trên mạng internet mà còn qua hệ thống mạng viễn thông di động. Đặc biệt, hiện nay nhiều nước trên thế giới không chỉ triển khai ứng dụng chữ ký số trên mạng máy tính mà còn áp dụng trên mạng điện thoại di động để thực hiện các giao dịch điện tử. Hướng đi này giúp đẩy nhanh giao dịch, đơn giản hoá mua sắm trực tuyến và giúp người dùng có thể truy cập mọi lúc, mọi nơi.

- Sự ra đời của chữ ký số khẳng đinh được lợi ích to lớn về chiến lược và kinh tế, đồng thời các vấn đề liên quan đến chữ ký số cũng là nhưng chủ đề quan trọng nhất của mật mã học.

1.5. Hàm băm mật mã

a. Hàm băm

Hàm băm là một giải thuật nhằm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu. Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu.



Hình 1.2

Hàm hash là một hàm số toán học (mathematical function) ánh xạ (mapping) từ dữ liệu có độ dài bất kỳ (arbitrary size) thành dữ liệu có độ dài cố định (fixed size).

Một giá trị hash (hash value) là một chuỗi ký tự gồm số và chữ đi kèm với nhau. Hashing là quá trình diễn ra một chiều, có nghĩa là không thể dịch ngược được. Khi có một giá trị hash, người đó không thể tìm được dữ liệu đầu vào ban đầu.

SHA-256:

SHA-256 là một nhánh của thuật toán băm SHA-2. Nó tạo ra một mã băm có kích thước cố định 256 bit (32-byte) gần như là duy nhất.

VD: Hai chuỗi sau sử dụng SHA-256 sẽ cho giá trị băm khác nhau:

- Hash của chuỗi ‘abc’ là:

ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

- Hash của chuỗi ‘abC’, sau khi đổi 1 kí tự c thành C cũng cho giá trị khác nhau:

0a2432a1e349d8fdb9bfca91bba9e9f2836990fe937193d84deef26c6f3b8f76

1.6. Các hệ mật mã

Mật mã khóa bí mật (secret key cryptosystem) hay hệ mật mã đối xứng là hệ mật mã mà trong đó việc lập mã và giải mã cùng sử dụng chung một khóa.

Mật mã khóa công khai (public key cryptosystem) hay hệ mật mã phi đối xứng là hệ mật mã mà trong đó việc lập mã và giải mã sử dụng 2 chìa khóa riêng biệt, từ chìa khóa này không thể tìm ra chìa khóa kia và ngược lại.

Mật mã có vai trò rất quan trọng, đặc biệt là trong giao dịch điện tử. Nó giúp đảm bảo bí mật, toàn vẹn của thông tin, khi thông tin đó được truyền trên mạng. Mật mã cũng là nền tảng của kĩ thuật chữ ký điện tử, hệ thống PKI...

1.7. Mật mã khóa bí mật (mã hóa khóa đối xứng) và những hạn chế:

Sử dụng thuật toán mã hóa đối xứng - giải thuật giải mã ngược với giải thuật tạo bản mã, cả 2 giải thuật dùng chung một khóa (Secret key). Khóa được dùng chung giữa bên gửi và bên nhận nên tồn tại một số điểm yếu:

- Vấn đề phân phối khóa khó bảo đảm chia sẻ mà không làm tiết lộ, hoặc trung tâm phân phối khóa có thể bị tấn công.

- Yêu cầu để tạo chữ ký số là phải bí mật chỉ người dùng duy nhất có khóa để tạo chữ ký nên mã hóa đối xứng không được áp dụng cho lĩnh vực chứ ký số.

1.8. Mật mã khóa công khai

Khắc phục điểm yếu của mã hóa khóa đối xứng với những đặc điểm nói trên, giải thuật mã hóa khóa công khai sử dụng 2 khóa khác nhau:

* Một khóa công khai.

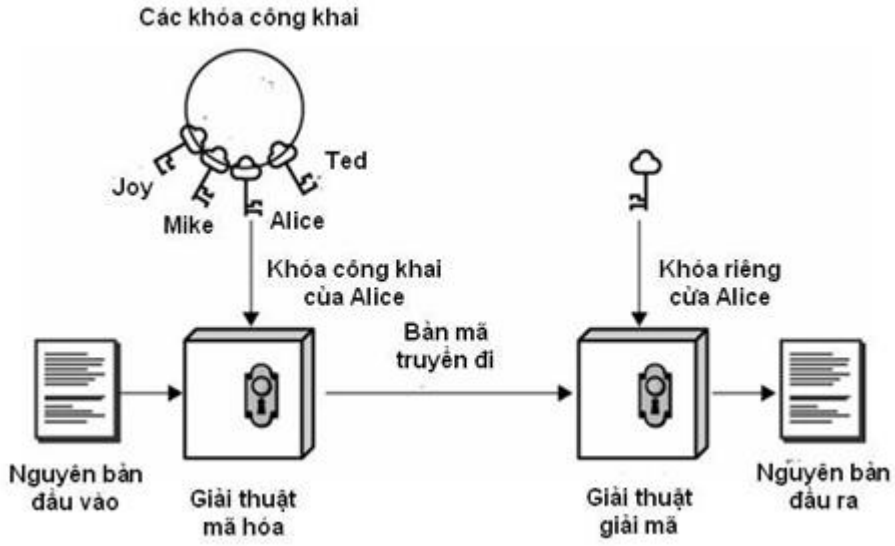
- Ai cũng có thể biết.

- Dùng để mã hóa thông báo và thẩm tra chữ ký.

* Một khóa riêng

- Chỉ nơi giữ được biết.

- Dùng để giải mã thông báo và ký chữ ký.



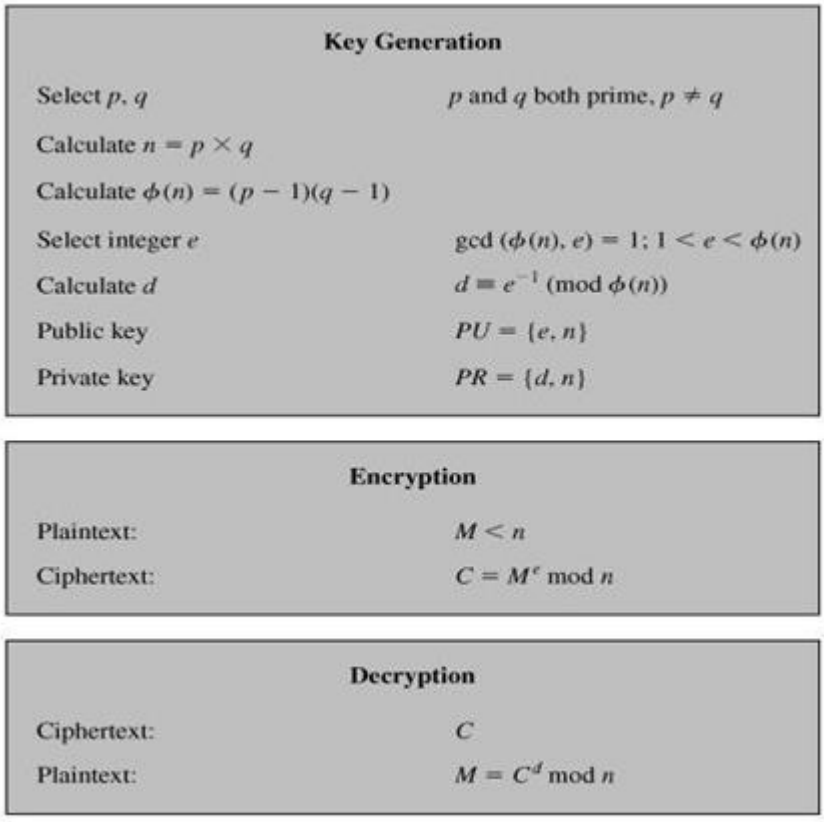
Hình 1.3 Mô hình của mật mã khóa công khai

1.9. Hệ mật mã RSA

Trong mật mã học, RSA là một thuật toán mật mã khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa bảo mật. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn .

Thuật toán RSA có hai khóa: khóa công khai (hay khóa công cộng) và khóa bí mật (hay khóa cá nhân). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa.

Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được.



Hình 1.4 Thuật toán mã hóa RSA

Hệ mã hóa khóa công khai với đầu vào là một khối số nguyên < n. Qui trình thực hiện gồm 3 bước: tạo khóa, tạo bản mã và giải mã.

Quá trình tạo khóa trong RSA:

Một cặp khóa công khai – khóa riêng được thực hiện theo các bước sau :

- Chọn ngẫu nhiên 2 số tự nhiên đủ lớn p, q (p khác q)
- Tính n = p x q
- Tính Φ(n) = (p-1)(q-1)
- Chọn ngẫu nhiên khóa mã hóa e sao cho 1 < e < Φ(n) và gcd(e, Φ(n)) = 1
- Tìm khóa giải mã d <= n thỏa mã e.d ≡ 1 mod (n)
- Công bố khóa mã hóa công khai KU = {e, n}
- Giữ bí mật khóa giải mã riêng KR = {d, n}
- Hủy bỏ các giá trị bí mật

Quá trình mã hóa:

Để mã hóa 1 thông báo nguyên bản M, bên gửi thực hiện (M < n)

- Lấy khóa công khai của bên nhận KU = {e, n}
- Tính $C = M^e \bmod n$ ➔ C là bản mã thu được

Quá trình giải mã:

Để giả mã bản mã C nhận được, bên nhận thực hiện

- Sử dụng khóa riêng KR = {d, n}
- Tính $M = C^d \bmod n$

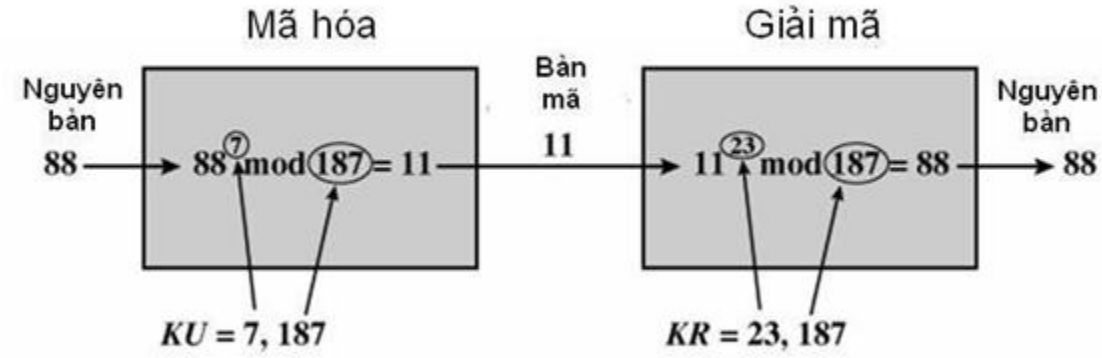
Tính đúng đắn của RSA:

Theo định lý Euler, a, n: gcd(a, n) = 1 ➔ $a^{(n)} \bmod n = 1$ và (n) là số các số nguyên tố nguyên dương nhỏ hơn n và nguyên tố cùng nhau của n.

Đối với RSA có :

n = p x q với p, q là các số nguyên tố

- $\Phi(n) = (p - 1)(q-1)$
- $ed \equiv 1 \bmod (n)$
- $M < n$
- Có thể suy ra $C^d \bmod n = M^{ed} \bmod n = M \bmod n = M$



Hình 1.5 Ví dụ RSA

Độ an toàn của RSA:

Độ an toàn của hệ thống RSA dựa trên 2 vấn đề của toán học: bài toán phân tích ra thừa số nguyên tố các số nguyên lớn và bài toán RSA. Với việc phân tích thừa số nguyên tố, giả sử khóa có độ dài 128 bit là một số giữa 1 và một số rất lớn:

340.282.366.920.938.000.000.000.000.000.000.000.000 ➔ Có khoảng ≈ n / ln(n) =2128 / ln(2128) ≈ 3.835.341.275.459.350.000.000.000.000.000.000.000.000 số nguyên tố giữa 1 và số này. Giả sử nếu mỗi giây có thể tính được 1012 số ➔ Cần hơn 121,617,874,031,562,000 năm (khoảng 10 triệu lần tuổi của vũ trụ) để tìm ra khóa.

Phá mã RSA :

- Phương pháp vét cạn: Thử tất cả các khóa riêng có thể ➔ Phụ thuộc vào độ dài khóa và gần như không thể.
- Phương pháp phân tích toán học: Phân tích n thành 2 thừa số nguyên tố p và q. Như trên ta đã nói việc phân tích một số ra số nguyên tố là rất khó khăn, với tốc độ của máy tính hiện nay cũng không thể đáp ứng được việc phân tích số nguyên tố lớn trong thời gian đa thức nếu các số p, q được chọn là lớn.
- Xác định trực tiếp Φ(n) không thông qua p và q
- Xác định trực tiếp d không thông qua Φ(n)
- Phương pháp phân tích thời gian: Dựa trên việc đo thời gian giải mã. Đây là một cách dựa vào thời gian giải mã. Phương pháp phân tích thời gian có thể loại bỏ bằng cách làm nhiễu bằng cách cho thời gian giải mã của thông báo bất kỳ là gần như không đổi.

1.10. Hạn chế của khóa công khai

- Tốc độ xử lý: Các giải thuật khóa công khai chủ yếu dùng các phép nhân chậm hơn nhiều so với các giải thuật đối xứng ➔ Không thích hợp cho mã hóa thông thường
- Thường dùng trao đổi khóa bí mật đầu phiên truyền tin.
- Tính xác thực của khóa công khai: Bất cứ ai cũng có thể tạo ra một khóa công bố đó là của một người khác ➔ Chừng nào việc giả mạo chưa bị phát hiện có thể đọc được nội dung các thông báo gửi cho người kia. Cần đảm bảo những người đăng ký khóa là đáng tin.

Nhận xét:

Hệ mã hóa RSA là một công cụ chính trong việc tạo ra chữ ký số. Qua việc trình bày ở trên ta thấy được sự an toàn cũng như cách tránh tấn công vào hệ mã hóa RSA.

CHƯƠNG 2: CHỮ KÝ SỐ VÀ CHỮ KÝ SỐ RSA

Chương này sẽ tập trung vào mô hình chữ ký số, trọng tâm là chữ ký số RSA và những ứng dụng của nó. Chữ ký số ra đời chính là nhằm giải quyết những vấn đề chưa giải quyết được của xác thực và toàn vẹn dữ liệu.

2.1. Một số khái niệm và tính chất của chữ ký số

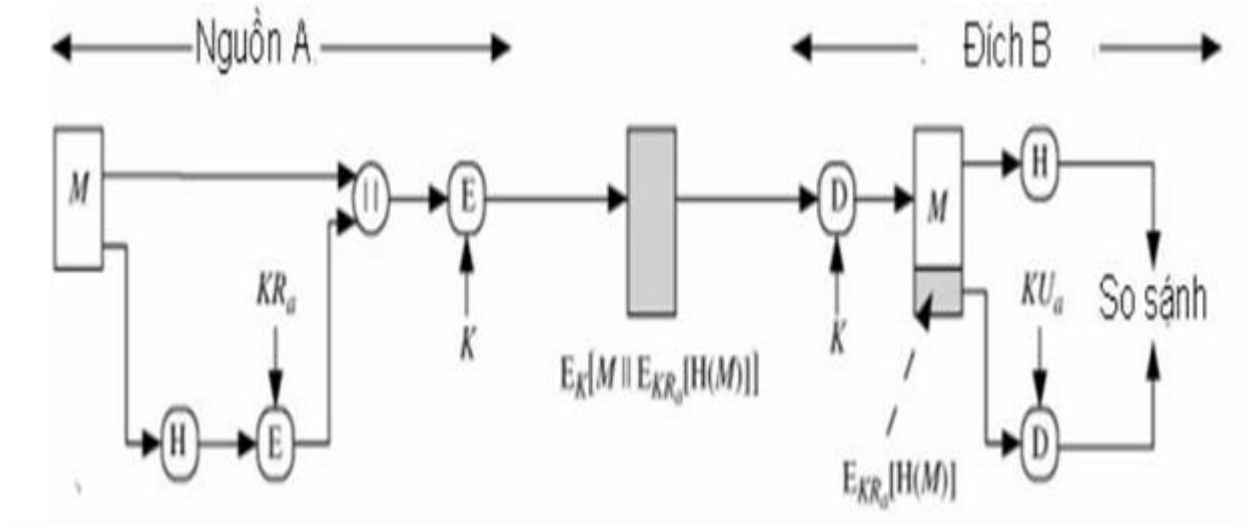
Khái niệm :

Chữ ký số khóa công khai là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật và qua đó có thể ký các văn bản điện tử. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký.

Chức năng chữ ký số:

- Xác minh tác giả và thời điểm ký thông tin được gửi.
- Xác thực nội dung thông tin gửi.
- Là căn cứ để giải quyết tranh chấp – không thể từ chối trách nhiệm.

Giao thức của chữ ký số bao gồm thuật toán tạo chữ ký số và thuật toán để kiểm tra chữ ký số.



Hình 2.1

Minh họa chữ ký số của bên gửi cho thông báo M

KRa, KUa: khóa bí mật và công khai của bên A

K: khóa phiên đối xứng dùng chung của A và B

M: thông báo gửi

H: hàm băm

E: Mã hóa

D: Giải mã

2.2.1. Các bước tạo và kiểm tra chữ ký điện tử

Bên gửi A thực hiện băm thông điệp cần gửi bằng hàm băm H, rồi mã giá trị vừa được băm này bằng mật mã khóa công khai với khóa bí mật của bên A là KRa, phần thông tin này chính là chữ ký xác thực của người dùng A đối với thông điệp M gửi đi.

A gửi cho B văn bản và chữ ký (Thông điệp có thể được mã hóa hoặc không mã hóa tùy theo yêu cầu. Như hình vẽ trên chữ ký được gắn liền với thông điệp rồi mã hóa bằng mật mã đối xứng với khóa dùng chung K giữa A và B).

B nhận được thông điệp (hoặc bản mã rồi giải mã với khóa chung K để lấy thông điệp) thì tiến hành 2 việc : băm giá trị của thông điệp bằng hàm băm H, giải mã chữ ký bằng khóa công khai KUa của bên gửi rồi so sánh 2 giá trị vừa tính toán được. Nếu 2 giá trị này trùng khớp thì chúng tỏ thông điệp nhận được có nội dung không thay đổi so với khi ký.

2.2.2. Lược đồ chữ ký số

Khi đề cập đến 1 lược đồ chữ ký số, người ta luôn phải đề cập đến 4 thuật toán sau:

Thuật toán khởi tạo tham số của hệ thống:

Là một thuật toán ngẫu nhiên nhận đầu vào là một tham số bảo mật k (k còn được gọi là độ dài bảo mật) và đưa ra các tham số chung cho hệ thống. Thuật toán này thường được tiến hành bởi server của hệ thống.

Ví dụ: Với RSA là việc chọn ngẫu nhiên các số nguyên tố lớn p & q, tính toán n...

Thuật toán sinh khóa:

Đây là thuật toán sinh ngẫu nhiên, được tiến hành bởi người dùng trong hệ thống. Thuật toán nhận đầu vào gồm các tham số của hệ thống và sinh ra cặp khóa bí mật/công khai.

Ví dụ: Với RSA : d, e.

Thuật toán sinh chữ ký số:

Thuật toán này nhận đầu vào là một tin nhắn/tài liệu, sinh ra một chữ ký số nhờ vào khóa bí mật.

Thuật toán xác thực chữ ký số:

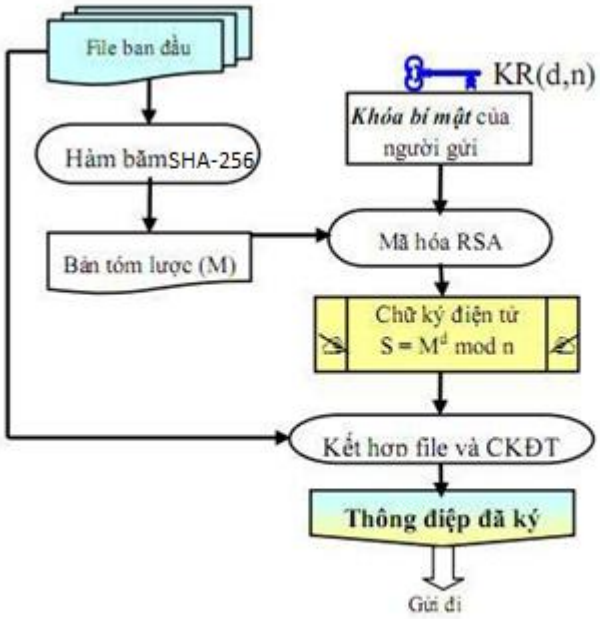
Thuật toán này được tiến hành bởi một người thứ ba khi muốn kiểm tra tính đúng đắn của một chữ ký số. Thuật toán nhận đầu vào là 1 tin nhắn, chữ ký số của tin nhắn đó và khóa công khai của người sở hữu tin nhắn & chữ ký số, đầu ra của thuật toán là câu trả lời "đúng" hoặc "sai". Thuật toán này là thuật toán đơn định.

2.3. Một số mô hình chữ ký số trong thực tế

Mô hình chữ ký số RSA trong các hệ thống quản lý: Quá trình gửi và nhận các tệp văn bản phục vụ quản lý dựa vào thuật toán băm SHA-256 và thuật toán RSA.

Quá trình ký và gửi các tệp văn bản

Từ file cần gửi ban đầu, chương trình sẽ sử dụng hàm băm SHA-256 để mã hóa thu được chuỗi ký tự dài 256 bit. Chương trình sử dụng thuật toán RSA để mã hóa giá trị băm thu được với khóa riêng của người gửi được một giá trị gọi là chữ ký điện tử. Kết hợp file ban đầu với chữ ký điện tử thành một thông điệp đã ký và gửi đi cho người nhận.



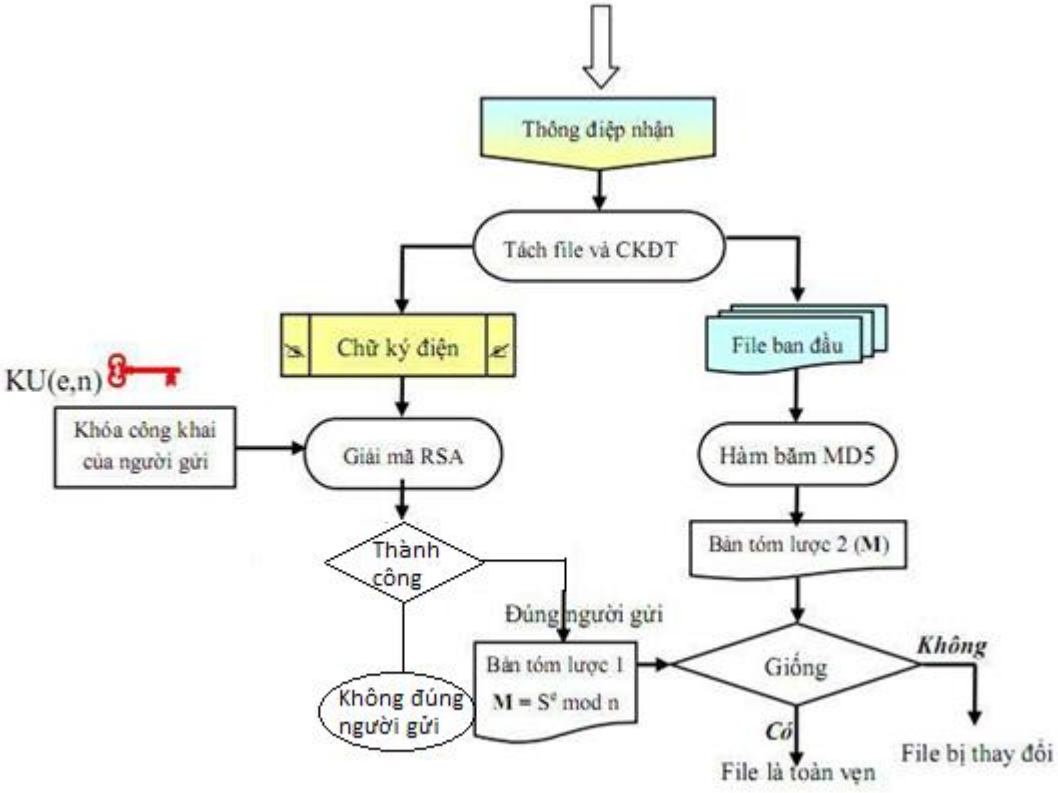
Hình 2.2 : Ký văn bản

Quá trình nhận các tệp văn bản :

Sau khi người nhận nhận được văn bản. Hệ thống sẽ tách thông điệp đã ký ra thành file và chữ ký điện tử. Đến giai đoạn này có 2 quá trình kiểm tra:

- Kiểm tra file có đúng người gửi hay không : Sử dụng thuật toán RSA để giải mã chữ ký điện tử bằng khóa công khai của người gửi. Nếu giải mã thành công thì đúng là người đó gửi và nhận được giá trị băm 1(bản toám lược 1). Nếu giải mã không thành công không phải người đó gửi.

- Kiểm tra file có bị thay đổi hay không :Từ file đuợc tách ra ta sử dụng hàm băm SHA-256 mã hóa thành giá trị băm 2 (bản tóm lược 2). Kiểm tra giá trị băm 1 và giá trị băm 2 có giống nhau hay không? Nếu giống nhau thì file nhận được là toàn vẹn, không bị thay đổi, ngược lại là file đã bị thay đổi (hình vẽ 2.3).



Hình 2.3 Xác thực chữ ký

CHƯƠNG 3: HÓA ĐƠN GIẤY VÀ HÓA ĐƠN ĐIỆN TỬ

3.1. Giới thiệu chung hóa đơn

3.1.1. Hóa đơn là gì?

Hóa đơn là một loại chứng từ thương mại được bên bán cung cấp cho bên mua, trong đó kê khai những thông tin về chủng loại, số lượng, giá thành của loại hàng hóa hoặc dịch vụ được giao cho bên mua. Các điều khoản thanh toán sẽ được ghi cụ thể trong hóa đơn (như thời hạn thanh toán, số dư nợ, chiết khấu, v.v). Nó sẽ được coi là hóa đơn bán hàng với bên bán và hóa đơn mua hàng với bên mua.

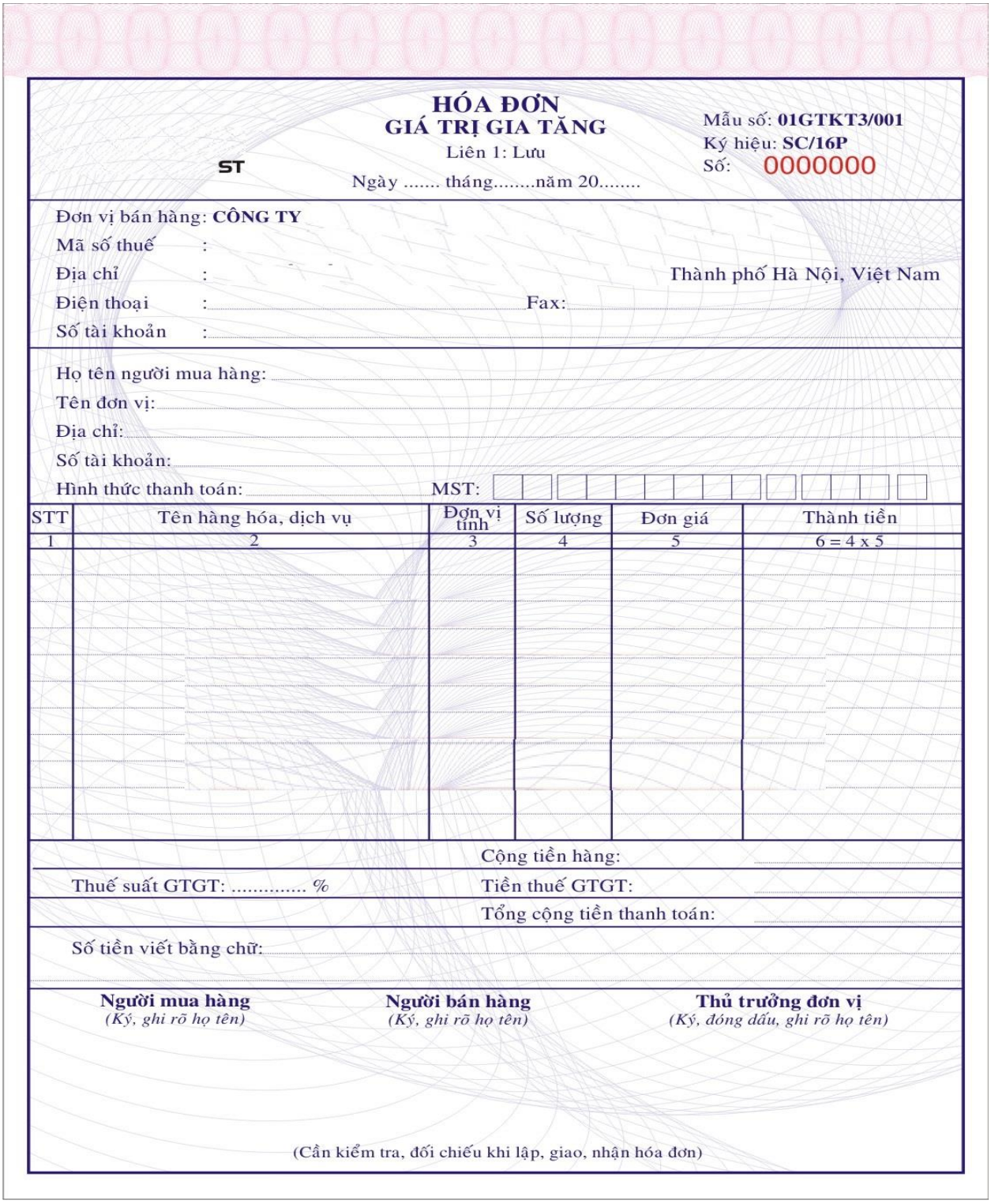
3.1.2. Các loại hóa đơn

Theo Thông tư 39/2014/TT-BTC và Thông tư 119/2014/TT-BTC của Bộ tài chính quy định các loại hóa đơn và hình thức hóa đơn cụ thể như sau:

- Hóa đơn giá trị gia tăng (Hóa đơn có dòng thuế GTGT trên tờ hóa đơn):

Là loại hóa đơn mà khi doanh nghiệp mua hàng hóa hoặc dịch vụ của Công ty tính thuế GTGT theo phương pháp khấu trừ sẽ xuất hóa đơn này cho doanh nghiệp. Và đây là loại hóa đơn tài chính Cơ quan thuế quản lý và các bạn phải báo cáo cho Cơ quan thuế định kỳ hàng quý nên đây là loại hóa đơn tài chính mà thuế chấp thuận được khấu trừ VAT đầu vào (nếu doanh nghiệp tính thuế GTGT theo phương pháp khấu trừ) và được chấp nhận là chi phí được trừ khi quyết toán thuế TNDN.

Mẫu hóa đơn GTGT như sau:



HÓA ĐƠN
GIÁ TRỊ GIA TĂNG
Liên 1: Lưu
ST
Ngày ..... tháng.....năm 20.....

Mẫu số: **01GTKT3/001**
Ký hiệu: **SC/16P**
Số: 0000000

Đơn vị bán hàng: **CÔNG TY**
Mã số thuế :
Địa chỉ : Thành phố Hà Nội, Việt Nam
Điện thoại : Fax:
Số tài khoản :

Họ tên người mua hàng:
Tên đơn vị:
Địa chỉ:
Số tài khoản:
Hình thức thanh toán: MST:

STT	Tên hàng hóa, dịch vụ	Đơn vị tính	Số lượng	Đơn giá	Thành tiền
1	2	3	4	5	6 = 4 x 5

Cộng tiền hàng:
Thuế suất GTGT: ..... % Tiền thuế GTGT:
Tổng cộng tiền thanh toán:

Số tiền viết bằng chữ:

Người mua hàng *(Ký, ghi rõ họ tên)*
Người bán hàng *(Ký, ghi rõ họ tên)*
Thủ trưởng đơn vị *(Ký, đóng dấu, ghi rõ họ tên)*

(Cần kiểm tra, đối chiếu khi lập, giao, nhận hóa đơn)

Hình 3.1 Hóa đơn giá trị gia tăng

- Hóa đơn bán hàng:

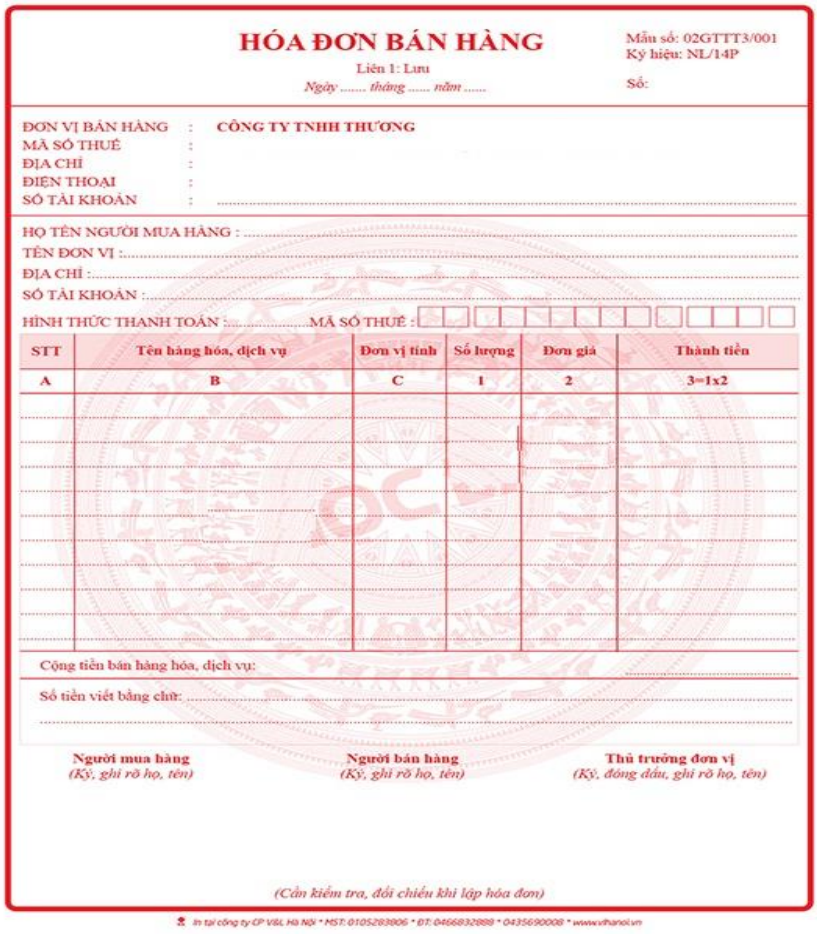
Hóa đơn bán hàng (Hay còn gọi là hóa đơn trực tiếp) trên hóa đơn không có dòng thuế GTGT.

Khi mua hàng hóa dịch vụ của những doanh nghiệp tính thuế GTGT theo phương pháp trực tiếp thì những doanh nghiệp này sẽ xuất hóa đơn trực tiếp cho doanh nghiệp mua;

Hoặc khi mua hàng hóa hoặc dịch vụ của các hộ và cá nhân kinh doanh;

Đây là loại hóa đơn thuế quản lý và các doanh nghiệp cũng phải báo cáo cho cơ quan thuế biết định kỳ hàng quý nên đây là loại hóa đơn tài chính mà thuế chấp thuận là chi phí được trừ khi quyết toán thuế TNDN.

Mẫu hóa đơn bán hàng:



HÓA ĐƠN BÁN HÀNG

Liên 1: Lưu

Ngày ..... tháng ..... năm .....

Mẫu số: 02GTTT3/001
Ký hiệu: NL/14P
Số:

ĐƠN VỊ BÁN HÀNG : CÔNG TY TNHH THƯƠNG
MÃ SỐ THUẾ :
ĐỊA CHỈ :
ĐIỆN THOẠI :
SỐ TÀI KHOẢN :

HỌ TÊN NGƯỜI MUA HÀNG :
TÊN ĐƠN VỊ :
ĐỊA CHỈ :
SỐ TÀI KHOẢN :
HÌNH THỨC THANH TOÁN : MÃ SỐ THUẾ :

STT	Tên hàng hóa, dịch vụ	Đơn vị tính	Số lượng	Đơn giá	Thành tiền
A	B	C	1	2	3=1x2

Cộng tiền bán hàng hóa, dịch vụ:

Số tiền viết bằng chữ:

Người mua hàng	Người bán hàng	Thủ trưởng đơn vị
(Ký, ghi rõ họ, tên)	(Ký, ghi rõ họ, tên)	(Ký, đóng dấu, ghi rõ họ, tên)

(Cần kiểm tra, đối chiếu khi lập hóa đơn)

In tại công ty CP VBL Hà Nội * MST: 0105283906 * ĐT: 0466832889 * 0435690008 * www.vhanoi.vn

Hình 3.2 Hóa đơn bán hàng

- Phiếu thu tiền cước vận chuyển hàng không; chứng từ thu cước phí vận tải quốc tế; chứng từ thu phí dịch vụ ngân hàng… hình thức và nội dung được lập theo thông lệ quốc tế và các quy định của pháp luật có liên quan.

Khi doanh nghiệp mua hàng hóa hoặc dịch vụ của vận chuyển hàng không (ví dụ như mua vé máy bay), hoặc phí dịch vụ ngân hàng thì sẽ được những hóa đơn đặc thù mà không có tên là hóa đơn GTGT hoặc hóa đơn bán hàng . Nhưng đây cũng chính là hóa đơn tài chính và thuế quản lý cũng như định kỳ phải báo cáo cho cơ quan thuế nên sẽ được chấp thuận là chi phí được trừ khi quyết toán thuế TNDN Và chấp thuận được khấu trừ VAT đầu vào (nếu công ty của các bạn tính thuế GTGT theo phương pháp khấu trừ).

Mẫu phiếu thu cước:

Vietnam Airlines

Nơi xuất vé (Issuing Office): CTY CP EN VIET
Địa chỉ (Address): 69B Nguyen Huu Dat, P. Tay Thanh, Q. Tan Phu, TP.HCM

Mẫu số (Form No): 01GTKT3/004
Ký hiệu (Serial): HK/11T
Số hóa đơn (Invoice No): 0091829

HÓA ĐƠN - PHIẾU THU TIỀN CƯỚC VẬN CHUYỂN
(SALES INVOICE/ RECEIPT)

Liên 2 : Giao cho khách (Copy 2 for Customer)

Tổng công ty Hàng không Viet Nam (Vietnam Airlines)
Mã số thuế (Vat Code) : 0100107518

Tên khách hàng (Customer):CÔNG TY TNHH HỖ TRỢ PHÁT TRIỂN PHẦN MỀM LUẬT VIỆT
Mã số thuế (VAT Code): 0401317822
Địa chỉ (Address):04 TRẦN QUANG DIỆU
1. Tiền vé (Due to VietNam Airlines):
1.1 Giá cước (Air fare):

Số vé (Ticket No)	Hành trình (Route)	Số lượng (Quantity)	Đơn giá (Unit price)	Thành tiền (Amount)	Loại tiền (Currency)
7382420567490	DADVNHAN	1	500.000	500.000	VND
1.2 Thuế GTGT (Value Added Tax)				50.000	VND
1.3 Thuế Phí khác (Other Tax charge):					
Thuế khác (Other Tax):				44.000	VND
Phí khác (Other charge):					
Hoa hồng (Commission):					
1.4 Tổng tiền vé (1.1+1.2+1.3):				594.000	VND

Tổng số tiền thanh toán (Equivalent amount paid): Tỷ giá 1 — 594.000 VND

Hình thức thanh toán (Form of payment):

CASH — 594.000 VND

Đề nghị quý khách kiểm tra kỹ trước khi rời quầy thu (Please kindly check before leaving)

Khách hàng
(Customer)

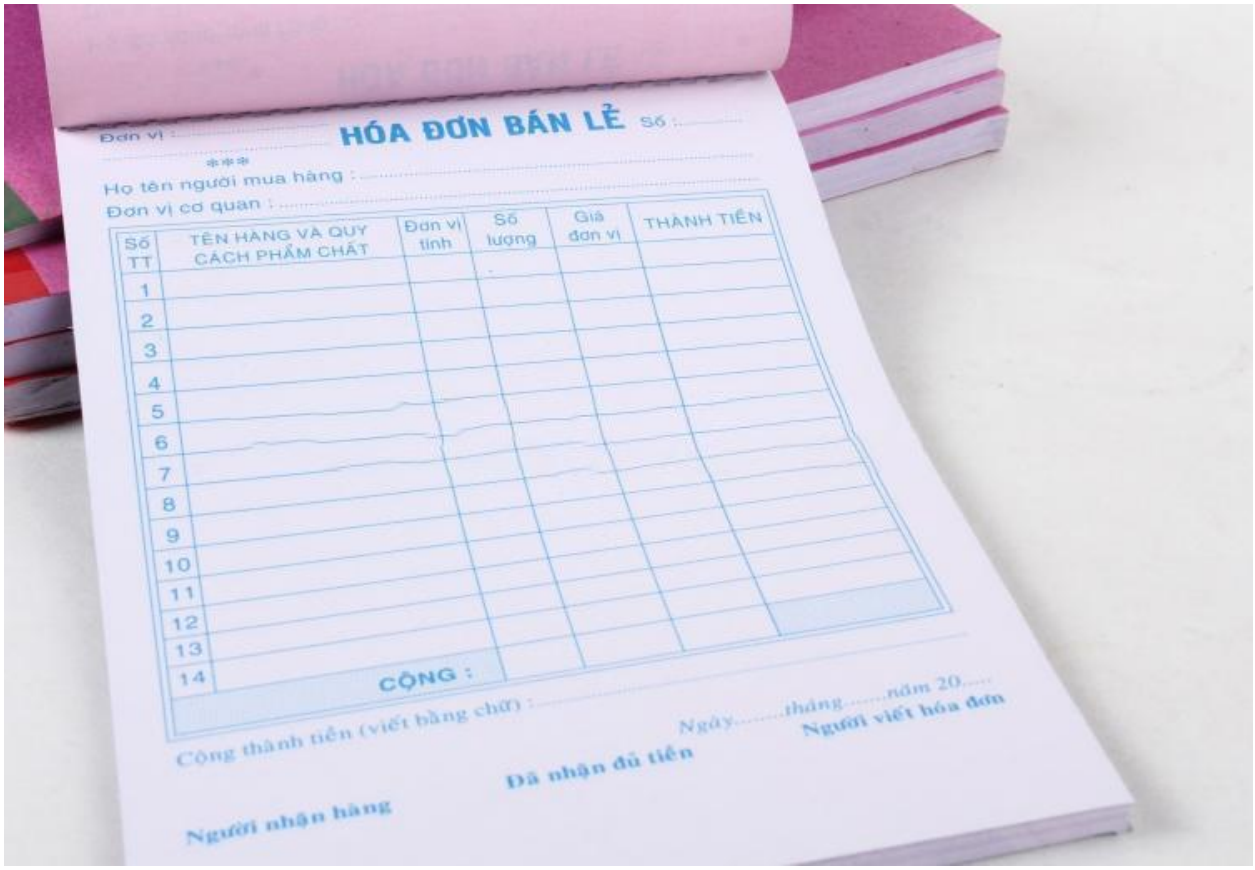
Ngày (Date): 10/05/2011
Người bán hàng
(Salesperson)

Hình 3.3 Phiếu thu

- Hóa đơn lẻ:

Hóa đơn lẻ là loại hóa đơn mà Cơ quan thuế không quản lý hóa đơn này và Các công ty cũng không phải báo cáo hóa đơn này cho Cơ quan thuế. Do thuế không quản lý hóa đơn này nên hóa đơn này sẽ không được thuế chấp thuận là chi phí được trừ khi quyết toán thuế TNDN. Do đó, khi các bạn mua hàng hóa và dịch vụ của các doanh nghiệp thì người đi mua lưu ý là hỏi họ có xuất được hóa đơn tài chính không (Hóa đơn GTGT hoặc hóa đơn bán hàng không)? thì doanh nghiệp mới mua hàng hóa và dịch vụ. Và doanh nghiệp nào khi bán hàng hóa và cung cấp dịch vụ mà sử dụng hóa đơn bán lẻ này để gửi cho khách hàng là doanh nghiệp này đang có hành vi TRỐN THUẾ, GIAN LẬN THUẾ

Mẫu hóa đơn lẻ:



Hình 3.4 Hóa đơn bán lẻ

- Hóa đơn khác gồm: tem, vé, thẻ, phiếu thu tiền bảo hiểm…

Đây là loại hóa đơn đặc thù của những công ty chuyên kinh doanh vận tải hành khách. Và đây là loại hóa đơn mà Cơ quan thuế quản lý và Công ty cũng phải định kỳ báo cáo cho cơ quan thuế, nên đây là loại hóa đơn mà thuế chấp thuận là chi phí được trừ khi

quyết toán thuế TNDN.Và cũng được khấu trừ VAT đầu vào (nếu công ty tính thuế GTGT theo phương pháp khấu trừ)

Hình 3.5 Vé xe

3.2. Những bất cập của hóa đơn giấy

Ở đây nhóm tác giả chỉ tổng kết lại các vấn đề khó khăn, bất cập của hóa đơn giấy từ các nghiên cứu có sẵn:

Hóa đơn giấy còn nhiều bất cập gây ảnh hưởng đến doanh nghiệp và cơ quan thuế: tốn chi phí vận chuyển, in ấn, thủ tục rườm rà, mất nhiều chi phí.

Thủ tục đăng ký hóa đơn rườm rà:

Dưới đây là thủ tục khi doanh nghiệp muốn xin hóa đơn đỏ:

- Doanh nghiệp làm đơn đề nghị xin hóa đơn đỏ.

- Đợi khoảng 7 ngày chờ được phê duyệt.

- Tìm nhà in đủ điều kiện để làm hợp đồng thuê in, làm hồ sơ đặt in…

- Đem mẫu hóa đơn được đăng ký tới xưởng in đặt in một số lượng nhất định để lưu trữ.

Tốn ngân sách và công sức:

Đối với doanh nghiệp: giá in mỗi quyển hóa đơn xê dịch từ khoảng 350.000 đồng – 500. 000 đồng/quyển. Thông thường doanh nghiệp sẽ in 5 – 10 quyển mỗi lần để lưu trữ. Đôi

khi, kế toán làm hóa đơn bị xảy ra sai sót rồi gạch xóa phải làm lại hóa đơn một lần nữa. Như vậy vừa tốn công sức vừa khó khăn trong việc quản lý hóa đơn của cơ quan thuế.

Đối với cơ quan thuế: doanh nghiệp muốn xin hóa đơn đỏ thì cơ quan thuế phải xét duyệt, nếu đủ điều kiện thì gửi hóa đơn qua bưu điện. Với số lượng lớn doanh nghiệp như hiện nay và phải gửi cho từng doanh nghiệp sẽ làm tốn chi phí in giấy và vận chuyển.

Hơn nữa, được làm bằng giấy nên hóa đơn truyền thống dễ bị mất, hư hỏng trong quá trình bảo quản. Nếu làm mất hóa đơn thì phải thực hiện nhiều công đoạn, thủ tục để giải trình chi tiết với cơ quan thuế.

Tình trạng hóa đơn giả:

Ngoài những thủ tục rườm rà, tốn chi phí công sức thì hóa đơn giấy còn một hạn chế lớn khác đó là dễ làm giả hóa đơn giấy. Hóa đơn không còn giá trị sử dụng tràn lan trên thị trường nên nhiều doanh nghiệp lo lắng khi sử dụng hóa đơn giấy. Và hóa đơn giả được các công ty "ma" cung cấp cho các doanh nghiệp trốn thuế, không muốn đóng thuế.

3.3. Hóa đơn điện tử

Hoá đơn điện tử là tập hợp các thông điệp dữ liệu điện tử về bán hàng hoá, cung ứng dịch vụ, được khởi tạo, lập, gửi, nhận, lưu trữ và quản lý bằng phương tiện điện tử. Đặc biệt là hóa đơn điện tử phải được khởi tạo, lập, xử lý trên hệ thống máy tính của tổ chức đã được cấp mã số thuế khi bán hàng hóa, dịch vụ và được lưu trữ trên máy tính của các bên theo quy định của pháp luật về giao dịch điện tử.

Trên hóa đơn điện tử bao gồm những nội dung như:

- Tên hóa đơn, ký hiệu hóa đơn, ký hiệu mẫu, số thứ tự hóa đơn; Ký hiệu hóa đơn, ký hiệu mẫu, số thứ tự trên hóa đơn thực hiện theo quy định tại Phụ lục số 1 Thông tư số 153/2010/TT-BTC của Bộ Tài chính.

- Tên, địa chỉ, mã số thuế của người bán.

- Tên, địa chỉ, mã số thuế của người mua.

- Tên hàng hóa, dịch vụ; đơn vị tính, số lượng, đơn giá hàng hoá, dịch vụ; thành tiền ghi bằng số và bằng chữ. Đối với hóa đơn giá trị gia tăng, ngoài dòng đơn giá là giá chưa có thuế giá trị gia tăng, phải có dòng thuế suất thuế giá trị gia tăng, tiền thuế giá trị gia tăng, tổng số tiền phải thanh toán ghi bằng số và bằng chữ.

Chữ ký điện tử theo quy định của pháp luật của người bán; ngày, tháng năm lập và gửi hóa đơn. Chữ ký điện tử theo quy định của pháp luật của người mua trong trường hợp người mua là đơn vị kế toán…

3.4. Lợi ích của hóa đơn điện tử mang lại cho doanh nghiệp

3.4.1. Tiết kiệm 80% thời gian và chi phí so với hóa đơn giấy

Việc sử dụng hóa đơn điện tử giúp Doanh nghiệp tiết kiệm được thời gian (giảm tới 70% các bước quy trình phát hành và 90% các tranh chấp liên quan đến hóa đơn, rút ngắn tới 99% thời gian thanh toán, quản lý hóa đơn, tiết kiệm 80% chi phí cho mỗi hóa đơn)… Khi sử dụng hóa đơn điện tử, Doanh nghiệp không cần chờ đợi nhận được hóa đơn theo đường bưu điện như cách làm truyền thống. Chỉ trong vài cú nhấp chuột, người mua hàng sẽ nhận được hóa đơn dù đang ở bất cứ nơi nào nếu có internet.

3.4.2. Giảm chi phí tuân thủ thủ tục hành chính Thuế

Việc sử dụng hóa đơn điện tử giúp doanh nghiệp giảm chi phí tuân thủ thủ tục hành chính thuế. Khi doanh nghiệp sử dụng hóa đơn điện tử, cơ bản các thủ tục hành chính thuế của doanh nghiệp cũng được thực hiện điện tử. Theo đó, doanh nghiệp chỉ cần thông báo qua mạng gửi đến cơ quan thuế về việc sử dụng hóa đơn điện tử và được sử dụng ngay sau khi thông báo được chấp nhận.

3.4.3. Không cần lập báo cáo tình hình sử dụng hóa đơn

Cùng với đó, doanh nghiệp không phải đăng ký mẫu hóa đơn điện tử, không phải gửi báo cáo tình hình sử dụng hóa đơn đến cơ quan thuế do phần mềm tạo hóa đơn điện tử cho phép tự xác định số lượng hóa đơn điện tử sử dụng.

3.4.4. Đơn giản hóa các quy trình liên quan đến hóa đơn

Áp dụng hoá đơn điện tử, có nghĩa là doanh nghiệp phải hoàn toàn chủ động các công việc khởi tạo và phát hành hóa đơn; đơn giản hóa việc phát hành, quản lý hóa đơn; đơn giản hóa thủ tục kê khai thuế và tình hình sử dụng hóa đơn; hóa đơn mang theo nhiều hơn thông tin, hình ảnh đặc trưng của doanh nghiệp.

Thêm vào đó, doanh nghiệp sẽ dễ dàng tra cứu thông tin hóa đơn và kiểm soát phát hành hóa đơn, tiết kiệm chi phí giao dịch hóa đơn, chi phí phát hành hóa đơn; doanh nghiệp cũng tự chủ, tự chịu trách nhiệm với thông tin hóa đơn được phát hành, hạn chế rủi ro và đơn giản hơn trong công tác bảo quản, lưu trữ…

3.4.5. An toàn – Bảo mật – Chống làm giả hóa đơn

Khác với hóa đơn giấy, hóa đơn điện tử là loại hóa đơn không thể làm giả, cũng khó có thể xảy ra các sai sót thường gặp khi viết hóa đơn giấy như viết sai tên người mua hàng, sai địa chỉ, sai mã số thuế, sai đơn giá…

3.5. Lợi ích của hóa đơn điện tử cho cơ quan thuế

Việc sử dụng hóa đơn điện tử còn giúp ngành Thuế xây dựng cơ sở dữ liệu về hóa đơn; hỗ trợ, phục vụ công tác thanh tra, kiểm tra, hoàn thuế, phân tích rủi ro doanh nghiệp, cá nhân kinh doanh.

Bên cạnh đó, giúp cơ quan Hải quan tại các cửa khẩu, sân bay nhanh chóng có thông tin để thực hiện hoàn thuế. Ngoài ra, cơ quan Thuế và các cơ quan khác của Nhà nước không tốn chi phí thời gian đối chiếu hóa đơn. Hiện nay, khi kiểm tra hoàn thuế giá trị gia tăng và kiểm tra thuế thu nhập doanh nghiệp, cơ quan Thuế và cơ quan khác của Nhà nước đều thực hiện đối chiếu hóa đơn, đây là công việc bắt buộc.

Ngoài những lợi ích trên, việc sử dụng hóa đơn điện tử cũng giúp cơ quan thuế kịp thời ngăn chặn hóa đơn của các doanh nghiệp bỏ trốn, mất tích, khắc phục tình trạng làm giả hóa đơn, tạo một môi trường kinh doanh lành mạnh cho các doanh nghiệp, thúc đẩy thương mại điện tử phát triển. Đồng thời, sử dụng hóa đơn điện tử góp phần bảo vệ môi trường; khắc phục được trình trạng gian lận sử dụng bất hợp pháp hóa đơn – lập hóa đơn sai lệch nội dung giữa các liên.

Ngoài những lợi ích trên, việc sử dụng hóa đơn điện tử cũng giúp cơ quan thuế kịp thời ngăn chặn hóa đơn của các doanh nghiệp bỏ trốn, mất tích, khắc phục tình trạng làm giả hóa đơn, tạo một môi trường kinh doanh lành mạnh cho các doanh nghiệp, thúc đẩy thương mại điện tử phát triển. Đồng thời, sử dụng hóa đơn điện tử góp phần bảo vệ môi trường; khắc phục được trình trạng gian lận sử dụng bất hợp pháp hóa đơn – lập hóa đơn sai lệch nội dung giữa các liên.

3.6. Ứng dụng của chữ ký số trong hóa đơn điện tử

Trong nền kinh tế hiện đại, xu hướng ứng dụng công nghệ thông tin được gắn liền với việc phát triển kinh doanh của các doanh nghiệp và được coi là yếu tố quan trọng giúp doanh nghiệp giữ vững, mở rộng thị trường, tăng tính cạnh tranh, và thực hiện các thỏa thuận thương mại với các nước trong khu vực cũng như trên thế giới. Quá trình giao dịch của các doanh nghiệp đòi hỏi một lượng thông tin trao đổi rất lớn qua mạng, song song với yêu cầu độ an toàn và tính xác thực cao. Chỉ có chữ ký số mới đảm bảo được sự an toàn này; và nó cũng được coi là phương tiện hữu hiệu để các doanh nghiệp tăng cường sức cạnh tranh thông qua thương mại điện tử.

Lợi ích của chữ ký số:

– Việc ứng dụng của chữ ký số sẽ giúp cho các doanh nghiệp tiết kiệm được thời gian cũng như công sức và chi phí giao dịch. Ngoài ra, sử dụng chữ ký số giúp hoạt động giao dịch điện tử cũng được đẩy mạnh hơn, không mất thời gian chờ đợi, đi lại.

– Không phải in ấn các hồ sơ.

– Việc ký kết các văn bản điện tử có thể diễn ra ở bất kỳ đâu, bất kỳ thời gian nào, mọi lúc mọi nơi.

– Việc chuyển hồ sơ, tài liệu đã ký cho các đối tác, khách hàng… diễn ra tiện lợi và nhanh chóng.

Từ những lợi ích của chữ ký số mà chúng ta có thể đem áp dụng vào để làm chữ ký đại diện cho doanh nghiệp, chữ ký số cũng là một phần không thể thiếu trong hóa đơn điện tử.

CHƯƠNG 4: SẢN PHẨM THỬ NGHIỆM

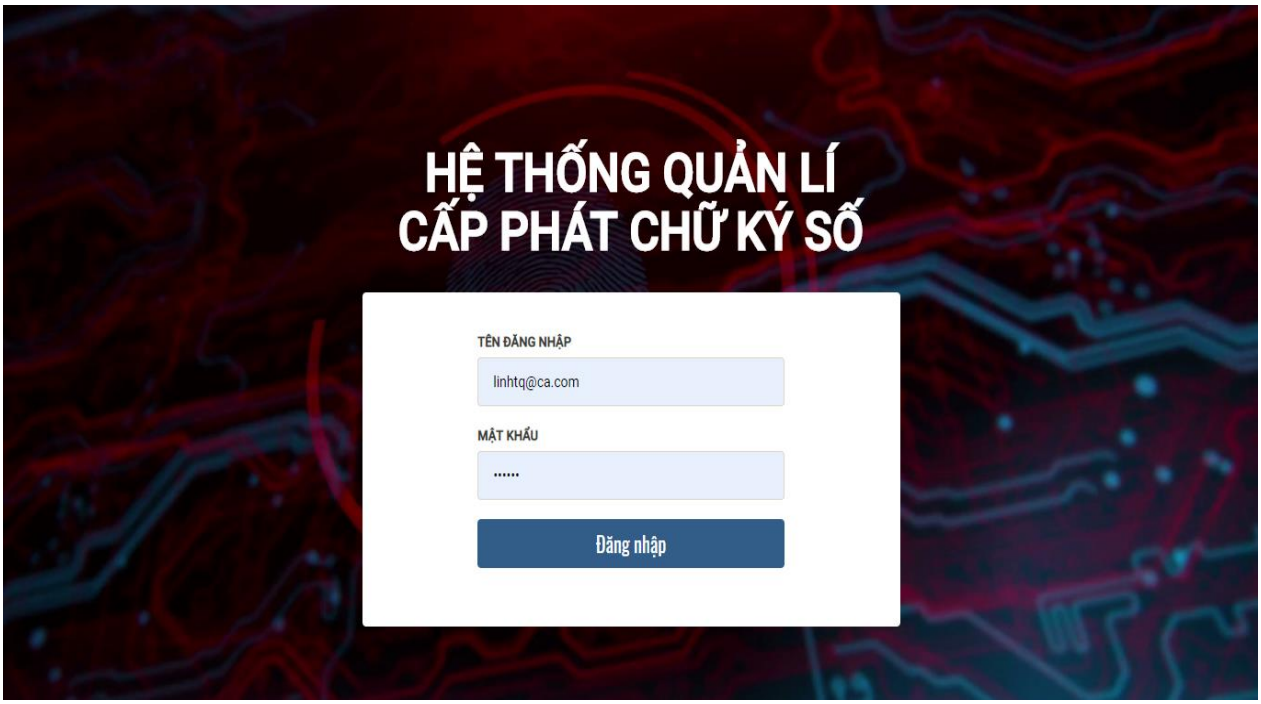
4.1 Giới thiệu về sản phẩm thử nghiệm:

Sản phẩm thử nghiệm được viết trên ngôn ngữ PHP nhằm khắc họa lại toàn bộ lý thuyết nếu trên. Sản phẩm gồm 3 trang:

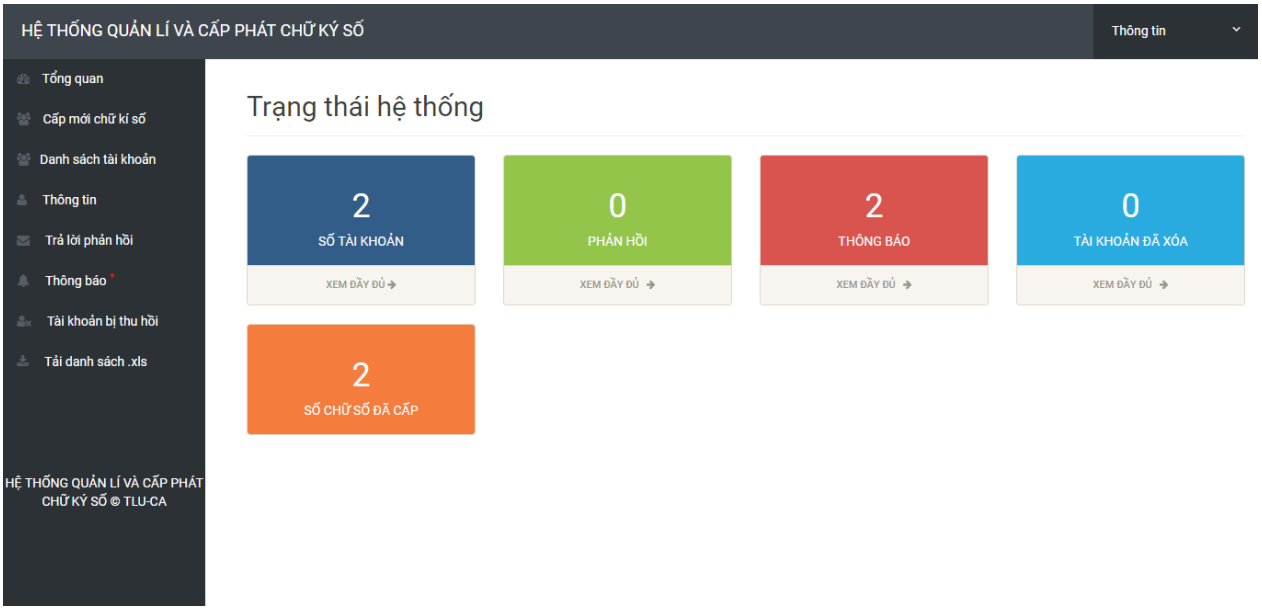
- Trang thứ nhất là trang e-hoadon: là trang web mô tả lại quá trình người dùng tạo hóa đơn điện tử và phát hành cũng như khai báo lên cơ quan thuế.
- Trang thứ hai là trang tlu-ca: là trang web mô tả lại quá trình của các nhà cấp phát chữ ký số cho người dùng.
- Trang thứ ba là trang tc-thue: là trang web mô tả lại quá trình cơ quan thuế xác nhận hóa đơn được người khai báo gửi lên và lưu trữ hóa đơn lại để phục vụ cho việc kiểm toán sau này.

4.2 Hình ảnh về các trang web thực nghiệm:

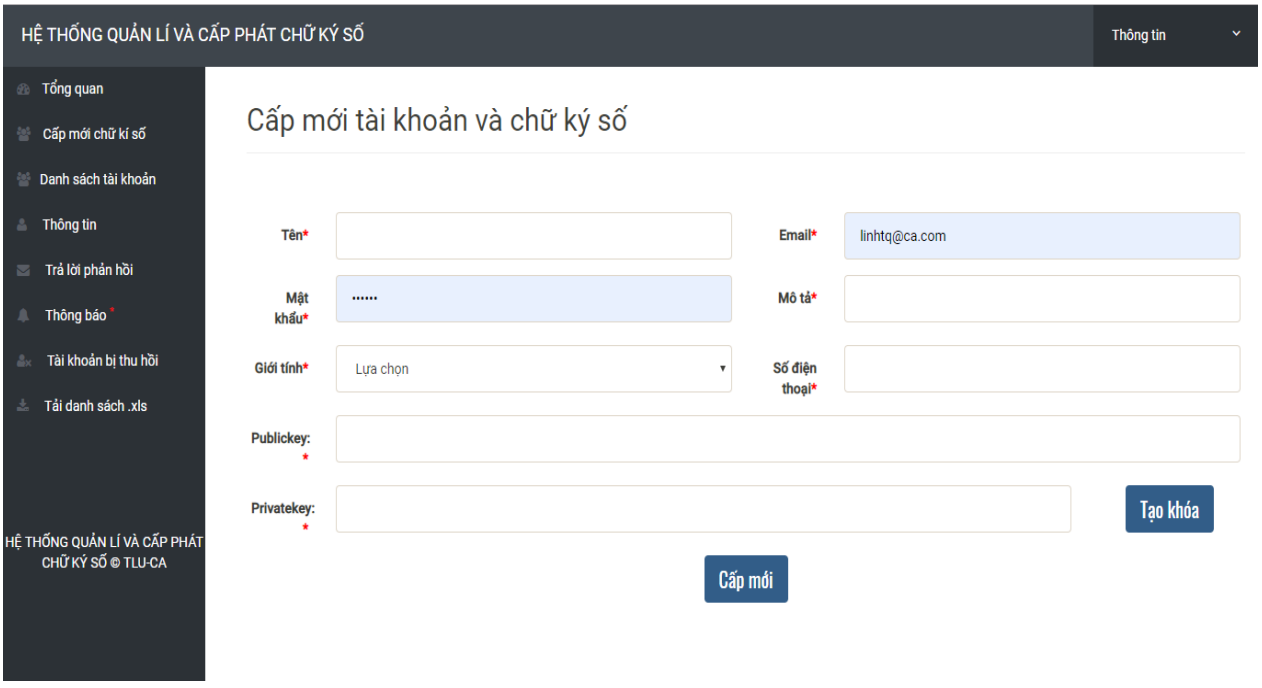
Trang tlu-ca mô tả lại quá trình đơn vị cấp phát chữ ký số và tài khoản để người dùng sử dụng:



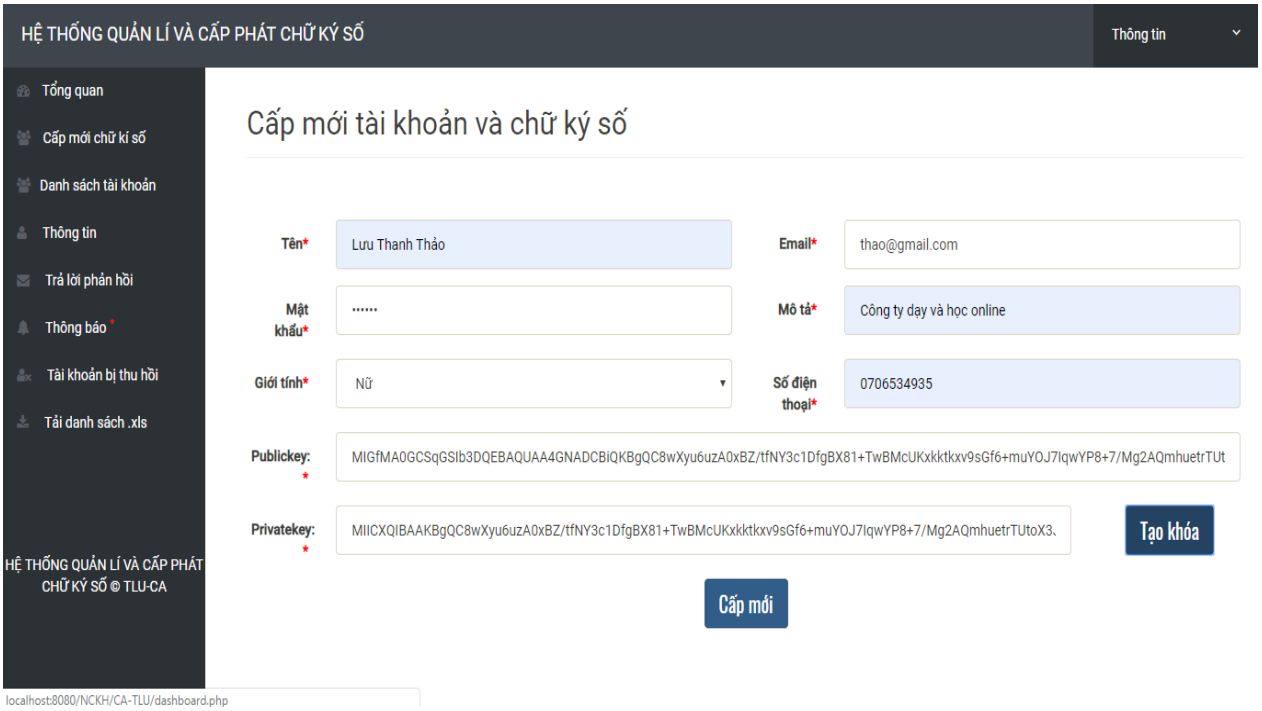
Sau khi đăng nhập vào :



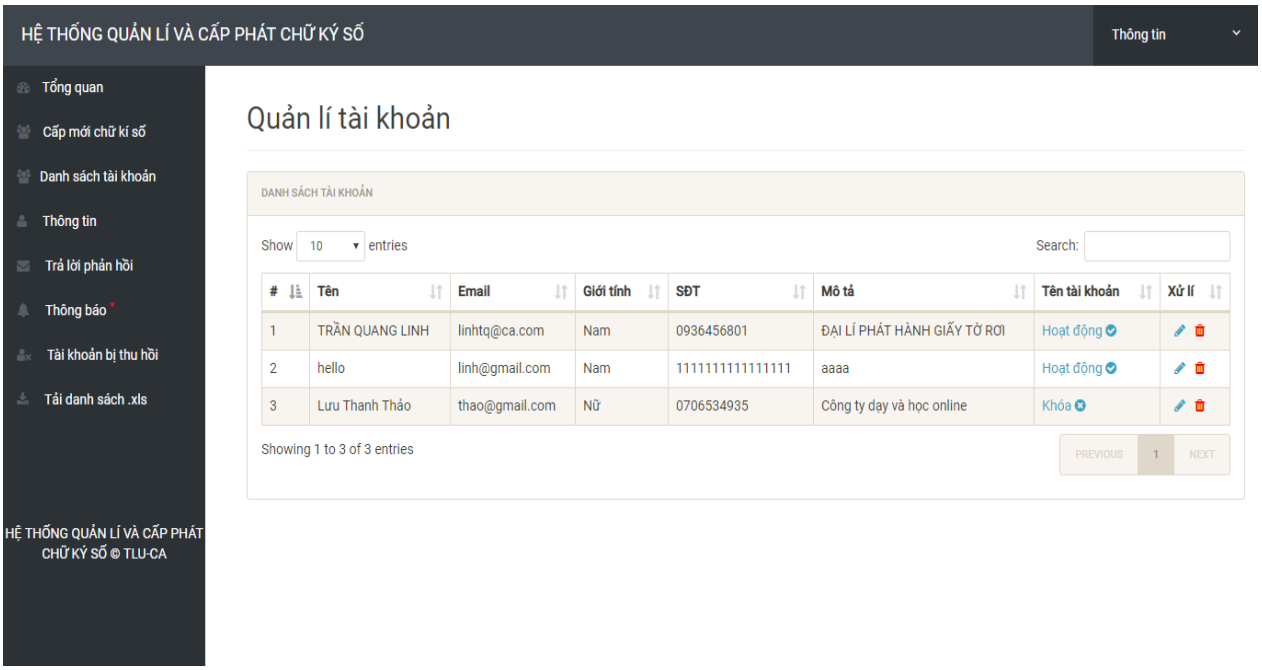
Bấm vào mục cấp chữ kí số:



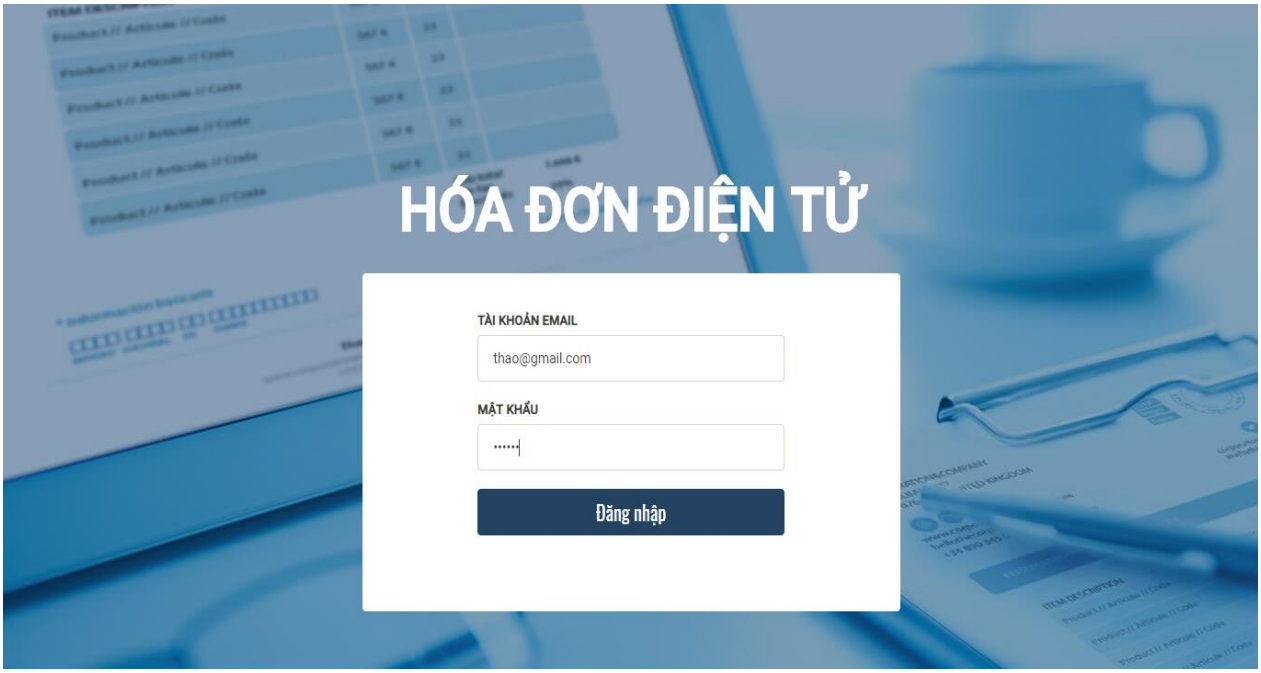
Điền đầy đủ thông tin và bấm tạo khóa:



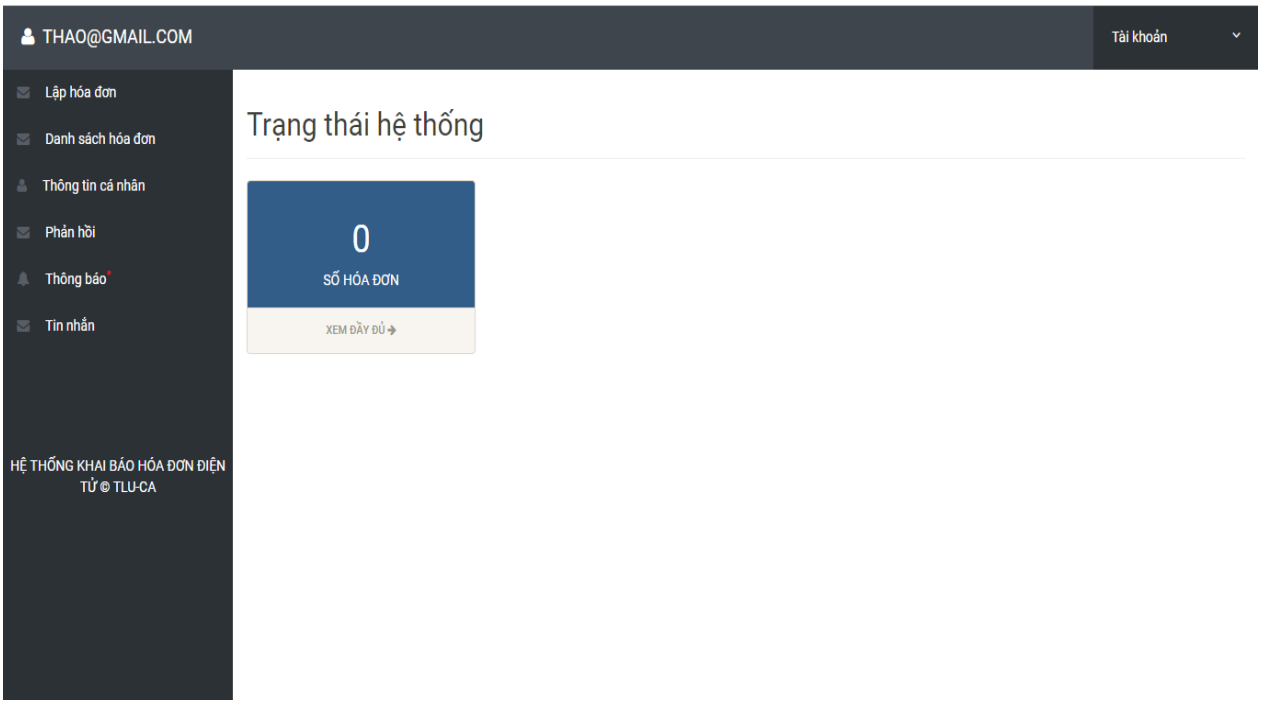
Bấm cấp mới:



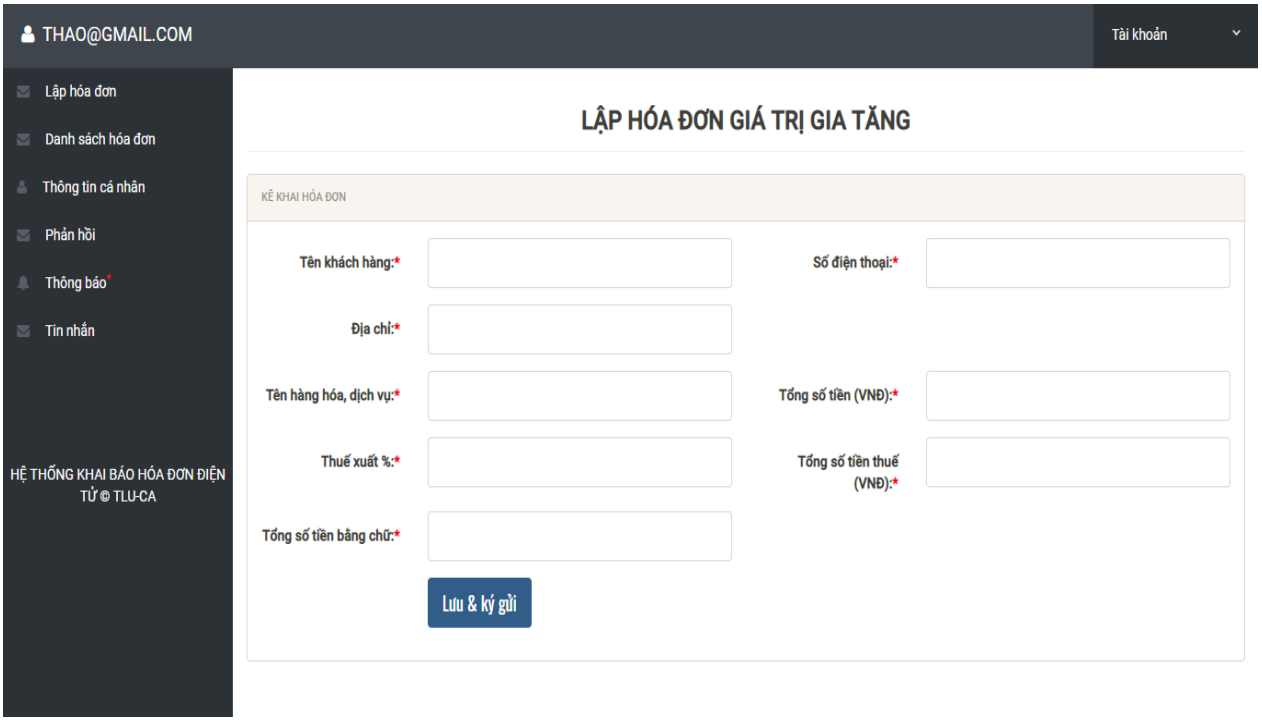
Như vậy tài khoản đã có thể dùng để khai báo trên e-hoadon:



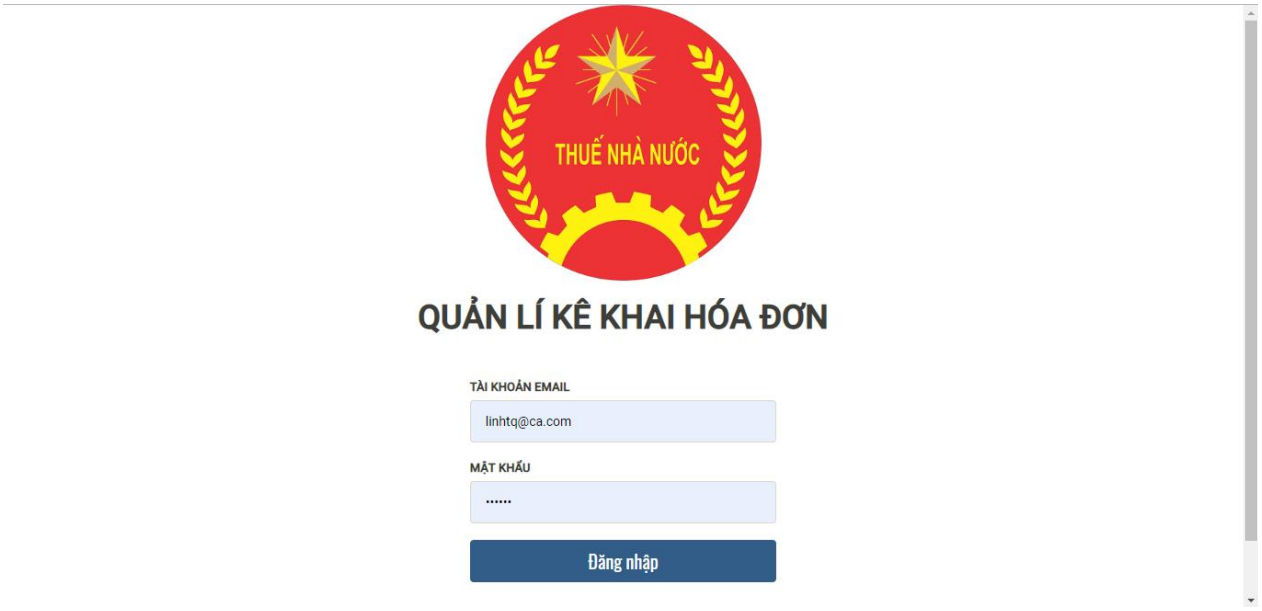
Đăng nhập vào e-hoadon:



Bấm vào mục lập hóa đơn:



Khi bấm nút kí gửi dữ liệu sẽ đến trang tc-thue:



KẾT LUẬN

Bài báo cáo khoa học:" CHỮ KÝ SỐ VÀ HÓA ĐƠN ĐIỆN TỬ " thu được một số kết quả:

-Nghiên cứu về chữ ký số.

-Nghiên cứu về thuật toán mã hóa RSA.

-Nghiên cứu về thuật toán mã hóa SHA-256.

-Nghiên cứu về hóa đơn và hóa đơn điển tử.

Trong thời gian tới nhóm nghiên cứu sẽ tiếp tục nghiên cứu để tối ưu về RSA cũng như tìm ra những ứng dụng mới của chữ ký số.

TÀI LIỆU THAM KHẢO

[1] Phạm Huy Điển , Mã hóa thông tin 2003, tr. 14-20.

[2] Ths.Trần Minh Triết.ChuKyDienTu-Revised-2008-Apr.ppt, tr11.

[3] Lê Đại Thọ, Slide bài giảng An Toàn Mạng 2009, tr.30-35

[4] Phan Huy Khánh, Hồ Phan Hiếu ,Trường Đại học Bách khoa, Đại học Đà Nẵng Giải pháp ứng dụng chữ ký điện tử trong quá trình gửi và nhận văn bản, Tạp chí khoa học và công nghệ, Đại học Đà Nẵng – số 5(34).2009

[5] TS Lê Đức Phong, Cryptographic protocols, tr.13

[6] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, November 16, 2005, tr.30-35

[7] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, 1976

[8] Bart Van Rompay. Analysis and Desigbn of Cryptographic Hash Functions, MAC Algorithms and Block Ciphers, Juni 2004, tr. 27-28.

[9] Burt Kaliski,RSA Laboratories, The Mathematics of the RSA Public-Key Cryptosystem

[10] Trang Web : http://vi.wikipedia.org/wiki/Chữ_ký_số, tr. 9.

[11] Trang Web : http://vi.wikipedia.org/wiki/Hàm_băm_mật_mã_học, tr.21.

[12] Trang Web : http://vi.wikipedia.org/wiki/Mật_mã_học, tr.29

[13] Trang Web : http://chukysotoanquoc.com/chi-tiet-tin-tuc/loi-ich-cua-chu-ky-so-va-ung-dung-hiennay-102.html

[14] Trang Web: http://chukysotoanquoc.com/chi-tiet-tin-tuc/loi-ich-cua-chu-ky-so-va-ung-dung-hiennay-102.html

[15] Trang Web: https://einvoice.vn/tin-tuc/nhung-bat-cap-cua-hoa-don-giay-va-huong-toi-xu-huong-su-dung-hoa-don-dien-tu-hien-nay