**Ứng dụng chữ ký số trong thương mại điện tử**

Hiện nay, với sự bùng nổ của cách mạng công nghệ 4.0, **chữ ký số** dần trở thành hình thức chữ ký điện tử phổ biến nhất trong các giao dịch điện tử. Tại Việt Nam, xu hướng phát triển và ứng dụng chữ ký số tại các doanh nghiệp (DN) đang trở nên phổ biến và phát triển rộng rãi. Do vậy, bài nghiên cứu tổng quan về thương mại điện tử, tìm hiểu về chữ ký số, lợi ích và ứng dụng của chữ ký số trong **thương mại điện tử.**

**1. Đặt vấn đề**

Ứng dụng mã hóa và **bảo mật thông tin** trong các hệ thống thương mại điện tử, giao dịch chứng khoán,… đã trở nên phổ biến trên thế giới và sẽ ngày càng trở nên quen thuộc với người Việt Nam. Tháng 7/2000, thị trường chứng khoán lần đầu tiên được hình thành tại Việt Nam; các thẻ tín dụng bắt đầu được sử dụng, các ứng dụng hệ thống thương mại điện tử đang ở bước đầu được quan tâm và xây dựng. Do đó, nhu cầu về các ứng dụng mã hóa và bảo mật thông tin trở nên rất cần thiết.

Chính vì những vấn đề thực tiễn trên, bài viết với đề tài: “Ứng dụng Chữ ký số trong thương mại điện tử” sẽ tập trung nghiên cứu một trong những phương pháp bảo vệ an toàn dữ liệu có tính an toàn cao nhất hiện nay là hệ mật mã có khóa công khai RSA, chữ ký số, chứng thực chữ ký số, công nghệ bảo mật sử dụng cho thương mại điện tử,…

**2. Tổng quan thương mại điện tử**

Thương mại điện tử hay còn gọi là E-commerce, là sự mua bán trao đổi sản phẩm hàng hóa, giao dịch, dịch vụ trên các hệ thống điện tử như Internet, mạng máy tính,… Thương mại điện tử dựa trên một số công nghệ như chuyển tiền điện tử, quản lý chuỗi cung ứng, giao dịch trực tuyến, tiếp thị Internet, hệ thống tự động thu nhập dữ liệu, hệ thống quản lý hàng tồn kho,… Việc sử dụng thương mại điện tử trong kinh doanh giúp cho các DN tiết kiệm được một  khoản chi phí cho việc thuê mặt bằng, thuê nhân viên, trang thiết bị, nhà kho,… Mặt khác, thương mại điện tử giúp các bên có thể tiến hành giao dịch khi ở cách xa nhau, từ thành phố đến nông thôn, giữa các nước với nhau mà không bị giới hạn về địa lý, thời gian. Điều này cho phép các DN tiết kiệm chi phí sản xuất, giao dịch. Đặc biệt, DN có thể mở rộng thị trường, tìm kiếm, liên lạc với đối tác và khách hàng ở bất kỳ đâu với chi phí thấp hơn phương pháp truyền thống. Với khả năng truyền bá thông tin và làm hài lòng các khách hàng, thương mại điện tử đã góp phần không nhỏ trong việc tăng doanh thu của DN. Đánh giá  được tầm quan trọng của thương mại điện tử, các DN đã và đang tích cực đầu tư vào hình thái hoạt động này. Tuy thấy được lợi ích và tầm quan trọng của thương mại điện tử nhưng không phải DN nào cũng có thể đáp ứng được những điều kiện cần để xây dựng thương mại điện tử. Sự đòi hỏi của thương mại điện tử là sự tổng hợp của hàng chục các vấn đề đan xen vào nhau bao gồm: hạ tầng cơ sở công nghệ, hạ tầng cơ sở nhân lực, bảo mật, an toàn, hệ thống thanh toán tự động, bảo vệ sở hữu trí tuệ, bảo vệ người tiêu dùng, môi trường kinh tế và pháp lý, tác động văn hóa xã hội, lệ thuộc công nghệ.

Nhằm giải quyết vấn đề bảo mật an toàn cho các giao dịch trao đổi văn bản trên mạng, đã có rất nhiều các giải pháp được đưa ra và đều xoay quanh việc mã hóa văn bản và chữ ký số là một trong số những giải pháp đó. Chữ ký số là công nghệ xác thực, đảm bảo an ninh, an toàn cho các giao dịch trong môi trường Internet, giúp chúng ta giải quyết vấn đề về toàn vẹn dữ liệu, là bằng chứng để ngăn chặn việc chối bỏ trách nhiệm trên nội dung đã ký, giúp các DN, tổ chức, cá nhân có thể yên tâm với các giao dịch của mình trong môi trường Internet.

**3. Chữ ký số**

**3.1. Khái niệm chữ ký số**

Theo Điều 1, Khoản 4, Nghị định số 26/2007/NĐ-CP, chữ ký số là một dạng chữ ký điện tử (hay còn gọi là sơ đồ chữ ký số) được tạo ra bằng sự biến đổi một thông điệp dữ liệu, sử dụng hệ thống mật mã không đối xứng. Người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác:

- Việc biến đổi nói trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai đó.

- Thông điệp được giữ nguyên vẹn toàn bộ nội dung kể từ khi thực hiện việc biến đổi dữ liệu.

Có thể hiểu, chữ ký số là phương pháp ký một bức điện lưu dưới dạng điện tử. Một sơ đồ chữ ký số thường chứa 2 thành phần: thuật toán ký và thuật toán xác minh.

Hay chữ ký số là một thiết bị được mã hóa tất cả các dữ liệu, thông tin của một DN/cá nhân/tổ chức thay cho chữ ký tay trên các loại văn bản và tài liệu số thực hiện đối với các giao dịch điện tử qua mạng internet. Cũng có thể hiểu chữ ký số như một con dấu điện tử của DN/cá nhân/tổ chức, được thừa nhận về mặt pháp lý khi giao dịch trên môi trường điện tử, như: ký hợp đồng điện tử, ký kê khai thuế, ký phát hành hóa đơn điện tử, ký giao dịch tài chính,…

**3.2. Đặc điểm của chữ ký số**

- Khả năng xác định nguồn gốc: Chữ ký số có thể xác thực danh tính chủ nhân của chữ ký số thông qua chứng thư số của cá nhân, tổ chức, DN.

- Tính bảo mật cao: Chữ ký số có 2 lớp mã khóa, đảm bảo tính bảo mật và không bị đánh cắp thông tin bởi hacker.

- Tính toàn vẹn: Chữ ký số đảm bảo chỉ có người nhận văn bản/tài liệu đã ký số mới có thể mở văn bản/tài liệu đó. Từ đó, đảm bảo tính toàn vẹn của văn bản/tài liệu điện tử trong môi trường điện tử.

- Tính không thể phủ nhận: Chữ ký số không thể xóa bỏ và thay thế.

**3.3. Vai trò của chữ ký số**

Chữ ký số đóng một vai trò quan trọng trong việc xác nhận, đảm bảo về trách nhiệm, quyền và nghĩa vụ của các chủ thể tham gia ký kết văn bản hay giao dịch điện tử.

Đặc biệt, chữ ký số có vai trò đảm bảo an toàn cho các giao dịch điện tử. Đây là yếu tố quan trọng nhất, là điều kiện tiên quyết khi chuyển các giao dịch có giá trị lớn trên giấy tờ sang giao dịch trên mạng, đem lại lợi thế cạnh tranh cho các DN trong bối cảnh hội nhập kinh tế quốc tế. Với các giao dịch thương mại điện tử B2C, giá trị các giao dịch nhỏ, các cá nhân thường sử dụng các thông tin trên thẻ tín dụng để xác thực sự đồng ý của mình và dùng các thông tin này tương đương với “chữ ký” khi thực hiện các giao dịch này. Với các giao dịch thương mại điện tử B2B có giá trị lớn, việc sử dụng chữ ký số là cần thiết vì tầm quan trọng của giao dịch và đòi hỏi về mức độ bảo mật cũng cao hơn.

**3.4. Cấu tạo của chữ ký số (Sơ đồ chữ ký RSA)**

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

Có thể coi bài toán xác thực là bài toán "đối ngẫu" với bài toán bảo mật. Vì vậy, sử dụng ngược thuật toán RSA ta có thể có được một sơ đồ chữ ký số RSA như sau:

Giả sử n = pq, trong đó p và q là các số nguyên tố có kích thước tương đương.

CT1

Với K = (n, e, d), ta có D = d là khóa bí mật,

E = (n, e) là khóa công khai, m là bản tin cần ký.

Tạo chữ ký:  S = SigD(m) = mdmod n.

Kiểm tra chữ ký: VerE (m, S) = TRUE ↔ m = Semod n.

**3.5. Lợi ích của ứng dụng chữ ký số trong thương mại điện tử**

Trong thương mại điện tử, các ứng dụng chữ ký số sẽ mang lại cho DN/cá nhân/tổ chức nhiều lợi ích như:

- Tiết kiệm được chi phí giấy tờ, thời gian luân chuyển hoạt động quản lý công văn thư, thư điện tử.

- Đẩy nhanh các giao dịch qua mạng mà vẫn đảm bảo độ an toàn và bảo mật thông tin tuyệt đối.

Ứng dụng các công nghệ thông tin trong kinh doanh là một yếu tố quan trọng giúp DN giữ vững, tăng tính cạnh tranh, mở rộng thị trường, thực hiện các thỏa thuận về thương mại trong khu vực và thế giới. Tất cả quá trình này đòi hỏi lượng thông tin trao đổi không hề nhỏ qua mạng với yêu cầu độ an toàn và tính xác thực cao. Chỉ có chữ ký số mới bảo đảm được sự an toàn này.

**3.6. Ứng dụng chữ ký số trong thương mại điện tử**

Chữ ký số được các DN/cá nhân/tổ chức dùng để:

- Chứng thực danh tính người tham gia giao dịch, xác thực tính an toàn của giao dịch điện tử qua mạng Internet.

- Chứng thực tính nguyên vẹn của hợp đồng, tài liệu,...

- Ứng dụng xác thực trong Internet banking

- Ứng dụng xác thực trong giao dịch chứng khoán

- Ứng dụng xác thực trong mua bán, đấu thầu qua mạng

**4. Mã hóa RSA**

Mật mã RSA được viết tắt bởi tên của 3 nhà Toán học (Rivest, Shamir, Adleman). Trong phương pháp mật mã RSA, việc mã hóa và giải mã sử dụng hàm lũy thừa với modul không nguyên tố.

**4.1. Mô tả giải thuật RSA**

*Tạo khóa:*

Mỗi đầu cần tạo 1 khóa công khai và 1 khóa riêng tương ứng theo các bước sau:

(1) Tạo 2 số nguyên tố lớn ngẫu nhiên và khác nhau p và q, p và q có độ lớn xấp xỉ nhau.

(2) Tính n = p.q và Ф(n)= (p-1).(q-1).

(3) Chọn một số ngẫu nhiên e, 1 < e < Ф(n), sao cho (e, Ф(n)) = 1.

(4) Sử dụng thuật toán Euclidean mở rộng để tính một số nguyên duy nhất 1 < d < Ф(n) thỏa mãn e.d Ф1 (mod Ф(n)) (d là nghịch đảo của e đối với Ф (n)).

(5) Khóa công khai là cặp số (n, e). Khóa bí mật là d

Các số nguyên e và d ở trên được gọi là số mũ mã hóa và số mũ giải mã.

*Mã hóa:*

A mã hóa một thông báo m để gửi cho B bản mã cần giải. A phải thực hiện:

(1) Thu nhận khóa công khai (n, e) của B.

(2) Biểu diễn bản tin dưới dạng một số nguyên m trong dải [0, n -1]

(3) Tính c = me mod n.

(4) Gửi bản mã c cho B.

*Giải mã:*

Khôi phục bản rõ m từ c. B phải thực hiện phép tính m = cd  mod n  bằng cách dùng khóa riêng.

**4.2. Độ an toàn của RSA**

Vì khóa là công khai, nên người giải mã thường dựa vào cặp khóa này để tìm cặp khóa bí mật. Điều quan trọng là dựa vào n để tính 2 thừa số p, q của n từ đó tính được d.

Có một vài điều cần lưu ý khi chọn các số p và q để tránh rơi vào trường hợp tích của pq bị phân tích nhanh nhờ những thuật toán đặc biệt: p và q cần chọn sao cho p - 1 và q - 1 không chỉ có toàn các ước nguyên tố nhỏ. Ngoài ra, ước chung lớn nhất (p - 1, q - 1) phải là số nhỏ, p và q phải có chữ số trong khai triển thập phân khác nhau không nhiều.

**4.3. Sự che dấu thông tin trong hệ thống RSA**

Hệ thống RSA có một đặc điểm đặc trưng là thông tin không phải luôn luôn được che dấu. Giả sử người gửi có e = 17, n = 35. Nếu anh ta muốn gửi bất cứ data nào thuộc tập sau:

{1, 6, 7, 8,  13, 14, 15, 20, 21, 22, 27, 28, 29, 34} thì mọi mật mã cũng chính là data ban đầu.

Để xác định chính xác số message không được che dấu (không bị thay đổi sau khi mã hóa) ta sử dụng định lý sau:

"*Nếu các message được mã hóa trong hệ thống RSA được xác định bởi số modul n = pq (p, q là số nguyên tố) và khóa công khai e thì có:*

*m = [1 + UCLN(e-1, p-1)][1 + UCLN(e-1, q-1)] message không bị che dấu*".

**4.4. Một số lưu ý khi sử dụng hệ mật mã RSA**

RSA đã phải đương đầu với các kiểu tấn công đủ loại của giới thám mã chuyên nghiệp. Kết quả hơn 20 năm "công phá" hệ mã RSA của các nhà thám mã đã được tóm lược trong bài báo của Dan Boneh với tựa đề "Hai mươi năm tấn công hệ mã RSA" (đăng trong tờ Notices of the AMS, tháng 2, năm 1999), trong đó cho thấy rõ RSA có thể bị "bẻ"  khi người ta không biết dùng nó một cách "bài bản". Khi chìa khóa lập mã (hoặc giải mã) là những số nguyên tố nhỏ thì người ta có những giải pháp bẻ RSA một cách không mấy khó khăn. Thêm vào đó, không phải mọi hợp số lớn đều khó phân tích (kể cả khi nó là tích của 2 số nguyên tố rất lớn), cho nên việc chọn các số nguyên tố p, q phải rất thận trọng.

**5. Cài đặt một số ứng dụng**

Phần này trình bày một số giao diện và các chức năng chính của 2 phần mềm ứng dụng: phần mềm mã hóa và ứng dụng chữ ký số RSA, trang web bán hàng trực tuyến hỗ trợ giao thức bảo mật SSL.

**5.1. Phần mềm mã hóa và ứng dụng chữ ký số RSA**

Các chức năng chính của phần mềm:

- Soạn thảo văn bản;

- Chức năng tạo cặp khóa riêng và công khai;

- Chức năng demo giải thuật RSA;

- Mã hóa văn bản trong vùng nhập văn bản;

- Giải mã văn bản trong vùng nhập văn bản;

- Chức năng mã hóa và giải mã file;

- Lấy mã băm (SHA-1) của văn bản trong vùng nhập văn bản;

- Lấy mã băm (SHA-1) của một tập tin bất kỳ;

- Ký văn bản trong vùng nhập văn bản;

- Chức năng xác minh chữ ký.

**5.2. Trang web bán hàng trực tuyến hỗ trợ giao thức SSL**

Các chức năng chính của trang web:

- Đăng ký, đăng nhập;

- Liệt kê lịch sử đặt hàng của từng khách hàng;

- Hiển thị và nhóm sản phẩm theo từng danh mục và nhà sản xuất;

- Quản lý thông tin giỏ hàng;

- Hiển thị sản phẩm mới trong tháng;

- Hiển thị sản phẩm giảm giá, sản phẩm bán nhiều nhất;

- Tìm kiếm và tìm kiếm nâng cao bằng các toán tử AND, OR;

- Chức năng cho ý kiến về sản phẩm;

- Quản lý và chuyển đổi tiền tệ qua lại;

- Chức năng thanh toán qua mạng;

- Chức năng quản trị trang web dành cho administrator.

**6. Kết luận**

Mặc dù còn mới đối với phần lớn các DN Việt Nam, nhưng chữ ký số đóng vai trò hết sức quan trọng đối với tương lai của thương mại điện tử và Chính phủ điện tử trong bối cảnh hội nhập kinh tế thế giới hiện nay. Việc ứng dụng chữ ký số trong thương mại điện tử sẽ đem lại cho DN/cá nhân/tổ chức rất nhiều lợi ích, như: tiết kiệm chi phí giấy tờ, thời gian luân chuyển trong hoạt động quản lý công văn, giấy tờ, thư điện tử. Bên cạnh đó, còn góp phần đẩy nhanh các giao dịch qua mạng trong khi vẫn đảm bảo độ an toàn và bảo mật thông tin.

**TÀI LIỆU THAM KHẢO:**

1. Dương Quang Thiện. (2005). *Net toàn tập - Tập 3: Lập trình giao diện người dùng theo C#.* TP. Hồ Chí Minh: NXB Tổng hợp TP. Hồ Chí Minh.
2. Hà Duy Khoái. (2004). *Mã hóa thông tin Cơ sở toán học và ứng dụng.* Hà Nội: NXB Đại học Quốc gia Hà Nội.
3. Kenneth H. Rosen. (1995). *The CRC Press Series on Discrete Mathematics and its Applications.* USA: CRC Press, Inc.
4. Nguyễn Bình. (2004). *Giáo trình Mật mã học.* Hà Nội: NXB Bưu điện (Học viện Công nghệ Bưu chính Viễn thông).
5. Nguyễn Nam Hải. (2004). *Chứng thực trong thương mại điện tử.* Hà Nội: NXB Khoa học và Kỹ thuật.
6. Nguyen Phong Quang (ED.). (2006). *Pre-Proceedings of International Conference on Cryptology in Vietnam - VIETCRYPT06.* Ha Noi: FPT Software.
7. Thái Hồng Nhị. (2004). *An toàn thông tin mạng máy tính, truyền tin số và truyền dữ liệu*. Hà Nội: NXB Khoa học và Kỹ thuật.
8. Trịnh Nhật Tiến. (2006). *Giáo trình An toàn dữ liệu và mã hóa*. Hà Nội: NXB Đại học Quốc gia Hà Nội.

https://tapchicongthuong.vn/bai-viet/ung-dung-chu-ky-so-trong-thuong-mai-dien-tu-86815.htm