BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH: CÔNG NGHỆ THÔNG TIN

Sinh viên : Phạm Trung Hiếu

Giảng viên hướng dẫn: Đại tá,Ts Hồ Văn Canh

HẢI PHÒNG – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

TÌM HIỂU VỀ CHỮ KÝ SỐ VÀ ỨNG DỤNG CỦA NÓ TRONG THƯƠNG MẠI ĐIỆN TỬ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
NGÀNH: CÔNG NGHỆ THÔNG TIN

Sinh viên : Phạm Trung Hiếu
Giảng viên hướng dẫn: Đại tá, TS Hồ Văn Canh

HẢI PHÒNG – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên : Phạm Trung Hiếu Mã SV : 1612404011

Lớp : CT2001C Ngành : Công nghệ thông tin

Tên đề tài: Tìm hiểu về chữ ký số và ứng dụng trong thương mại điện tử

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

- Nghiên cứu tìm hiểu mật mã khóa công khai và chữ ký số
- Nắm vững vai trò của mật mã khóa công khai và thương mại điện tử
- Hiểu biết về cơ sở mật mã và an toàn thông tin

2. Các tài liệu, số liệu cần thiết

- Ho Van Canh, Le Danh Cuong (2018): Mật mã và an toàn thông tin – Lý thuyết và ứng dụng

3. Địa điểm thực tập tốt nghiệp

VPĐD Công ty cổ phần đầu tư tài chính và công nghệ Datatech

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Họ và tên : Hồ Văn Canh

Học hàm, học vị : Đại tá, Tiến sĩ

Cơ quan công tác : Cục KTNV-BCA

Nội dung hướng dẫn:

- Tìm hiểu về mật mã với khóa công khai.
- Lựa chọn một loại mật mã khóa công khai làm chuẩn chữ ký số
- Trình bày tóm lược về thương mại điện tử
- Thực hành ký trên một văn bản bằng chuẩn chữ ký số, nhận xét, đánh giá, kết luận.

Đề tài tốt nghiệp được giao ngày 11 tháng 10 năm 2021.

Yêu cầu phải hoàn thành xong trước ngày 31 tháng 12 năm 2021.

Đã nhận nhiệm vụ ĐTTN
Sinh viên

Đã giao nhiệm vụ ĐTTN
Giảng viên hướng dẫn

Hải Phòng, ngày tháng năm 2021

TRƯỞNG KHOA

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

Họ và tên giảng viên: ……

Đơn vị công tác: ……

Họ và tên sinh viên: …… Ngành: ..…….

Nội dung hướng dẫn: …….

……

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp

.....

.....

.....

.....

.....

.....

Đánh giá chất lượng của đồ án/khóa luận (so với nội dung yêu cầu đó đề ra trong nhiệm vụ Đ.T. T.N trên các mặt lý luận, thực tiễn, tính toán số liệu…)

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. Ý kiến của giảng viên hướng dẫn tốt nghiệp

Đạt ☐ Không đạt ☐ Điểm:……...

Hải Phòng, ngày ... tháng ... năm 2021

Giảng viên hướng dẫn

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên: ……

Đơn vị công tác: ……..

Họ và tên sinh viên: …… Ngành: ……

Đề tài tốt nghiệp:……..

……

1. Phần nhận xét của giảng viên chấm phản biện

.....

.....

.....

.....

.....

2. Những mặt còn hạn chế

.....

.....

.....

.....

.....

.....

.....

3. Ý kiến của giảng viên chấm phản biện

Đạt ☐ Không đạt ☐ Điểm:……...

Hải Phòng, ngày ... tháng ... năm 2021

Giảng viên chấm phản biện

LỜI CẢM ƠN

Lời đầu tiên, tôi muốn gửi lời cảm ơn sâu sắc đến TS. Hồ Văn Canh, thầy là người đã tận tình hướng dẫn, giúp đỡ tôi trong suốt quá trình làm đồ án tốt nghiệp, giúp tôi đạt được kết quả tốt nhất có thể.

Tôi cũng xin bày tỏ lòng biết ơn sâu sắc tới các Thầy, Cô trong Khoa Công nghệ Thông tin những người đã đồng hành cùng tôi trong suốt thời gian học tập tại trường và đã truyền đạt cho tôi những kiến thức vô cùng quý giá.

Tôi xin trân trọng cảm ơn các Thầy Cô giáo trong trường và Ban lãnh đạo nhà Trường đã tạo dựng cho tôi một môi trường lành mạnh để tôi học tập, phấn đấu để ra đời lập nghiệp.

Tôi xin gửi lời cảm ơn chân thành đến các bạn đồng môn, toàn thể bạn bè và gia đình đã luôn chia sẻ và động viên tôi trong suốt thời gian học tập cũng như thực hiện đồ án tốt nghiệp này.

Hải Phòng, ngày tháng năm 2021

Sinh viên

Phạm Trung Hiếu

MỤC LỤC

DANH SÁCH HÌNH ẢNH

LỜI MỞ ĐẦU

Trong thời đại Công nghệ thông tin hiện nay thì việc rút ngắn khoảng cách giữa không gian, thời gian là yếu tố quan trọng trong công việc kinh doanh. Vì vậy Chữ ký số ra đời giúp cho Doanh nghiệp tiết kiệm được thời gian, công sức trong một số công việc giao dịch với Ngân hàng, cơ quan hành chính…

Chữ ký số không đòi hỏi phải sử dụng giấy mực, nó là một dạng chữ ký điện tử. Chữ ký số được tạo ra bởi người ký đóng vai trò như chữ ký đối với cá nhân hay con dấu đối với doanh nghiệp và được thừa nhận về mặt pháp lý. Chữ ký số được coi là phương án giải quyết tốt nhất mọi vấn đề khi giao dịch trên môi trường Internet và còn được ứng dụng vào nhiều lĩnh vực bảo mật cao khác.

Chữ ký số xuất hiện trở thành một phương tiện tốt nhất để tăng sự cạnh tranh giữa các doanh nghiệp. Đặc biệt trong bối cảnh công nghệ ngày càng hiện đại như hiện nay thì việc sử dụng dịch vụ này như một điều tất yếu không thể thiếu, đảm bảo sự thành công của các giao dịch. Chữ ký số là một loại chữ ký được sử dụng phổ biến nhất hiện nay. Tầm quan trọng của chữ ký số được thể hiện bởi các thành phần của chữ ký số, đó là: khóa bí mật và khóa công khai.

Dựa vào tầm quan trọng của chữ ký số thì nhiều doanh nghiệp đã sử dụng ứng dụng này để tạo ra nhiều loại ứng dụng khác biệt phù hợp nhất và mã hóa để đảm bảo tính an toàn cho doanh nghiệp. Các doanh nghiệp thường sử dụng chữ ký số để xác nhận email, kiểm soát các giao dịch trên sàn thương mại điện tử như: như ngân hàng điện tử, mua sắm điện tử của công ty và quản lý bảo mật các thông tin khách hàng. Ngoài ra, chữ ký số còn được ứng dụng trong hệ thống mạng di động rất hiệu quả.

Hiểu được tầm quan trọng của chữ kí số trong xã hội hiện nay, dưới sự hướng dẫn giúp đỡ của thầy cô và các bạn tôi đã nghiêm cứu tìm hiểu phương pháp xây dựng lược đồ chữ kí số dựa trên bài toán khai căn. Trong quá trình tìm hiểu, nghiên cứu để hoàn thành đồ án tốt nghiệp này, tôi đã nhận được sự giúp đỡ quý

báu của thầy cô, của bạn bè. Với lòng kính trọng và biết ơn sâu sắc tôi xin được bày tỏ lời cảm ơn chân thành tới:

Ban Giám hiệu, Phòng đào tạo, các Thầy Cô giáo trong Khoa Công nghệ thông tin – Trường Đại học Quản lý và Công nghệ Hải Phòng đã giảng dạy, nhiệt tình đóng góp ý kiến và tạo điều kiện cho tôi trong suốt thời gian học tập và thực hiện đồ án.

Đại tá, Tiến sĩ Hồ Văn Canh, người đã hết lòng giúp đỡ, dạy bảo, động viên và tạo điều kiện thuận lợi cho tôi trong suốt quá trình học tập và hoàn thành đồ án tốt nghiệp này.

CHƯƠNG I. THƯƠNG MẠI ĐIỆN TỬ VÀ VAI TRÒ CỦA CHỮ KÝ SỐ TRONG THƯƠNG MẠI ĐIỆN TỬ

Chương này trình bày về thanh toán trong thương mại điện tử và các vấn đề liên quan. Nội dung cụ thể bao gồm các yêu cầu đối với một hệ thống thanh toán điện tử, các phương tiện và giao thức thanh toán được dùng hiện nay, các cấu hình có thể của một hệ thống thanh toán. Phần cuối của chương sẽ trình bày vấn đề sử dụng ký thuật chữ ký điện tử và chứng chỉ số để đảm bảo an toàn cho giao dịch thanh toán.

1.1. Giới thiệu về thương mại điện tử

1.1.1. Thương mại điện tử là gì?

Càng về những năm gần đây, tại các nước công nghiệp phát triển cũng như ở các nước NICs, xuất hiện ngày càng nhiều loại hình kinh doanh mới hoạt động trên các mạng truyền thông số và đặc biệt là trên mạng Internet. Đó là các doanh nghiệp thương mại điện tử. Sự xuất hiện của mô hình kinh doanh này không chỉ làm đa dạng hoá hoạt động doanh nghiệp của con người mà còn thực sự trở thành một cuộc cách mạng kinh tế - xã hội có ý nghĩa lịch sử, đánh dấu bước đột phá mới về kinh tế của nhân loại trong thiên niên kỷ thứ ba.

Ủy ban Châu Âu đưa ra định nghĩa về Thương mại điện tử như sau [12]: *Thương mại điện tử được hiểu là việc thực hiện hoạt động kinh doanh qua các phương tiện điện tử. Nó dựa trên việc xử lý và truyền dữ liệu điện tử dưới dạng text, âm thanh và hình ảnh. Thương mại điện tử gồm nhiều hành vi trong đó hoạt động mua bán hàng hóa và dịch vụ qua phương tiện điện tử, giao nhận các nội dung kỹ thuật số trên mạng, chuyển tiền điện tử, mua bán cổ phiếu điện tử, vận đơn điện tử, đấu giá thương mại, hợp tác thiết kế, tài nguyên mạng, mua sắm công cộng, tiếp thị trực tiếp tới người tiêu dùng và các dịch vụ sau bán hàng. Thương mại điện tử được thực hiện đối với cả thương mại hàng hóa (ví dụ như hàng tiêu dùng, các thiết bị y tế chuyên dụng) và thương mại dịch vụ (ví dụ như dịch vụ cung cấp thông tin, dịch vụ pháp lý, tài chính); các hoạt động truyền thống (như chăm sóc sức khỏe, giáo dục) và các hoạt động mới (ví dụ như siêu thị ảo).*

Tóm lại, *theo nghĩa rộng* thì thương mại điện tử có thể được hiểu là các giao dịch tài chính và thương mại bằng phương tiện điện tử như: trao đổi dữ liệu điện tử; chuyển tiền điện tử và các hoạt động gửi rút tiền bằng thẻ tín dụng.

Thương mại điện tử *theo nghĩa hẹp* bao gồm các hoạt động thương mại được thực hiện thông qua mạng Internet. Các tổ chức như: Tổ chức Thương mại thế giới (WTO), Tổ chức Hợp tác phát triển kinh tế đưa ra các khái niệm về thương mại điện tử theo hướng này. Thương mại điện tử được nói đến ở đây là hình thức mua bán hàng hóa được bày tại các trang Web trên Internet với phương thức thanh toán bằng thẻ tín dụng.

Để có một cách hiểu thống nhất, có thể định nghĩa :

Thương mại điện tử là việc ứng dụng các công nghệ thông tin để tiến hành các giao dịch mua – bán các sản phẩm, dịch vụ và thông tin thông qua các mạng máy tính có sử dụng các tiêu chuẩn truyền thông chung.

Thương mại điện tử sử dụng hệ thống mạng truyền thông số toàn cầu để tạo ra một thị trường điện tử cho tất cả các loại hình sản phẩm, dịch vụ, công nghệ và hàng hoá; bao hàm tất cả các hoạt động cần thiết để hoàn tất một thương vụ, trong đó có đàm phán, trao đổi chứng từ, truy cập thông tin từ các dịch vụ trợ giúp (thuế, bảo hiểm, vận tải...) và ngân hàng, tất cả được thực hiện trong các điều kiến an toàn và bảo mật. Trong thương mại điện tử, người ta hiện sử dụng các phương tiện chủ yếu như máy điện thoại, fax, hệ thống thiết bị thanh toán điện tử, mạng nội bộ (Inttranet), mạng ngoại bộ (Extranet) và mạng toàn cầu (Internet).

1.1.2 Giao dịch trong thương mại điện tử

[12]Giao dịch trong thương mại điện tử là một hệ thống bao gồm không chỉ các giao dịch liên quan đến mua bán hàng hóa và dịch vụ, tạo thu nhập, mà còn là các giao dịch có khả năng trợ giúp quá trình tạo ra thu nhập: kích thích nhu cầu đối với hàng hóa và dịch vụ, cung ứng dịch vụ trợ giúp bán hàng, trợ giúp người tiêu dùng, hoặc trợ giúp trao đổi thông tin giữa các doanh nghiệp.

Tính chất và nội dung của các giao dịch trong thương mại điện tử phụ thuộc nhiều vào việc chúng xảy ra trong môi trường của mô hình kinh doanh nào?

Hiện nay có hai mô hình kinh doanh cơ bản nhất được hầu hết các doanh nghiệp thương mại điện tử quan tâm [26]: thương mại điện tử giữa doanh nghiệp và người tiêu dùng (B2C), thương mại giữa các doanh nghiệp (B2B).

- ***Mô hình giao dịch B2C*** : Các doanh nghiệp bán các hàng hóa vật thể trực tiếp đến từng cá nhân người tiêu dùng cuối cùng. B2C đang trở nên phổ biến khi ngày càng nhiều người nhận ra sự thuận tiện của nó và khả năng đáp ứng nhanh những yêu cầu của khách hàng cũng như sự xuất hiện của vô số các dịch vụ B2C trên thị trường.
- ***Mô hình giao dịch B2B***: Các doanh nghiệp bán buôn thông qua các catalog bán hàng trực tuyến cho các doanh nghiệp khác. So với B2C, B2B liên quan đến giao dịch giữa các tổ chức. Một trong những mục tiêu chính của B2B là cải thiện một cách đáng kể việc cung cấp và trao đổi hàng hoá nhanh chóng, hiệu quả trong quá trính sản xuất. Hơn nữa viêc trao đổi hàng hoá trong B2B ngày càng có khuynh hướng bảo mật,việc trao đổi này cho phép các công ty buôn bán với các bạn hàng hiện tại trong một môi trường kinh doanh thuận lợi mà không cần phải đi qua một số giai đoạn ban đầu của chu trình B2B.

Quá trình mua bán trên mạng diễn ra bao gồm các giao dịch cơ bản sau:

- Thu hút khách hàng
- Tương tác với khách hàng
- Đặt hàng
- Thanh toán
- Thực hiện đơn đặt hàng
- Dịch vụ hỗ trợ

1.2. Giao dịch thanh toán điện tử

1.2.1. Giới thiệu chung

Xét trên nhiều phương diện, thanh toán trực tuyến là nền tảng của các hệ thống thương mại điện tử. Sự khác biệt cơ bản giữa thương mại điện tử với các ứng dụng khác mà Internet cung cấp chính là nhờ khả năng thanh toán trực tuyến này.

An toàn đang trở thành một trong những vấn đề được quan tâm nhất khi tiến hành thương mại điện tử. Mối lo ngại về an toàn trong thanh toán điện tử là một trong các lý do được đưa ra nhiều nhất dẫn đến người dùng không sử dụng phương thức thanh toán này. Do đó việc xác định rõ các yếu tố liên quan đến an toàn thanh toán điện tử và tìm ra các giải pháp công nghệ nhằm đáp ứng các yêu cầu trên là vấn đề quan trọng thúc đẩy sự phát triển của thương mại điện tử.

Bản chất của an toàn là một vấn đề phức tạp, liên quan đến nhiều khía cạnh khác nhau. Đối với an toàn thanh toán điện tử và các giao dịch trực tuyến, nói chung có năm khía cạnh cần giải quyết bao gồm: Tính sẵn dùng, tính xác thực, tính toàn vẹn, tính không chối bỏ, tính tin cậy.

Trong các hệ thống thanh toán điện tử trên Internet, nhiều giải pháp công nghệ cho phép thực hiện điều này. Kỹ thuật mã hóa thông tin, ***Chữ ký điện tử và chứng thực điện tử*** được sử dụng để đáp ứng các yêu cầu trên.

Trong không gian ảo (cyberspace), để có thể đảm bảo tính tin cậy, tính xác thực và riêng tư của các giao dịch cần phải áp dụng kỹ thuật mã hóa. Yêu cầu đặt ra đối với mỗi hệ thống thanh toán phụ thuộc vào những thông tin sẽ được mã hóa. Ví dụ, khi tiến hành các giao dịch mua – bán, để đảm bảo tính tin cậy của giao dịch, tất cả các thông tin được mã hóa bởi trình duyệt Web của khách hàng sẽ được chuyển tới máy chủ Web của người bán. Nhưng nếu người bán có thể giải mã toàn bộ thông tin này thì tính an toàn sẽ không được đảm bảo. Trong trường hợp người bán chỉ được phép giải mã các thông tin đặt hàng, còn có các thông tin liên quan đến thanh toán (như việc kiểm tra tài khóa n, số thẻ tín dụng...) đã được mã hóa sẽ được chuyển tới ngân hàng thanh toán được ủy quyền, thì chắc chắn những hành vi gian lận thương mại sẽ ít xảy ra hơn.

Trong thương mại điện tử, muốn đối phó với các hành vi gian lận, cần sử dụng những kỹ thuật để xác thực đối với người bán cũng như người mua và đảm bảo tính toàn vẹn của một người bán. Thí dụ, một người mua hàng cần có đủ bằng chứng giúp họ có thể tin tưởng vào người bán, tin tưởng vào những gì mà người này cung cấp. Vì vậy, cần sử dụng nhiều thủ tục để giải quyết vấn đề này như sử dụng chữ ký

điện tử nhằm xác thực các giao dịch điện tử, sử dụng các chứng chỉ điện tử khi nhận biết một doanh nghiệp.

1.2.2. Yêu cầu đối với các hệ thống thanh toán điện tử

Những yêu cầu đặt ra đối với các hệ thống thanh toán điện tử được chỉ ra dưới đây:

Tính an toàn (Security) – Tính an toàn bao gồm nhiều khía cạnh, từ vấn đề an toàn máy tính nói chung đến các công nghệ mã hóa. Sau đây là các vấn đề ảnh hưởng đến tính an toàn của một hệ thống thanh toán điện tử:

Tính trong suốt (Transperency) – Mô hình thanh toán và quá trình thanh toán phải dễ hiểu. Các thủ tục tự động thực hiện thay mặt cho vai trò người dùng và các chế tác tạo ra được thể hiện rõ ràng và dễ dàng chuyển cho các giao dịch tương ứng.

Tính mở (Extensibility) – Hệ thống thanh toán phải hỗ trợ và dễ dàng được chấp nhận bởi nhiều loại mô hình thương mại.

Chi phí giao dịch thấp (Low Transaction Costs) – Chi phí một giao dịch phải cân xứng với giá trị kinh tế được chuyển giao. Cần phải có sự cân bằng giữa yếu tố hiệu năng tính tính toàn nhằm hoàn thành giao dịch và các yêu cầu an toàn do các bên tham gia đưa ra.

Tính hiệu quả - Thuật toán sử dụng cần hiệu quả và phải hạn chế tối đa các truyền thông ngoài để quản lý giao dịch thanh toán. Các yêu cầu tính toán và lưu trữ từ phía người bán và nhà cung cấp dịch vụ thanh toán phải được giảm thiểu để duy trì dữ liệu khách hàng và đáp ứng các yêu cầu an toàn.

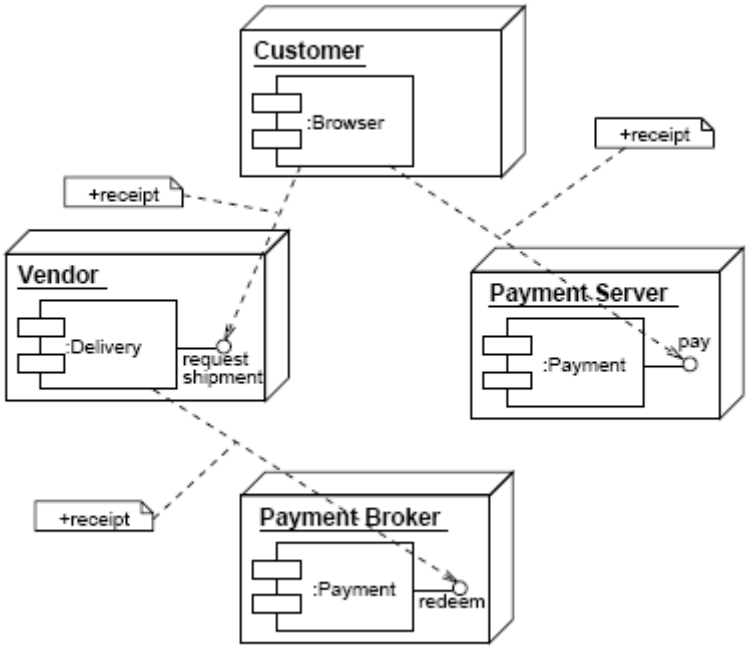
1.3. Thanh toán điện tử dùng chứng chỉ số và chữ ký số

1.3.1. Mô hình thanh toán dùng chứng chỉ số và chữ ký số

Để có mô hình thương mại linh hoạt hỗ trợ một hệ thống mang tính modul cao, chúng ta cần phân tách việc phân phối hàng hóa với thanh toán, và định nghĩa các cơ chế truyền thông giữa hai thành phần này (có thể đặt tại các node mạng khác nhau). Một phương pháp là sử dụng các chứng chỉ được ký (signed receipt) làm bằng chứng cho việc thanh toán trong truyền thông giữa các đối tác kinh doanh. Chứng chỉ là các khẳng định (statements) được bảo vệ bằng phương thức mã hóa.

Tùy vào chuẩn sử dụng, nó cho phép đảm bảo các thông tin về người giữ chứng chỉ, như tên, hay địa chỉ email. Nhưng chứng chỉ còn được dùng để đảm bảo các thuộc tính khác như gán quyền truy nhập cho người giữ chứng chỉ nếu họ chứng minh được quyền sở hữu. Xem "*chương 3 – chữ ký điện tử*" để có thêm thông tin về chứng chỉ và chữ ký số.

Cấu hình thanh toán tổng quát dùng chứng chỉ được mô tả trong hình 4.4

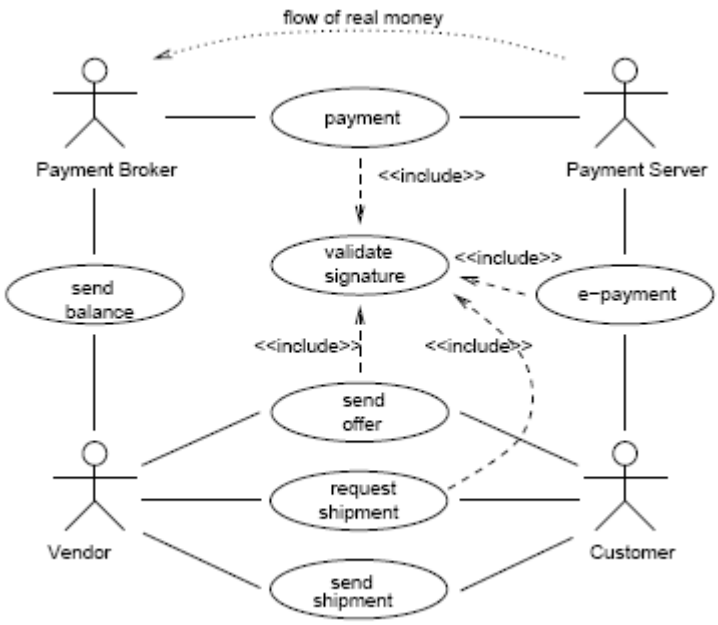


Hình 4.4: Mô hình tổng quát sử dụng chứng chỉ số

Trong mô hình tổng quát trên, chứng chỉ được dùng làm cơ sở trung tâm cho việc triển khai các mô hình thương mại, phụ thuộc vào dữ liệu nó lưu giữ và ngữ nghĩa gán cho dữ liệu này. Khách hàng có một tài khóa n tại một Server thanh toán (ví dụ như ISP) và nó dùng tài khóa n này để xác nhận thanh toán (thông qua giao diện thanh toán – "pay" Interface). Chứng chỉ Server thanh toán gửi lại cho khách hàng được dùng làm bằng chứng duy nhất cho việc thanh toán.

1.3.2. Hoạt động của mô hình thanh toán dùng chứng chỉ số và chữ ký số

Các tác nhân tham gia vào hoạt động của mô hình thanh toán tổng quát trong "Hình 4.4" được mô tả dưới dạng lược đồ Usecase như sau:



Hình 4.5: Các tác nhân tham gia trong mô hình thanh toán dùng chữ ký số

Quá trình hoạt động được thực hiện như sau:

▪ Người bán (Vendor) gửi lời chào hàng (offer) chứa thông tin muốn bán tới khách hàng (Customer).

▪ Dựa trên cơ sở các lời chào hàng nhận được, khách hàng yêu cầu một mặt hàng

▪ Tùy thuộc vào mô hình kinh doanh, khách hàng có thể phải trả trước hoặc sau khi mặt hàng được gửi đi, và phải trình diện một chứng chỉ làm bằng chứng cho việc thanh toán.

▪ Để tiến hành thanh toán, khách hàng liên lạc với Server thanh toán (Payment Server).

▪ Server thanh toán chấp nhận kýểu thanh toán và phát hành chứng chỉ được ký cho các thanh toán thành công.

▪ Server này được điều hành hoặc phối hợp với các môi giới thanh toán (Các trung tâm tài chính chịu trách nhiệm chuyển tiền thực từ tài khóa n của Server thanh toán tới tài khóa n của người bán). Nhận dạng của tất cả các bên tham gia có thể

được đảm bảo thông qua cơ sở hạ tầng khóa công khai (*Public Key Infrastructure - Pký*).

1.4. Kết luận

Chương này đã trình bày các vấn đề đối với thanh toán điện tử nhằm có một cái nhìn tổng quan về các hệ thống thanh toán đang được dùng trong thương mại điện tử hiện nay. Chương cũng đã mô tả phương pháp sử dụng chữ ký điện tử và chứng chỉ số để đảm bảo an toàn cho một giao dịch thanh toán. Đây cũng là cơ sở để xây dựng ứng dụng mô phỏng hệ thống thanh toán trong phần tiếp theo của đồ án.

CHƯƠNG II. CƠ SỞ TOÁN HỌC VÀ CÁC HỆ MÃ HÓA KHÓA CÔNG KHAI

2.1. Giới thiệu về lý thuyết số

Hầu hết các thuật toán mật mã khóa công khai được xây dựng dựa trên các khái niệm của lý thuyết số. Trong phần này tôi sẽ trình bày ngắn gọn những kiến thức cơ bản về lý thuyết số, nó là công cụ hữu ích để giúp các bạn hiểu sâu một thuật toán mật mã nào đó.

2.1.1. Các số nguyên tố và các số nguyên tố cùng nhau

2.1.1.1 Các ước số

Nói rằng, *b* (một số khác 0) là ước số của *a* nếu $a = mb$, với một giá trị *m* nào đó, ở đây *a, b, m* là các số nguyên. Như vậy, *b* là ước số của *a*, nếu như chia *a* cho *b* không còn lại số dư. Để kí hiệu *b* là ước số của *a* thường sử dụng cách viết $b \mid a$.

Có các quan hệ sau:

- Nếu $a \mid 1$, thì $a = \pm 1$.
- Nếu $b \mid a$ và $a \mid b$, thì $a = \pm b$.
- Số *b* bất kỳ khác 0 là ước số của 0.
- Nếu $b \mid g$ và $b \mid h$, thì $b \mid (mg + nh)$ đối với bất kì số nguyên *m, n*.

Để chứng minh khẳng định cuối cùng, cần chú ý như sau:

Nếu $b \mid g$ thì *g* có dạng $g = b * g_1$, đối với số nguyên g_1 nào đó,

Nếu $b \mid h$ thì *h* có dạng $h = b * h_1$, đối với giá trị nguyên h_1 nào đó,

Vì vậy: $mg + nh = mbg_1 + nbh_1 = b * (mg_1 + nh_1)$

Cuối cùng, *b* là ước số của $mg + nh$.

Ví dụ 2.1.1.1: Các số 2,3,5 là các ước số của 30.

2.1.1.2. Các số nguyên tố

Một số nguyên $p > 1$ được gọi là số nguyên tố, nếu chỉ có ± 1 và $\pm p$ là ước số của nó.

Một số nguyên bất kỳ $a > 1$ có thể phân tích thành các thừa số và được trình bày dưới dạng:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t},$$

Ở đây: $p_1 < p_2 < \ldots < p_t$ là các số nguyên tố, còn các giá trị $\alpha_i > 0$.

Ví dụ 2.1.1.2.1: $119 = 7 * 17$; $63 = 3^2 * 7$.

Nếu P là kí hiệu tập hợp tất cả các số nguyên tố, thì đối với một số nguyên dương bất kì được viết duy nhất dưới dạng:

$a = \prod_P p^{a_p}$, ở đây tất cả các $a_p \geq 0$

Trong công thức này, biểu thức ở vế phải sau dấu bằng, ký hiệu tích theo tất cả khả năng của các số nguyên tố p. Đối với mỗi giá trị cụ thể của a thì giá trị lớn nhất của chỉ số a_p sẽ bằng 0.

2.1.1.2.2: $3600 = 2^4 * 3^2 * 5^2$.

Các giá trị của một số nguyên dương bất kỳ có thể liệt kê dưới một dạng đơn giản của tất cả các chỉ số khác không theo công thức ở trên.

2.1.1.2.3: Số nguyên 12 có thể trình bày như $\{a_2 = 2, a_3 = 1\}$.

Số nguyên 18 có thể trình bày như $\{a_2 = 1, a_3 = 2\}$.

Phép nhân hai số nguyên tương đương với phép cộng các giá trị các chỉ số phù hợp:

$k = m * n \rightarrow k_p = m_p + n_p$, đối với tất cả các p.

2.1.1.2.4: $k = 12 * 18 = 216$,

$k_2 = 2 + 1 = 3$, $k_3 = 1 + 2 = 3$,

$216 = 2^3 * 3^3$

Bổ đề: Một số nguyên dương bất kì dạng p^k chỉ có thể chia hết cho một số nguyên, khi số bị chia có bậc của số nguyên tố p với chỉ số không vượt hơn k, nghĩa là số p^j với $j \leq k$. Như vậy:

$a \mid b \rightarrow a_p \leq b_p$, đối với tất cả p.

2.1.1.2.5: $a = 12$, $b = 36$, $12 \mid 36$, $12 = 2^2 * 3$, $36 = 2^2 * 3^2$

$a_2 = 2 = b_2$,

$a_3 = 1 \leq 2 = b_3$.

2.1.1.3. Các số nguyên tố cùng nhau

Chúng ta sẽ sử dụng ký hiệu gcd(a, b) để chỉ ước số chung lớn nhất (UCLN) của số a và b. Nói rằng, một số nguyên dương c là UCLN của a và b, nếu:

- c là ước số của a và b.
- Ước số bất kỳ của a và b đều là ước số của c.

Có thể định nghĩa tương đương như sau:

$\gcd(a, b) = \max [k,$ khi $k| a$ và $k| b]$.

Bởi vì, đòi hỏi rằng UCLN là một số dương, chúng ta có $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$. Nói chung, $\gcd(a, b) = \gcd(|a|, |b|)$.

Ví dụ 2.1.1.3.1: $\gcd(60, 24) = \gcd(60, -24) = 12$.

Bởi vì tất cả các số nguyên khác không đều là ước số của số 0, chúng ta luôn luôn có: $\gcd(a, 0) = |a|$.

Dễ dàng xác định được UCLN của hai số nguyên dương, nếu các số này được trình bày dưới dạng tích của các thừa số nguyên tố.

Ví dụ 2.1.1.3.2:

$300 = 2^2 * 3^1 * 5^2$,

$18 = 2^1 * 3^2$.

$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$.

Trong trường hợp chung:

$k = \gcd(a, b) \rightarrow k_p = \min (a_p, b_p)$, đối với tất cả các p.

Việc xác định các thừa số nguyên tố của các số lớn là bài toán không đơn giản, bởi vì rằng các trình bày ở trên không cho một khả năng thực tiễn để tính UCLN của hai số.

Các số nguyên a và b là nguyên tố cùng nhau, nếu chúng không có ước số nguyên tố chung, hay ước số chung duy nhất của chúng là 1. Nói một cách khác a và b là hai số nguyên tố cùng nhau nếu $\gcd(a, b) = 1$.

Ví dụ 2.1.1.3.3: Số 8 và số 15 là các số nguyên tố cùng nhau, bởi vì ước số của 8 là 1, 2, 4 và 8, còn các ước số của 15 là 1, 3, 5 và 15. Như vậy, 1 là ước số chung duy nhất của hai số này.

2.1.1.4. Số học trong lớp số dư

Đối với bất kỳ một số nguyên dương *n* và một số nguyên *a* bất kỳ, khi chia *a* cho *n*, ta nhận được một số nguyên *q* nào đó và số dư *r*, phù hợp với quan hệ sau:

$a = qn + r,\ 0 \le r < n,\ q = \lfloor a / n \rfloor.$

ở đây $\lfloor x \rfloor$ ký hiệu số nguyên lớn nhất, không lớn hơn *x*.

Đối với một số dương *a* và một số nguyên dương *n*, luôn luôn có thể tìm được *q* và *r*, phù hợp với quan hệ tính toán trên.

Ví dụ 2.1.1.4.1: $a = 11;\ n = 7;\ 11 = 1 * 7 + 4;\ r = 4.$

Nếu *a* là một số nguyên, còn *n* là một số nguyên dương, thì *a* mod *n*, được xác định như phần dư của phép chia *a* cho *n*. Như vậy, đối với một số nguyên *a* bất kỳ có thể viết :

$a = \lfloor a / n \rfloor * n + (a \bmod n)$

Ví dụ 2.1.1.4.2: 11 mod 7 = 4 ; –11 mod 7 = 3.

2.1.2. Lý thuyết về đồng dư

Định nghĩa 2.1.2 (Đồng dư)

Cho a,b∈Z, n∈N. Ta nói *a* đồng dư với *b* theo modulo *n*, khi *a* và *b* chia cho *n* có cùng số dư, và được viết dưới dạng sau:

$a \equiv b \bmod n$.

Chứng minh: Giả sử chia *a* và *b* cho *n* và thu được các thương nguyên và phần dư. Các phần dư nằm giữa 0 và *n* – 1, nghĩa là $a = q_1 n + r_1$ và $b = q_2 n + r_2$. Trong đó $0 \le r_1 \le n-1$ và $0 \le r_2 \le n-1$. Khi đó có thể dễ dàng thấy rằng $a \equiv b \bmod n$ khi và chỉ khi $r_1 = r_2$. Như vậy:a $a \equiv b \bmod n$ khi và chỉ khi $a \bmod n = b \bmod n$

2.1.3. Các số nguyên modulo n

Các số nguyên modulo *n* (ký hiệu Z_n) là tập hợp các số nguyên $\{0, 1, ..., n-1\}$ bao gồm 2 phép toán cộng và nhân. Việc cộng và nhân trong Z_n được

thực hiện giống như cộng và nhân các số nguyên, ngoại trừ một điểm là các kết quả sẽ được rút gọn theo modulo *n*.

Ví dụ 2.1.3: Tính $11*13$ trong Z_{16}. Tương tự như với các số nguyên ta có $11*13=143$. Để rút gọn 143 theo modulo 16, ta thực hiện phép chia bình thường: $143=8\times16+15$, bởi vậy $143 \bmod 16=15$. Do đó $11\times13=15$ trong Z_{16}.

Các định nghĩa trên phép cộng và phép nhân trong Z_n thoả mãn hầu hết các quy tắc quen thuộc trong số học. Sau đây ta sẽ liệt kê mà không chứng minh các tính chất này:

- Phép cộng là đóng, tức với bất kì $a, b \in Z_n$, $a+b \in Z_n$.
- Phép cộng là giao hoán, tức là với bất kì $a, b \in Z_n$ thì: $a + b = b + a$.
- Phép cộng là kết hợp, tức với bất kì $a, b, c \in Z_n$:

  $$(a + b) + c = a + (b + c).$$
- 0 là phần tử đơn vị của phép cộng, có nghĩa là với bất kì $a \in Z_n$:

  $$a + 0 = 0 + a = a.$$
- Phần tử nghịch đảo của phép cộng của một phần tử bất kì $a \in Z_n$ là $m – a$, nghĩa là $a + (m – a) = (m – a) + a = 0$ với bất kì $a \in Z_n$.
- Phép nhân là đóng, tức với bất kì $a, b \in Z_n$, $a * b \in Z_n$.
- Phép nhân là giao hoán, nghĩa là với bất kì $a, b \in Z_n$, $a * b = b * a$.
- Phép nhân là kết hợp, nghĩa là với $a, b, c \in Z_n$, $(a*b)*c=a*(b*c)$.
- 1 là phần tử đơn vị của phép nhân, tức là với bất kì $a \in Z_n$:

  $$a*1=1*a=a.$$
- Phép nhân có tính chất phân phối đối với phép cộng, tức là đối với $a, b, c \in Z_n$, $(a+b)*c=a*c+b*c$ và $a*(b+c)=a*b+a*c$.

2.1.4. Hàm Euler, định lý Euler và định lý Fermat

2.1.4.1. Hàm Euler, định lí Euler

Định nghĩa 2.1.4 (Hàm Euler)

Cho *n* là số nguyên dương, đặt $\phi(n)$ là số các phần tử của tập hợp, mà tập này là các số nguyên trong khoảng $[1, n]$ và nguyên tố cùng nhau với *n*, thì $\phi(n)$ gọi là hàm Euler.

Ta công nhận một số tính chất quan trọng của hàm Euler:

1. $\phi(1) = 1$
2. Nếu *p* là số nguyên tố thì $\phi(p) = p - 1$
3. Nếu như *p* và *q* là hai số nguyên tố cùng nhau thì $\phi(pq) = \phi(p) * \phi(q)$
4. $\phi(p^s) = p^{s-1}(p-1)$
5. Nếu như $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, ở đây p_1, p_2, …, p_k là số nguyên tố, thì

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

Định lý Euler: Cho *n> 1*, gcd*(a,n)* =1, và ϕ(n) là hàm Euler. Khi đó ta có:

$$a^{\phi(n)} \equiv 1 \bmod n$$

Ví dụ 2.1.4: *a* = 3, *n* = 10, $\phi(10) = 4$, $3^4 = 81 \equiv 1 \bmod 10$,

a = 2, *n* = 11, $\phi(11) = 10$, $2^{10} = 1024 \equiv 1 \bmod 11$.

Định lý Fermat nhỏ: Cho *p* là số nguyên tố, *a* là số nguyên dương không chia hết cho *p*. Khi đó ta có

$$a^{p-1} \equiv 1 \bmod p.$$

Chứng minh: Ta có $\phi(p) = p - 1$, áp dụng định lý Euler ta có điều phải chứng minh.

Từ định lý Fermat chúng ta có các hệ quả quan trọng sau:

1. Cho a∈Z, *p* là số nguyên tố, thì ta có: $a^p \equiv a \bmod p$

2. Cho a,b∈Z, *p* là số nguyên tố $(a+b)^n \equiv a^n+b^n$

2.1.5. Thuật toán Euclide và thuật toán Euclide mở rộng

2.1.5.1. Thuật toán Euclide

Định lý Euclide: Cho $a, b \in Z, b \neq 0$, tồn tại duy nhất cặp giá trị (*q*, *r*) với $q \in Z$ và $r \in N$ thỏa mãn:

$a = bq + r$, $0 \leq r < |b|$.ở đây *r* gọi là số dư.

Có một số ký hiệu cho số dư như sau:

$r = R_b(a)$, $r = a \bmod b$.

Một số tính chất đơn giản của về số dư:

1. $R_{-b}(a) = R_b(a)$, bởi vì

$$\left.\begin{array}{l} a = qb + r \\ 0 \leq r < |b| \end{array}\right\} \Leftrightarrow \begin{cases} a = (-q)(-b) + r \\ 0 \leq r < |b| \end{cases}$$

2. $R_b(a + ib) = R_b(a), \forall i \in Z$, bởi vì

$a + ib = (q + i)b + r$.

Nếu như *r* = 0 thì ta nói *a* chia hết cho *b*, ký hiệu là $a \vdots b$.

Định lý 2.1.5.1: Đối với bất kỳ các số $a, b, i \in Z$:

$$\gcd(a, b) = \gcd(a + ib, b) .$$

Định lý 2.1.5.2: Đối với bất kỳ $a, b \in Z, b \neq 0$, ta có:

$$\gcd(a, b) = \gcd(b, R_b(a))$$

Từ định lý 2.1.5.2 ta có thuật toán Euclide. Đây là thuật toán giúp tìm UCLN của hai số nguyên dương a_0 và a_1 với $a_0 > a_1$.

Thuật toán được miêu tả bằng dãy các phép chia như sau:

$a_0 = a_1 q_1 + a_2$, $0 < a_2 < a_1$

$a_1 = a_2 q_2 + a_3$, $0 < a_3 < a_2$

…

$a_{k-2} = a_{k-1}q_{k-1} + a_k,\ 0 < a_k < |a_{k-1}|$

$a_{k-1} = a_k q_k + 0$

Dựa vào định lý 2.1, nhận được gcd(a_0, a_1) = gcd(a_1, a_2) = … = gcd(a_k, 0) = a_k.

Ví dụ 2.16 (Thuật toán Euclide): Tìm gcd(814, 187).

Giải: Khai triển dãy phép tính theo thuật toán Euclide:

814 = 4 * 187 + 66

187 = 2 * 66 + 55

66 = 1 * 55 + 11

55 = 5 * 11 + 0

Vậy gcd(814, 187) = 11.

Thuật toán có thể viết như sau:

Vào: Hai số nguyên dương *a* và *b* với *a* > *b*

Ra: UCLN của *a* và *b*

While *b* # 0 do

r ← *a* mod *b*, *a* ← *b*, *b* ← *r*

Return (*a*).

2.1.5.2 Thuật toán Euclide mở rộng

Định nghĩa 2.1.5.2 (Phần tử nghịch đảo)

Cho $a \in Z_n$. Phần tử nghịch đảo của a là phần tử $b \in Z_n$ sao cho a*b ≡ b*a ≡ 1mod n. Kí hiệu phần tử nghịch đảo của a là a^{-1}.

Định lý 2.1.5.2: Cho số nguyên a > 0 nguyên tố cùng nhau với n, thì luôn tồn tại phần tử nghịch đảo của a theo modulo n.

Hệ quả 2.1.5.2: Nếu như p là số nguyên tố, thì bất kỳ số a, 0 < a < p, luôn tồn tại phần tử nghịch đảo theo modulo p.

Chúng ta sẽ tìm hiểu về cách tìm phần tử nghịch đảo thông qua thuật toán Euclide mở rộng.

Từ dãy chia của thuật toán Euclide

$a_0 = a_1q_1 + a_2$, $0 < a_2 < a_1$

$a_1 = a_2q_2 + a_3$, $0 < a_3 < a_2$

…

$a_{k-2} = a_{k-1}q_{k-1} + a_k$, $0 < a_k < a_{k-1}$

Ta dễ dàng rút ra dãy sau:

$a_k = a_{k-2} - q_{k-1}a_{k-1}$ mà $a_{k-1} = a_{k-3} - q_{k-2}a_{k-2}$ nên suy ra $a_k = a_{k-2} - q_{k-1}(a_{k-3} - q_{k-2}a_{k-2})$, tương tự như thế, chúng ta rút ra a_{k-2}, đến cuối cùng chúng ta có được biểu thức dạng sau:

$a_k = a_0x + a_1y$ (2.1)

Nếu như $\gcd(a_0, a_1) = 1$, chúng ta có x là phần tử nghịch đảo của a_0 theo modulo a_1.

Ví dụ 2.17 (Thuật toán Euclide mở rộng):

1. Tìm *x* và *y* trong biểu thức (2.1) với $a_0 = 814$ và $a_1 = 187$.

Giải: Theo ví dụ 2.16 ta thu được dãy:

814 = 4 * 187 + 66

187 = 2 * 66 + 55

66 = 1 * 55 + 11

55 = 5 * 11 + 0

Suy ra: 11 = 66 – 1 * 55 = 66 – 1 * (187 – 2 * 66) = 3 * 66 – 1 * 187 = 3 * (814 – 4 * 187) –187 = 3 * 814 – 13 * 187. Vậy *x* = 3 và *y* = –13.

2. Tìm phần tử nghịch đảo của 17 theo modulo 74.

Giải: Theo ví dụ trên ta có được 3 * 74 – 13 * 17 = 1. Nên phần tử nghich đảo của 17 là –13, nhưng chỉ lấy số dương, nên phần tử nghịch đảo của 17 là 74 – 13 = 61.

2.2. Tổng quan về hệ mã hóa khóa công khai

Vào năm 1874, William Stanley Jevons viết trong quyển *The Principles of Science* về mối liên hệ giữa các hàm một chiều và mật mã học. Đặc biệt, ông đã đi

sâu vào bài toán phân tích ra thừa số nguyên tố (sau này được sử dụng trong thuật toán RSA).

Liệu rằng bạn đọc có thể đoán được 2 số nguyên nào có tích bằng 8,616,460, 799? Tôi nghĩ rằng ngoài tôi ra thì không ai có thể biết kết quả được.
Năm 1976, Whitfield Diffie và Martin Hellman công bố bài báo New Directions in Cryptography, làm thay đổi căn bản về cách các hệ mật mã hoạt động. Bài báo đã đưa ra một hệ thống mã hóa bất đối xứng trong đó nêu ra phương pháp trao đổi khóa công khai, giải quyết các hạn chế của mã đối xứng.

Khác với mã đối xứng, mã hóa khóa bất đối xứng sử dụng một cặp khóa: **khóa công khai** (**public key**) và **khóa bí mật** (**private key**). Hai khóa này được xây dựng sao cho từ một khóa, rất khó có cách sinh ra được khóa còn lại. Một khóa sẽ dành để mã hóa, khóa còn lại dùng để giải mã. Chỉ có người sở hữu nắm được khóa bí mật trong khi khóa công khai được phổ biến rộng rãi. Hình vẽ sau minh họa việc mã hóa và giải mã

2.2.1. Nguyên lý cơ bản của hệ mật mã khoá công khai

- Hệ mật mã khoá công khai được xây dựng dựa trên ba quan điểm sau:

- Hệ mật mã khoá công khai dựa trên quan điểm hàm một chiều (one-way function) và khoá công khai, để biến đổi một bản rõ thành bản mã với thời gian tính toán hợp lý. Nhưng nếu muốn tính ngược lại (inverse function) thì phải mất nhiều thời gian, đến mức không thực hiện nổi. Vì vậy các hacker khó có thể tính toán để thu được bản rõ từ bản mã chặn được

- Một quan điểm khác dùng trong hệ mật mã khoá công khai đó là thông tin "cửa sập" (**trap door**) mà hàm một chiều phải có. Thông tin bí mật này (khoá riêng) chỉ có thể được đưa vào bởi người sở hữu cặp khóa. Khi có được thông tin "cửa sập" thì công việc giải mã sẽ trở nên dễ dàng.

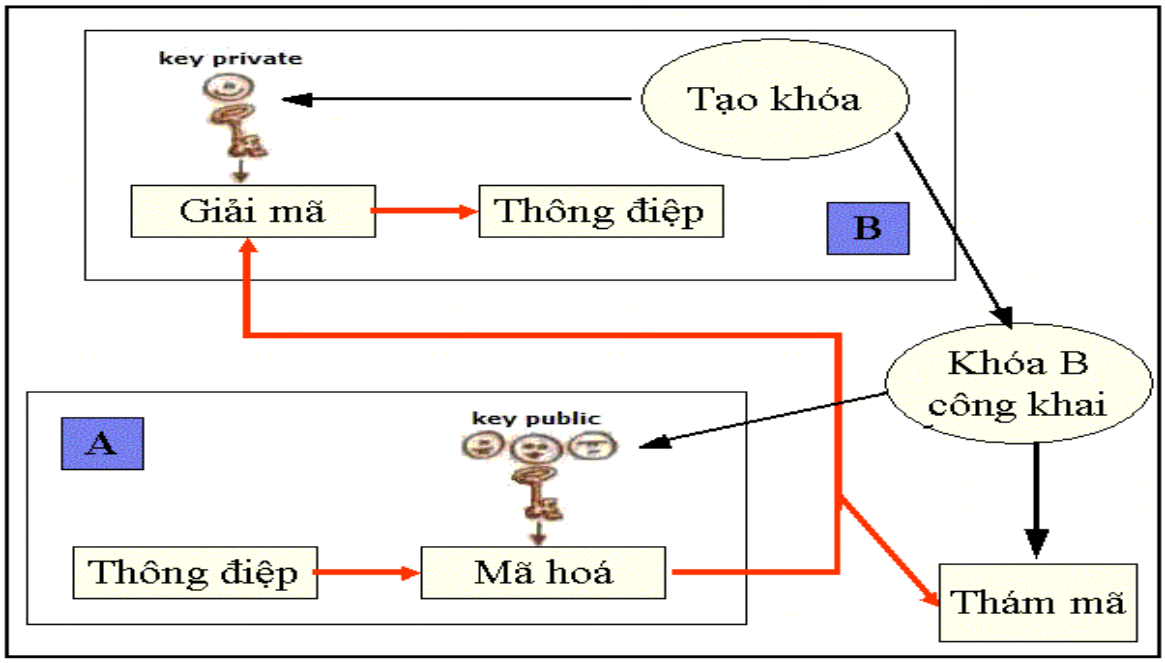
- Hầu hết các hệ mật mã khóa công khai được xây dựng dựa trên những bài toán khó đã biết như:, hệ ElGamal dựa trên bài toán logarithm rời rạc trong trường hữu hạn Z_p và hệ RSA dựa trên bài toán phân tích một số nguyên lớn ra các thừa số nguyên tố.

2.2.2. Hoạt động của hệ mật mã khóa công khai

Trong hệ thống mã hóa khóa công khai, mỗi người sử dụng đều tạo riêng cho mình một cặp khóa. Trong đó, một khóa gọi là khóa công khai (public key) cùng với thuật toán mã hóa **E**, được công bố rộng rãi tại thư mục dùng chung cho mọi người sử dụng (giống như số điện thoại). Khóa còn lại gọi là khóa riêng (private key) và thuật toán giải mã **D** được giữ bí mật bởi từng người sử dụng.

Giả sử người A muốn gửi thông điệp M đến người B (Hình 5). Người A sẽ tìm khóa công khai $\mathbf{k_{eB}}$ của người B trong thư mục dùng chung, và tính $C = E_{keB}(M)$ rồi gửi bản mã C cho người nhận B. Khi nhận được bản mã C, người B sẽ giải mã dựa vào khóa riêng $\mathbf{k_{dB}}$ của mình để tính $M=D_{kdB}(C)$. Trong quá trình trao đổi, mặc dù người thám mã có thể chặn được bản mã C, và biết khóa lập mã $\mathbf{k_{eB}}$, nhưng để giải mã thông điệp, họ phải đối mặt với bài toán rất khó đến mức không thể giải nổi.

Như vậy hệ thống mã hóa khóa công khai đã loại bỏ được sự cần thiết phải có kỹ thuật quản lý và phân phối khóa phức tạp như ở hệ thống mã hóa khóa đối xứng. Do tất cả các thành viên đều có thể dùng khóa công khai của thành viên khác để mã hóa thông tin gửi cho họ. Nhưng chỉ có duy nhất một thành viên có khóa riêng tương ứng, mới giải mã được thông điệp.

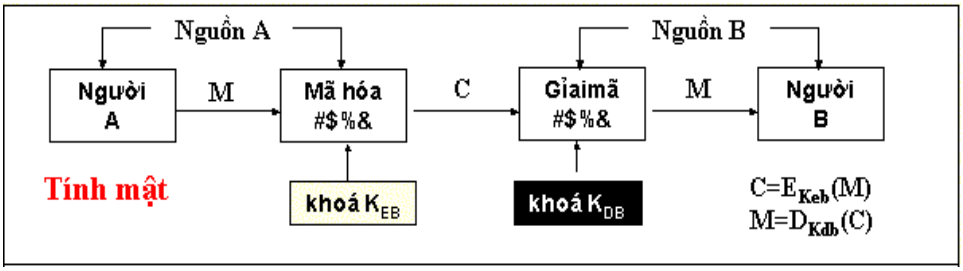


Hình 2.1: Sơ đồ hoạt động của hệ mật mã khoá công khai

2.2.3. Khả năng ứng dụng của hệ mật mã khóa công khai.

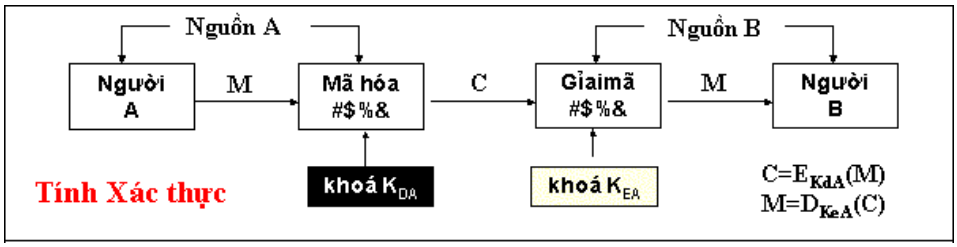
Tùy thuộc vào những lĩnh vực ứng dụng cụ thể mà người gửi sử dụng khóa bí mật của mình, khóa công khai của người nhận hoặc cả hai để hình thành một số các mô hình ứng dụng phù hợp như sau.

Mã hoá và giải mã: người gửi A thực hiện mã hóa thông điệp M bằng khóa công khai k_{eB} của người nhận B: $C = E_{keB}(M)$. Còn người nhận giải mã bằng khóa riêng k_{dB} của mình: $M = Dk_{dB}(C)$. Như vậy chỉ có duy nhất người B mới giải mã được thông điệp, điều này gọi là **tính mật** của hệ.



Hình 2.2: Sơ đồ minh họa tính mật của hệ mật mã khóa công khai

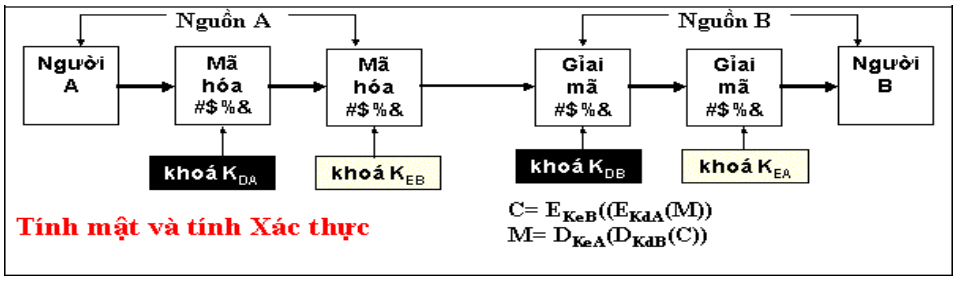
Chữ ký điện tử: người gửi A thực hiện mã hóa (hay ký) một thông điệp M bằng khóa riêng k_{dA}: $C = E_{kdA}(M)$. Người nhận B giải mã bằng khóa công khai k_{eA} của người gửi A: $M = D_{keA}(C)$. Như vậy chỉ có duy nhất A là người có khóa riêng để mã hóa, cho nên thông điệp nhận được là của A, điều này gọi là **tính xác thực** của hệ.



Hình 2.3: Sơ đồ minh họa tính xác thực của hệ mật mã khóa công khai

Chuyển đổi khóa: người gửi A thực hiện mã hoá thông điệp hai lần, lần thứ nhất sử dụng khóa bí mật k_{dA} của mình $E_{kdA}(M)$, lần thứ hai sử dụng khóa công khai k_{eB} của người nhận B: $E_{keB}(E_{kdA}(M))$. Khi nhận bản mã, người nhận B cũng thực hiện giải mã hai lần, đầu tiên dùng khóa riêng k_{dB} của mình $D_{kdB}(E_{keB}[E_{kdA}(M)])$, sau đó dùng khóa công khai k_{eA} của người gửi A: $D_{keA}\{D_{kdB}(E_{keB}[E_{kdA}(M)])\} = M$.

Như vậy chỉ người gửi mới có khóa riêng để mã hoá và cũng chỉ người nhận mới có khóa riêng để giải mã, đây chính là **tính xác thực và tính mật** của hệ.



Hình 2.4: Sơ đồ minh họa tính mật và tính xác thực của hệ mã khóa công khai

2.2.4. Các yêu cầu của hệ mật mã khóa công khai

- Công việc tính toán thì dễ dàng đối với các thành viên khi muốn tạo một cặp khóa (bao gồm khóa công khai k_e và khóa riêng k_d)
- Công việc tính toán thì dễ dàng cho người gửi, khi biết khóa công khai và thông điệp M cần mã hoá thành một bản mã tương ứng $C = E_{Ke}(M)$.
- Công việc tính toán thì dễ cho người nhận, sử dụng khóa riêng để giải mã bản mã C, khôi phục lại đoạn tin ban đầu: $M = D_{KdB}(C) = D_{kdB}\ [E_{KeB}(C)]$.
- Tính toán không tính nổi đối với người thám mã, khi biết được khóa công khai k_e, muốn xác định khóa bí mật k_d.
- Tính toán không tính nổi, đối với các thám mã khi biết được khóa công khai k_e và bản mã C để khôi phục lại thông điệp M ban đầu.

Nhận xét: Hệ thống mã hóa khóa công khai không hẳn là đảm bảo được tính an toàn tuyệt đối. Bởi vì với một bản mã C quan sát được, về mặt lý thuyết người thám mã đều có thể tìm ra bản rõ M sao cho C là bản mã được mã hóa từ bản rõ M. Tuy nhiên, việc giải bài toán ngược là rất khó, mất rất nhiều thời gian.

2.3. Kỹ thuật mã hóa khóa công khai

Mã hóa khóa đối xứng đã và đang được sử dụng rất rộng rãi, tạo ra nhiều hệ thống liên lạc một cách an toàn qua mạng công cộng. Tuy nhiên, mã hóa khóa đối xứng gặp một số vấn đề, đặc biệt đối với các hệ thống lớn:

Vấn đề quản lý khóa (Tạo, lưu mật, trao chuyển …) là rất phức tạp và ngày càng khó khi sử dụng trong môi trường trao đổi tin giữa rất nhiều người dùng. Với

số lượng user là n thì số lượng khóa cần tạo lập là n(n - 1)/2. Mỗi người dùng phải tạo và lưu (n-1) khóa bí mật để làm việc với (n-1) người khác trên mạng. Như vậy rất khó khăn và không an toàn khi n tăng lớn.

Vấn đề thứ hai là trên cơ sở mã đối xứng, không thể thiết lập được khái niệm chữ ký điện tử (mà thể hiện được các chức năng của chữ ký tay trong thực tế) và cũng do đó không có dịch vụ không thể phủ nhận được (non - repudiation) cho các giao dịch thương mại trên mạng.

Xuất phát từ sự hạn chế của phương pháp mã hoá đối xứng, *mã khóa công khai* hay *mã hoá bất đối xứng* (*asymmetric algorithm*) đã ra đời và nhanh chóng tạo ra một cuộc cách mạng trong toàn bộ lịch sử mã hoá.

2.3.1. Mã khóa công khai

Diffie và Hellman trong các công trình của mình (1975 - 1976) đã đề xuất một loại hệ mã với nguyên tắc mới gọi là hệ mã với khóa công khai (public key cryptosystems), trong đó hệ mã được gắn với một người sử dụng (user) nhất định chứ không phải gắn với một cuộc truyền tin giữa một cặp người dùng.

Trong hệ thống mã hóa khóa công khai, mỗi user có hai khóa , một được gọi là khóa bí mật (secret key hay private key) và một được gọi là khóa công khai (public key). khóa thứ nhất chỉ mình user biết và giữ bí mật, khóa thứ hai được phổ biến công khai. khóa thứ nhất thường đi liền với thuật toán giải mã, còn khóa thứ hai thường đi liền với thuật toán sinh mã, tuy nhiên điều đó không phải là bắt buộc. ký hiệu z là khóa riêng và Z là khóa công khai.

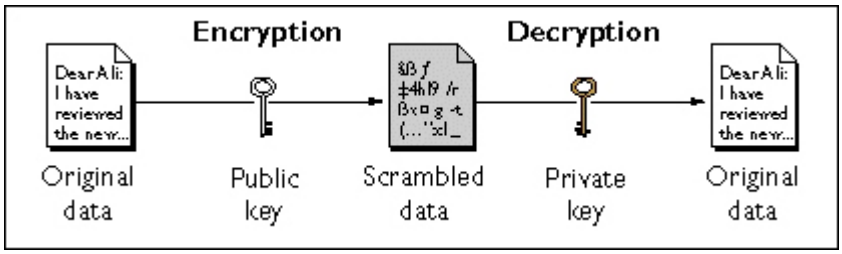
Hoạt động của chúng là đối xứng:

$$X = D(z, E(Z,X)) \qquad (1)$$

$$\text{Và} \qquad X = E(Z, D(z,X)) \qquad (2)$$

Trong đó (1) được sử dụng cho truyền tin mật : B, C, D muốn gửi tin cho A chỉ việc mã hóa thông tin với khóa công khai (ZA) của A rồi gửi đi. Chỉ có A mới có thể có khóa riêng để giải mã (zA) và đọc được tin, E dù nghe trộm cũng không thể giải mã để lấy được tin vì không có khóa zA.

Còn (2) sẽ được sử dụng để xây dựng các hệ chữ ký điện tử (Ký bằng E(ZA) và kiểm định bằng D(zA)).



Hình 2.10: Sơ đồ minh hoạ Public-key Crytography

2.3.2. Nguyên tắc cấu tạo một hệ khóa công khai

Một hệ mã PKC có thể được tạo dựng trên cơ sở sử dụng một hàm kiểu one – way (một chiều). Một hàm f được gọi là one – way nếu:

- Đối với mọi X tính ra Y = f(X) là dễ dàng;
- Khi biết Y rất khó để tính ra X.

Cần một hàm one – way đặc biệt mà có trang bị một trap – door (cửa bẫy), sao cho nếu biết trap – door thì việc tính X khi biết f(X) là dễ dàng còn ngược lại sẽ khó khăn.

Một hàm one – way có trap – door như thế có thể dùng để tạo một hệ mã PKC. Lấy E_z (hàm sinh mã) là hàm one – way có trap – door. Trap – door chính là khóa bí mật, mà nếu biết nó thì có thể dễ dàng tính được nghịch đảo của E_z tức là biết D_z, còn nếu không biết thì rất khó tính được.

Những giải thuật khóa công khai dựa vào khóa công khai để mã hoá và khóa bí mật có liên quan để giải mã. Như vậy, mỗi người tham gia vào hệ thống đều có hai khóa : khóa mã hoá E và khóa giải mã D.

Những giải thuật này có những đặc tính quan trọng sau:

- D(E(P)) = P (Plaintext - bản tin mã hoá)
- Khối lượng tính toán không khả thi để xác định khóa giải mã D khi chỉ biết giải thuật mật mã và khóa mã hóa E.
- Không thể phát hiện khóa mã hoá E từ bản tin P chọn sẵn
- Trong một số giải thuật như RSA còn có đặc điểm: hoặc một trong hai khóa liên quan có thể được sử dụng cho mã hóa còn khóa kýa được dùng cho giải mã.

• Ngoài ra có một đặc tính khác, đó là việc tính toán cho các bên tạo cặp khóa mã hoá - giải mã, việc tính toán khi biết bản tin cần mã hoá và khóa công khai của bên kýa để tạo bản mã tương ứng, việc sử dụng bản tin đã được mã hoá và khóa bí mật của mình để khôi phục bản tin ban đầu phải dễ dàng thực hiện và với tốc độ cao.

Các bước cần thiết trong quá trình mã hóa khóa công khai:

• Mỗi hệ thống đầu cuối trong mạng tạo ra một cặp khóa để dùng cho mã hóa và giải mã đoạn tin mà nó sẽ nhận.

• Mỗi hệ thống công bố rộng rãi khóa mã hóa bằng cách đặt khóa vào một thanh ghi hay một file công khai. Đây là khóa công khai (*public key*), khóa còn lại được giữ riêng (*private key*).

• Nếu A muốn gửi một đoạn tin P tới B thì A mã hóa đoạn tin bằng khóa công khai E_B của B (gửi $E_B(P)$ cho B).

• Khi B nhận đoạn tin mã hóa, nó giải mã bằng khóa bí mật D_B của mình (tính $D_B(E_B(P))=P$). Không một người nào khác có thể giải mã đoạn tin mã này bởi vì chỉ có mình B biết khóa bí mật đó thôi.

Với cách tiếp cận này, tất cả những người tham gia có thể truy xuất khóa công khai. khóa riêng được tạo ra bởi từng cá nhân, vì vậy không bao giờ được công bố. Ở bất kỳ thời điểm nào, hệ thống cũng có thể thay đổi khóa riêng của nó và công bố khóa công khai tương ứng để thay thế khóa công khai cũ.

2.4. Tổng kết chương 2

Qua chương này chúng ta đã nắm được các cơ sở toán học là cơ sở để nghiên cứu các hệ mật mã hóa khóa công khai và chữ kí số. Tìm hiểu khái quát về hệ mã hóa khóa công khai nói chung và hệ mã hóa khóa công khai RSA nói riêng. Nghiên cứu về chữ ký số, các yêu cầu đối với một hệ chữ ký và lược đồ chung của chữ ký số.

CHƯƠNG III. CHỮ KÝ SỐ VÀ HÀM BĂM

Hệ mật mã khóa công khai RSA là hệ mật mã đầu tiên dựa vào phương pháp mã hóa khóa bất đối xứng, được đưa ra vào năm 1977 bởi các giáo sư Ronald Rivest, Adi Shamir, và Leonard Adleman, nhằm sử dụng cho cả hai mục đích bảo mật thông tin và chữ ký điện tử. Hệ mật mã này được thiết kế làm việc trên trường số Z_N, có độ an toàn phụ thuộc vào độ khó giải bài toán phân tích số nguyên N lớn ra các thừa số nguyên tố.

Vấn đề của thực tiễn trong thanh toán điện tử là làm sao xác thực được việc thanh toán đó có bị giả mạo hay không, hay có một tác nhân nào đó cố tình làm thay đổi những dữ liệu trong quá trình thanh toán đó. Hàm băm (hash) sẽ giúp chúng ta giải quyết vấn đề này. Hàm băm (hash), là một thuật toán dùng để biến một thông điệp ở đầu vào (input) có chiều dài thay đổi bất kỳ, thành một giá trị ở đầu ra (output) có chiều dài cố định, giá trị đầu ra(output) được gọi là giá trị **hash**. Hàm băm được sử dụng trong rất nhiều lĩnh vực tính toán, mật mã là một trong số đó.

3.1. Bài toán phân tích số nguyên

Bài toán phân tích số nguyên là một trong những bài toán được quan tâm đến những năm gần đây, độ an toàn của nhiều kỹ thuật mật mã phụ thuộc vào sự không giải nổi của bài toán này như hệ mật mã RSA, lược đồ chữ ký RSA…

Bài toán 1 (Bài toán phân tích số nguyên): Cho một số nguyên dương N, tìm các thừa số nguyên tố của N. Nghĩa là, $N = p_1^{e1}, p_2^{e2}, \ldots p_k^{ek}$, với p_i là những số nguyên tố phân biệt và $e_i \geq 1$ (với i = 1,..., k).

Bài toán này được tin tưởng là khó giải khi N là một số nguyên lớn, có nhiều thuật toán để giải bài toán này. Nhưng hiện nay vẫn chưa có thuật toán nào hiệu quả để phân tích số nguyên N có khoảng 232 chữ số thập phân (768-bits) trở lên.

Bài toán 2 (Bài toán RSA): Cho số nguyên dương N là tích của hai số nguyên tố phân biệt p và q ($N = p * q$), số nguyên e sao cho thỏa mãn $\gcd(e, (p - 1) * (q - 1)) = 1$, và số nguyên c. Tìm một số nguyên m sao cho $m^e \equiv c \pmod N$.

Rõ ràng bài toán RSA cũng có độ khó tương tự như bài toán phân tích số nguyên, nhưng nó dễ dàng được giải nếu như biết được hai số nguyên tố p và q.

3.2. Mô tả các quá trình tạo khoá, mã hoá và giải mã

3.2.1. Tạo khóa

Để sử dụng được hệ mật mã khóa công khai RSA, trước tiên mỗi người phải tạo riêng cho mình một cặp khóa gồm khóa công khai, và khóa riêng như sau:

- Tạo hai số nguyên tố phân biệt p và q lớn, sao cho bài toán phân tích thật sự là khó giải (kích cỡ mỗi số khoảng 512 bits $\rightarrow$ 1024 bits).
- Tính N = p$*$ q và ϕ(N) = (p – 1) $*$ (q – 1), (*ϕ(N) là Euluer Totient Function*)
- Chọn một số nguyên ngẫu nhiên e sao cho 1 < e < ϕ(N) và gcd(e, ϕ(N)) = 1
- Sử dụng thuật toán Euclide mở rộng, để tính số nguyên d duy nhất, sao cho 0 < d < ϕ(N) và e $*$ d $\equiv$ 1 mod ϕ(N) (d là nghịch đảo của e modulo N)
- Công bố hai số (e, N) làm khóa công khai, còn (d, N) được giữ bí mật làm khóa riêng. Các số nguyên tố p, q sẽ bị xóa khi kết thúc quá trình tạo khóa.
- Mã hóa:

Hệ RSA là một hệ mật mã điển hình về kiểu mã hóa khối. Nghĩa là, thông điệp được chia thành nhiều khối (hoặc chuỗi) có chiều dài cố định, và mỗi khối sẽ được mã hóa riêng. Giả sử để gửi thông điệp bí mật M cho người B trong nhóm gửi thông tin an toàn, người A phải thực hiện các bước như sau:

- Lấy khóa công khai đích thực của người nhận B (e, N).
- Thực hiện một thuật toán để biến đổi thông điệp **m** thành những số nguyên M_i tương ứng sao cho M_i < N, (i = 1,…, k). ví dụ như phép biến đổi sau:

– Biến đổi các ký tự trong thông điệp **m** thành các số nguyên theo qui tắc: $\cup \leftrightarrow$ 00, A $\leftrightarrow$ 01, B $\leftrightarrow$ 02,…, Z $\leftrightarrow$ 26 (với $\cup$ là khoảng trắng).

– Chia thông điệp vừa biến đổi thành k nhóm có chiều dài bằng nhau, mỗi nhóm biểu diễn một số nguyên $M_i \in \{0,\ldots, N-1\}$ (với $1 \leq i \leq k$).

- Thực hiện mã hóa lần lượt cho từng số $M_i \rightarrow C_i$ bằng cách tính:

$C_i = E_{ke}(M_i) = M_i^e \pmod N$.

Tập các số nguyên $\{C_1, C_2,...,C_k\}$ là bản mã để gửi đến người nhận B.

- Giải mã:

Để thực hiện quá trình giải mã, khôi phục lại nội dung của thông điệp M từ bản mã C nhận được, người nhận B sẽ thực hiện các bước như sau:

- Thực hiện giải mã lần lượt cho từng số nguyên $C_i \rightarrow M_i$ bằng cách tính:

  $M_i = D(C_i) = C_i^d \pmod N$ với $0 \leq M_i < N$, (d là khoá bí mật của B).

- Thực hiện phép biến đổi ngược lại từ các số M_i thành các chuỗi ký tự tương ứng, để khôi phục lại nội dung thông điệp M ban đầu.

Bảng 3: Bảng tóm tắt các bước tạo khoá, mã hoá, giải mã của hệ RSA

Tạo khoá:

- Tạo 2 số nguyên tố lớn p và q
- Tính N = p * q và
  Tính ϕ(N) = (p-1) * (q-1).
- Chọn 1<e<ϕ(N): gcd(ϕ(N), e) = 1.
- Tính $d = e^{-1} \bmod \phi(N)$

(dùng thuật toán Euclidean mở rộng).

- **Khóa công khai:** $k_e = (e, N)$
- **Khóa riêng:** $k_d = (d, N)$

Mã hóa: khối bản rõ M < N

- Tính: $\mathbf{C = M^e \bmod N}$

Gửi khối bản mã (số nguyên) C đến người nhận

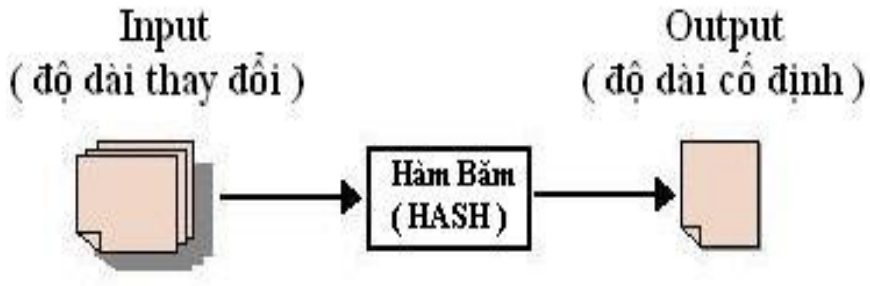
Giải mã: khối bản mã C < N

- Tính: $\mathbf{M = C^d \bmod N}$

khôi phục lại khối bản rõ (số nguyên) M ban đầu

3.2.2. Hàm băm

Hàm băm (hash), là một thuật toán dùng để biến một thông điệp **M** ở đầu vào (input) có chiều dài thay đổi bất kỳ, thành một giá trị **h** ở đầu ra (output) có chiều dài cố định, **h** được gọi là giá trị **hash**. Hàm băm được sử dụng trong rất nhiều lĩnh vực tính toán, mật mã là một trong số đó.



Hình 2.5: Sơ đồ minh họa hàm băm (HASH)

◆ Hai ứng dụng phổ biến nhất của hàm hash trong lĩnh vực mật mã là:

• Nén thông điệp thành một khối nhỏ có chiều dài xác định, phục vụ cho các lược đồ chữ ký điện tử, khối dữ liệu nhỏ này gọi là thông điệp thu gọn (Message Digest). Ví dụ như chữ ký điện tử DSA (Digital Signature Algorithm) dùng hàm băm SHA-1 để tạo thông điệp thu gọn dài 160-bits.

• Kiểm tra tính toàn vẹn dữ liệu (Data Integrity), nghĩa là kiểm tra xem dữ liệu có bị thay đổi trên đường truyền hay không, bằng cách tạo mã chứng thực thông điệp MAC (Message Authentication Code).

3.2.2.1. Yêu cầu của một hàm băm

◆ Hàm hash dùng trong lĩnh vực mật mã phải thỏa các tiêu chuẩn sau:

• Thông điệp (Message) ở đầu vào có chiều dài bất kỳ.

• Thông điệp thu gọn (Message digest) đầu ra có chiều dài cố định (đủ nhỏ).

• Hàm băm H(x) dễ dàng tính toán cho mọi thông điệp x

• Hàm băm H(x) là hàm một chiều (one-way-function): cho trước một giá trị hash **h** thì khó tính toán để tìm ra thông điệp ở đầu vào x sao cho H(x) = h.

• Đụng độ (collision-free): hàm băm H(x) có hai cấp đụng độ là:

• Đụng độ cấp độ yếu (Weakly collision-free): cho trước thông điệp **x**, không thể tính toán tìm ra một thông điệp **y** khác **x** mà H(x) = H(y).

• Đụng độ cấp độ mạnh (Strongly collision-free): không thể tính toán để tìm ra hai thông điệp bất kỳ **x** và **y** khác nhau, mà có cùng giá trị **hash**, nghĩa là H(x) = H(y).

3.2.2.2. Ứng dụng hàm băm

Các hàm băm được ứng dụng trong nhiều lĩnh vực, chúng thường được thiết kế phù hợp với từng ứng dụng. Ví dụ, các hàm băm mật mã học giả thiết sự tồn tại của một đối phương – người có thể cố tình tìm các dữ liệu vào với cùng một giá trị băm. Một hàm băm tốt là một phép biến đổi "một chiều", nghĩa là không có một phương pháp thực tiễn để tính toán được dữ liệu vào nào đó tương ứng với giá trị băm mong muốn, khi đó việc giả mạo sẽ rất khó khăn. Một hàm một chiều mật mã học điển hình không có tính chất hàm đơn ánh và tạo nên một hàm băm hiệu quả; một hàm trapdoor mật mã học điển hình là hàm đơn ánh và tạo nên một hàm ngẫu nhiên hiệu quả.

Bảng băm, một ứng dụng quan trọng của các hàm băm, cho phép tra cứu nhanh một bản ghi dữ liệu nếu cho trước khóa của bản ghi đó (Lưu ý: các khóa này thường không bí mật như trong mật mã học, nhưng cả hai đều được dùng để "mở khóa" hoặc để truy nhập thông tin.) Ví dụ, các khóa trong một từ điển điện tử Anh-Anh có thể là các từ tiếng Anh, các bản ghi tương ứng với chúng chứa các định nghĩa. Trong trường hợp này, hàm băm phải ánh xạ các xâu chữ cái tới các chỉ mục của mảng nội bộ của bảng băm.

Các hàm băm dành cho việc phát hiện và sửa lỗi tập trung phân biệt các trường hợp mà dữ liệu đã bị làm nhiễu bởi các quá trình ngẫu nhiên. Khi các hàm băm được dùng cho các giá trị tổng kiểm, giá trị băm tương đối nhỏ có thể được dùng để kiểm chứng rằng một file dữ liệu có kích thước tùy ý chưa bị sửa đổi. Hàm băm được dùng để phát hiện lỗi truyền dữ liệu. Tại nơi gửi, hàm băm được tính cho dữ liệu được gửi, giá trị băm này được gửi cùng dữ liệu. Tại đầu nhận, hàm băm lại được tính lần nữa, nếu các giá trị băm không trùng nhau thì lỗi đã xảy ra ở đâu đó trong quá trình truyền. Việc này được gọi là kiểm tra dư (redundancy check).

Các hàm băm còn được ứng dụng trong việc nhận dạng âm thanh, chẳng hạn như xác định xem một file MP3 có khớp với một file trong danh sách một loại các file khác hay không.

3.2.3. Chữ ký số

Trong giao dịch điện tử nói chung và thương mại điện tử nói riêng, quá trình trao đổi thông tin tương tác giữa các thành viên, đòi hỏi phải có một cơ chế hay hệ thống xác định nguồn gốc chủ sở hữu của thông tin. Giống như trong lĩnh vực tài liệu thông thường, nếu như chữ ký viết tay là để chứng minh tác giả hay người công nhận nội dung của tài liệu, thì lĩnh vực tài liệu điện tử cũng có một tiêu chuẩn như vậy về "chữ ký", gọi là chữ ký điện tử (digital signature).

Chữ ký điện tử là một đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc. Về nguyên tắc của chữ ký điện tử cũng gần như chữ ký thông thường, ví dụ như nếu người A muốn gửi thông điệp cho người B, thì A sẽ gửi chữ ký cùng với thông điệp của mình cho B. Khi nhận được thông điệp và chữ ký, bằng cách nào đó để B có thể xác định chữ ký kèm theo thông điệp có phải của người A hay không. Điểm khác biệt giữa chữ ký điện tử và chữ ký thông thường là: chữ ký thông thường thì nằm bên trong thông điệp, và chữ ký của một người là luôn giống nhau ở mọi thông điệp, còn chữ ký điện tử thì được gửi kèm với thông điệp nhưng tách biệt, và chữ ký của một người cho các thông điệp khác nhau là hoàn toàn khác nhau.

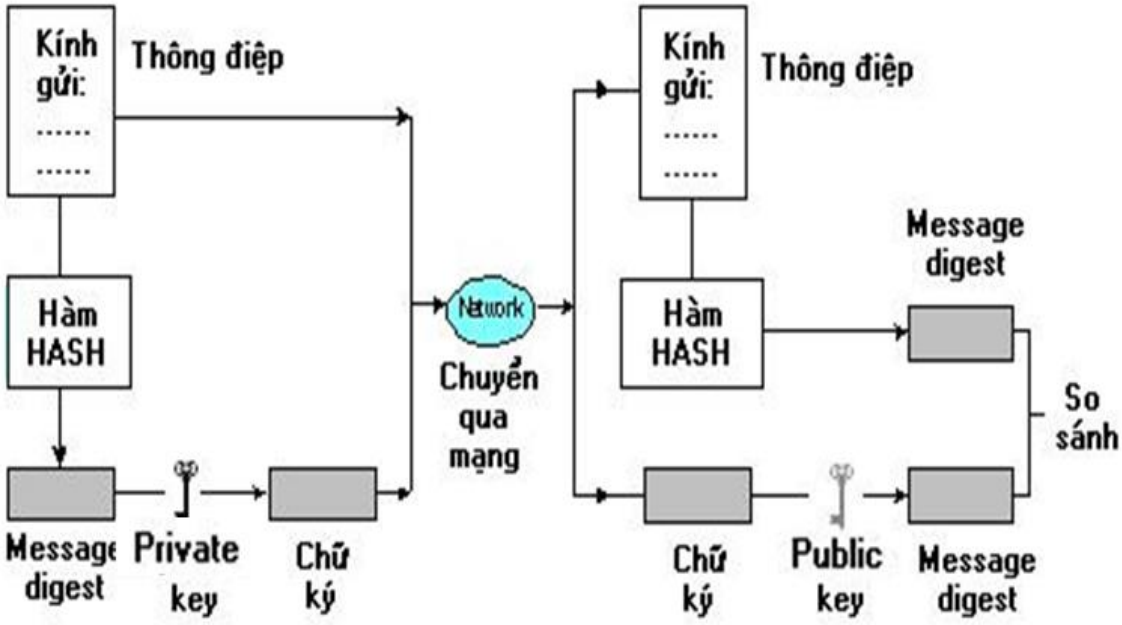
3.2.3.1. Yêu cầu của một hệ thống chữ ký điện tử

- Hệ thống chữ ký điện tử cần thỏa mãn các yêu cầu sau :

- Tính an toàn (security): chữ ký không thể làm giả được nếu không biết thông tin bí mật (private key) để tạo ra chữ ký.
- Tính hiệu quả (performance): ký và xác nhận chữ ký nhanh, dễ dàng.
- Chống nhân bản chữ ký: chữ ký không thể sao chép để dùng lại sau này. Ví dụ A ký chứng nhận cho phép B rút một số tiền, cần phải có cách nào đó để B không thể dùng chứng nhận này lại lần thứ hai.
- Tính không thể phủ nhận (non-repudiation): người ký không thể phủ nhận chữ ký của mình khi đã ký vào tài liệu.

3.2.3.2. Lược đồ chung của chữ ký điện tử

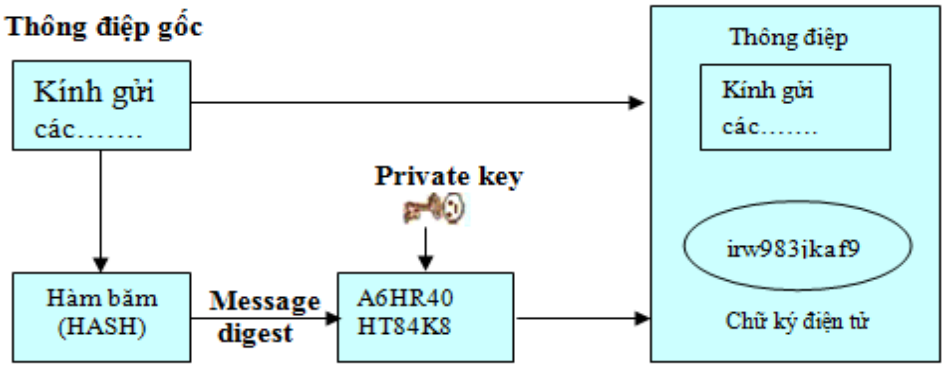
Một lược đồ chữ ký điện tử bao gồm 2 thành phần: thuật toán ký, và thuật toán xác nhận chữ ký. Nghĩa là, nếu người A muốn gửi cho người B một thông điệp x, thì A dùng một thuật toán và khoá bí mật của mình để tạo chữ ký $y = sign_{kdA}(x)$, rồi gửi cả thông điệp x lẫn chữ ký y cho B. Sau khi nhận được thông điệp x và chữ ký y. B sẽ dùng thuật toán cùng với khóa công khai của A để xác nhận chữ ký y có phải là chữ ký của A cho thông điệp x này hay không $verify_{keA}(x, y) = \{true, false\}$.



Hình 2.6: Mô hình tổng quát của chữ ký điện tử

◆ Các bước thực hiện tạo chữ ký điện tử:

- Người gửi sử dụng một hàm băm, để biến đổi thông điệp x thành một thông điệp thu gọn (message digest) **h** có chiều dài cố định: **h** = Hash(x).
- Người gửi dùng khoá riêng k_d của mình mã hóa chuỗi **h**: $y = E_{kd}(h)$, kết quả y thu được chính là chữ ký điện tử (digital signature) đối với thông điệp x.
- Cuối cùng chữ ký **y** có thể được nối vào cuối thông điệp **x** hoặc lưu vào một file gửi kèm với thông điệp. Sau khi đã ký nhận mọi sự thay đổi của thông điệp sẽ được phát hiện trong quá trình kiểm tra xác nhận chữ ký. Điều này đảm bảo cho người nhận tin rằng thông điệp họ nhận được đích thực là của người gửi và nội dung thông điệp hoàn toàn không bị thay đổi.



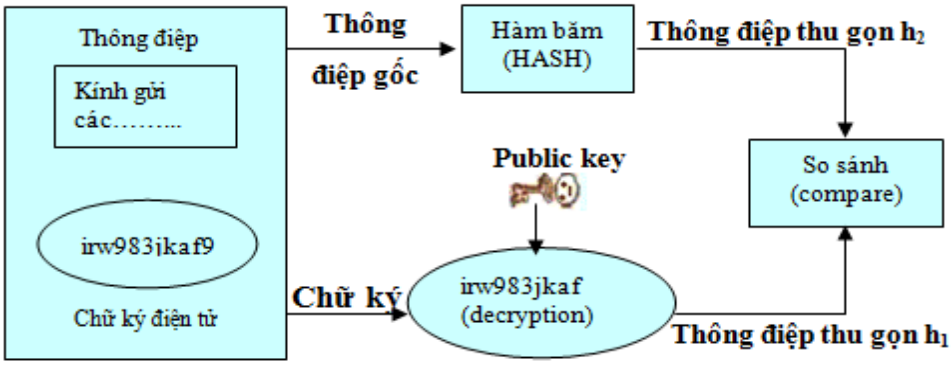
Hình 2.7: Sơ đồ minh họa các bước tạo chữ ký điện tử

◆ Các bước thực hiện kiểm tra tính đúng của chữ ký điện tử:

– Người nhận dùng khoá công khai (key public) k_e của người gửi để giải mã chữ ký điện tử y vừa nhận, khôi phục lại thông điệp thu gọn: $\mathbf{h_1} = D_{ke}(y)$.

– Người nhận sử dụng hàm băm giống như người gửi để biến đổi thông điệp x nhận được thành thông điệp thu gọn: $\mathbf{h_2}$ = Hash(x).

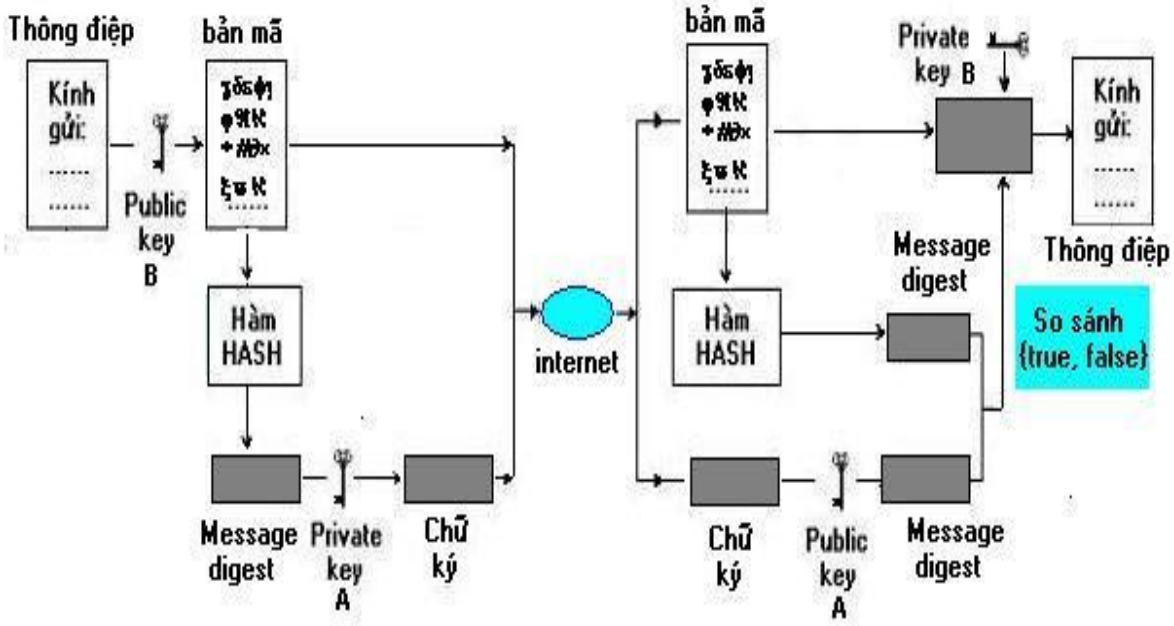
– So sánh kết quả, nếu $h_1 = h_2$ thì chấp nhận chữ ký là của người gửi. Ngược lại, chữ ký trên thông điệp không được chấp nhận.



Hình 2.8: Sơ đồ minh họa các bước kiểm tra chữ ký điện tử

Nhận xét: Lược đồ chữ ký điện tử theo kiểu này, cho phép xác định được chủ nhân đích thực của thông điệp, đồng thời đảm bảo nội dung của thông điệp không bị sửa đổi hay làm giả mạo bởi người khác trong quá trình truyền đi trên mạng. Nhưng nội dung của thông điệp có thể đọc được, do trong lược đồ này chỉ thực hiện mã hóa một khối dữ liệu nhỏ đặt trưng cho thông điệp mà không mã hoá toàn bộ thông điệp, điều này không phù hợp với nhu cầu trao đổi các thông tin bí

mật thông qua internet. Vì vậy để có thể đảm bảo được bí mật của nội dung, người gửi cần thực hiện quá trình mã hóa thông điệp bằng khóa công khai của người nhận, trước khi thực hiện ký xác nhận vào tài liệu, và người nhận phải thực hiện thêm một bước giải mã thông điệp bằng khoá riêng của mình sau khi kiểm tra đúng chữ ký của người gửi.



Hình 2.9: Mô hình chữ ký điện tử dùng quá trình mã hóa và giải mã

◆ Các bước thực hiện mã hoá và tạo chữ ký cho thông điệp

• Người gửi A mã hóa thông điệp x bằng khóa công khai của người nhận B: $C = E_{keB}(x)$. (k_{eB} là khoá công khai của người nhận B)

• Người gửi A thực hiện bước tạo chữ ký để xác nhận bản mã C với khóa riêng của mình: $y = Sig_{kdA}(C)$.

• Gửi chữ ký **y** và bản mã C đến người nhận B.

◆ Mô tả các bước kiểm tra chữ ký và giải mã thông điệp

• Người nhận kiểm tra chữ ký trên thông điệp bằng khóa công khai của người gửi A: $ver_{keA}(C, y) = \{true, false\}$.

• Nếu bước kiểm tra ở trên là đúng (true), thì người nhận tiếp tục thực hiện quá trình giải mã C với khóa riêng của mình: $x = D_{kdB}(C)$, để khôi phục lại thông điệp x. Ngược lại chữ ký của A đối với tài liệu x là không hợp lệ.

3.2.3.3. Ứng dụng chữ ký điện tử

Một e-mail có thể được ký bằng chữ ký điện tử và đảm bảo người nhận có thể chắc chắn rằng email đó đúng là của người gửi, chứ không phải e-mail giả mạo. Để đảm bảo được yếu tố này, người gửi và người nhận đều phải sử dụng cùng một hệ thống chứng thư số.

Vậy vai trò trong **chữ ký điện tử** của chứng thư số là gì? Dịch vụ chứng thư số thường được sử dụng nhiều trong các hoạt động giao dịch thương mại điện tử, đặc biệt trong thanh toán trực tuyến của ngân hàng.

Người dùng, ngoài cách bảo mật thông thường bằng mật khẩu, cũng cần dùng một chứng thư số cá nhân để xác định danh tính của mình, xác nhận các hoạt động giao dịch của mình tại ngân hàng. Chứng thực số sẽ giúp ngân hàng đảm bảo các khách hàng không thể chối bỏ các giao dịch của mình.

Các hoạt động liên ngân hàng như thanh toán, chuyển khoản…trong giao dịch điện tử cũng đều phải sử dụng chứng thực số để xác định rõ danh tính của các bên tham gia, trách nhiệm của các bên trong từng loại giao dịch. Đây là quy trình bảo mật quan trọng, là cơ sở pháp lý để căn cứ khi thực hiện các hoạt động giao dịch trực tuyến.

Không chỉ nằm trong lĩnh vực thương mại điện tử, chứng thư số hiện còn được sử dụng như một dạng của chứng minh thư nhân dân. Tại các nước phát triển, chứng thư số (CA) được tích hợp vào các con chíp nhớ nằm trong thẻ tín dụng để tăng khả năng bảo mật, chống giả mạo, cho phép chủ thẻ xác minh danh tính của mình trên các hệ thống khác nhau như xe bus, thẻ rút tiền ATM, hộ chiếu điện tử tại các cửa khẩu, kiểm soát hải quan …

Chữ ký điện tử dường như đã là một phần không thể thiếu của các doanh nghiệp hiện đại, muốn phát triển nhanh và xa hơn

3.2.3.4. Lược đồ chữ ký điện tử RSA

Hệ mật mã khóa công khai RSA cũng có thể được sử dụng để cung cấp một hệ thống chữ ký điện tử bằng cách đảo ngược vai trò của quá trình mã hóa và giải mã. Muốn thực hiện lược đồ chữ ký điện tử RSA, mỗi người sử dụng phải tạo một

cặp khóa, bao gồm khóa công khai và khóa riêng giống như trong lược đồ mã hóa và giải mã RSA, đồng thời thống nhất sử dụng cùng một hàm băm H(x). Giả sử để tạo chữ ký cho thông điệp (tài liệu) **m** người sử dụng A thực hiện như sau :

- Tính thông điệp thu gọn M = H(**m**) (M là duy nhất đối với thông điệp **m**).
- Tính S = $Sign_{Kd}$ (M) = M^d mod N (với d là khóa bí mật của người ký A).
- Kết quả S thu được chính là chữ ký của A đối với thông điệp **m**.

Khi kiểm tra chữ ký của tài liệu nhận được người sử dụng B thực hiện như sau:

- Lấy khóa công khai đích thực của người ký A (N, e) (ở tại thư mục chung).
- Kiểm tra chữ ký S ≤ N; nếu không thì từ chối chữ ký.
- Tính M' = S^e mod N.
- Tính M = H(m).
- Chấp nhận chữ ký là đúng của người gửi, nếu và chỉ nếu M □ M'.

Nếu quá trình kiểm tra chữ ký đúng (Ver_K(**m**, S) = true) thì người nhận B chắc chắn rằng thông điệp **m** đích thực là của người A gửi và nội dung thông điệp không bị thay đổi hay bị làm giả mạo bởi người khác khi truyền đi trên mạng.

3.2.3.5. Tóm tắt và kết luận ứng dụng

Lược đồ chữ ký RSA là lược đồ được dùng phổ biến nhất trong các ứng dụng bảo mật do có độ an toàn và hiệu quả thực hiện tốt nhất hiện nay. Các thuật toán cũng đơn giản, và dễ hiện thực.

Lược đồ chữ ký điện tử RSA được chọn để tích hợp vào hệ thống bảo vệ an toàn thư điện tử của đề tài. Kèm theo với lược đồ chữ ký RSA là thuật băm MD5 cũng được chọn để phù hợp cho yêu cầu tạo thông điệp thu gọn (message digest) dài 128-bits từ thông điệp đầu vào có chiều dài bất kỳ, phục vụ cho hệ thống chữ ký.

3.3. Mô tả hệ thống

Người bán cung cấp sản phẩm tới khách hàng thông qua một máy chủ bán hàng. Khách hàng lựa chọn sản phẩm cần mua, lựa chọn hình thức thanh toán thông qua trình duyệt Web phía người mua. Quá trình thanh toán sẽ do một máy chủ thanh toán thực hiện. Cả người bán và người mua đều phải đăng ký tài khóa n với máy chủ thanh toán. Khi khách hàng chấp nhận mua sản phẩm, một yêu cầu thanh toán

sẽ được chuyển tới máy chủ thanh toán. Nếu thanh toán thành công, máy chủ thanh toán gửi một chứng chỉ xác nhận tới khách hàng. Khách hàng gửi xác nhận tới máy chủ bán hàng của người bán, khi đó khách hàng nhận sản phẩm đã mua. Quá trình truyền thông giữa các bên tham gia được bảo đảm bằng cách sử dụng chữ ký số trên các thông điệp truyền đi. Cụ thể, lược đồ chữ ký số được sử dụng trong hệ thống như sau:

- User sau khi đăng ký tài khoản thành công, sẽ được cặp khóa công khai **(e_1, N_1)** và khóa bí mật **(d_1, N_1)** đã được mã hóa và lưu trong cơ sở dữ liệu của mỗi người dùng.

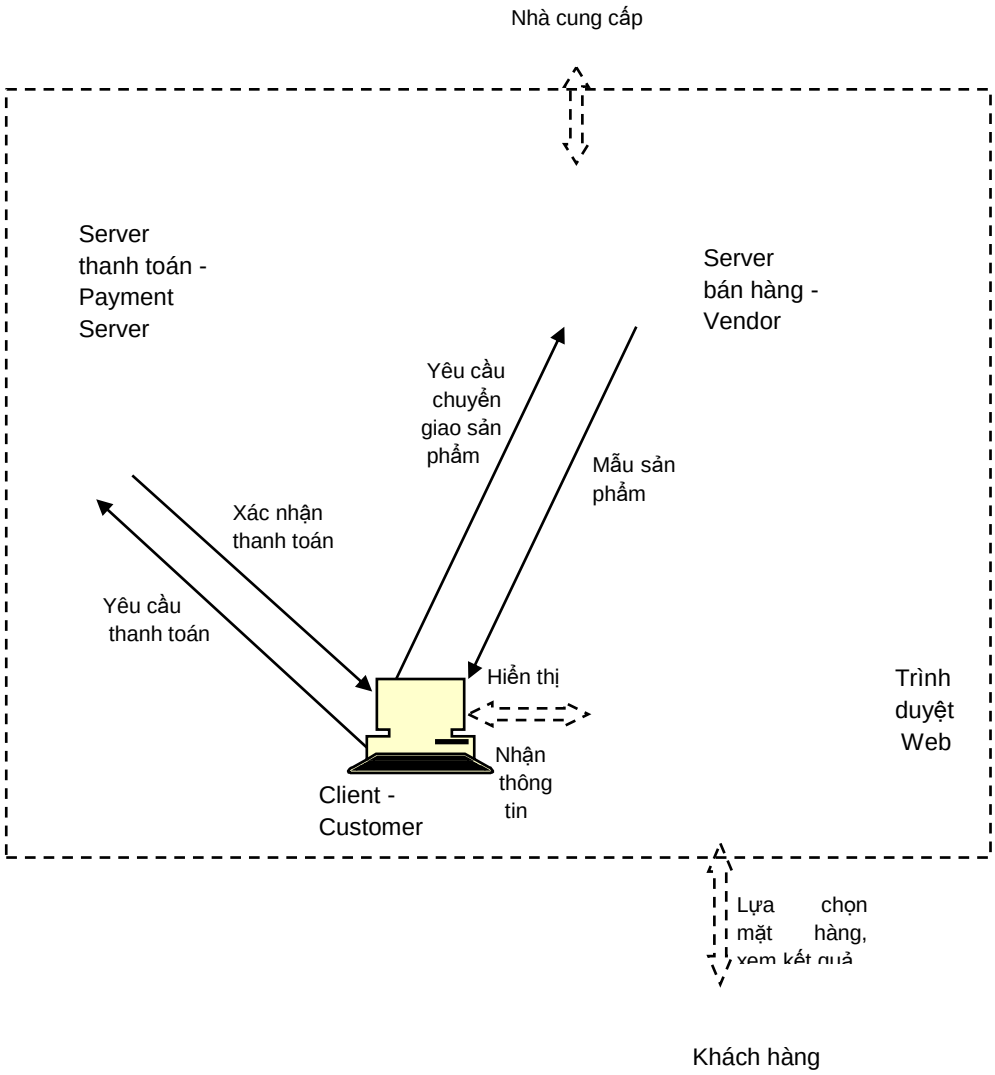
- Server sử dụng hàm băm **SHA-1** để băm thông điệp **X**. **X** ở đây là thông tin đặt hàng của **User** bao gồm: thông tin cá nhân, thông tin sản phẩm đã đặt.

Khi hoàn tất các thao tác thêm sản phẩm vào giỏ hàng, điền các thông tin đặt hàng. Hệ thống sẽ tự động thực hiện các công việc sau:

1. Thu gọn thông điệp **X** bởi hàm băm: **Y = H(X)**
2. **User** giải mã khóa bí mật và dùng nó để ký lên thông điệp đã băm Y (thông điệp rút gọn) để tạo ra chữ ký số trên **Y** bằng cách tính **S = modN1**
3. **User** gửi cặp **(X, S)** là chữ ký **S** cho **Server**. Sau khi nhận được cặp **(X, S)**, **Server** tiến hàng kiểm tra chữ ký như sau:
   - Dùng hàm băm **H** để rút gọn thông điệp **X** thành **Y = H(X)**
   - **Server** sử dụng cặp khóa công khai **(e_1, N_1)** của User để tính $\mathbf{Y^1 = modN_1}$. Nếu $\mathbf{Y^1 = Y}$ thì **Server** chấp nhập chữ ký **S** trên thông điệp **X** của **User** là đúng. Ngược lại $\mathbf{Y^1 \neq Y}$ thì **Server** không thừa nhận **S** là chữ ký của **User** trên thông điệp **X** vì cho đây là chữ ký giả mạo hoặc thông điệp đã bị thay đổi.

3.3. Phân tích hệ thống

3.3.1. Mô hình hệ thống



Hình 4.1: Mô hình hệ thống

Mô hình hệ thống được thể hiện trong hình 6.1. Mô hình gồm 3 node tham gia là Client, Server bán hàng và Server thanh toán.. Trước khi tham gia mua bán, cả nhà cung cấp và khách hàng đều phải đăng ký tài khóa n và dịch vụ thanh toán với Server thanh toán.

+ Server bán hàng – VendorServer: Cung cấp dịch vụ mua bán hàng qua mạng. Nhà cung cấp sẽ thông qua Server máy chủ bán hàng để phân phối mẫu sản phẩm đến người mua, nhận về yêu cầu mua của khách hàng và chuyển sản phẩm đã được thanh toán tới người mua.

+ Server thanh toán – Payment Server: Cung cấp dịch vụ thanh toán. Việc thanh toán giữa người bán và người mua sẽ do server thanh toán đảm nhiệm. Việc chuyển tác vụ thanh toán cho máy chủ thanh toán thực hiện sẽ giảm được gánh nặng cho máy chủ bán hàng và tăng mức độ an toàn cho hệ thống. Khi xảy ra tranh cãi giữa người bán và người mua thì máy chủ bán hàng sẽ đóng vai trò bên thứ ba tin cậy để giải quyết. Sau khi thực hiện thanh toán, máy chủ thanh toán gửi một xác nhận làm bằng chứng thanh toán cho người mua.

+ Client – Customer: Khách hàng tương tác với hệ thống thông qua một giao diện (trình duyệt Web) được cung cấp bởi node Client. Client nhận yêu cầu mua hàng từ phía khách hàng, gửi yêu cầu thanh toán tới máy chủ thanh toán, nhận về xác nhận thanh toán từ máy chủ thanh toán, sau đó gửi yêu cầu chuyển hàng cùng xác nhận thanh toán tới máy chủ thanh toán và nhận về sản phẩm từ máy chủ thanh toán.

3.3.2. Các chức năng chính của hệ thống

❖ *Đăng ký thành viên*

Chức năng này cho phép một khách hàng mới đăng ký là thành viên sử dụng hệ thống.

❖ *Đăng nhập hệ thống*.

Khách hàng đăng nhập hệ thống sử dụng *username / password* đã đăng ký với hệ thống. Sau khi đăng nhập khách hàng có thể thực hiện đăng ký tài khóa n với Server thanh toán và thực hiện mua hàng.

❖ *Đăng ký tài khóa n.*

Chức năng này được thực hiện đồng thời khi người dùng đăng ký thành viên. Cho phép khách hàng và nhà cung cấp đăng ký một tài khóa n với một nhà cung cấp dịch vụ thanh toán – máy chủ thanh toán, tài khóa n này được dùng để thanh toán

giữa hai bên mua và bán. Sau khi yêu cầu đăng ký tài khóa n được thực hiện, máy chủ thanh toán sẽ gửi lại ID và số tiền hiện có trong tài khóa n của bên đăng ký và khóa công khai của Payment Server dùng cho việc trao đổi thông tin sau này.

❖ *Thanh toán.*

Chức năng này do Payment Server thực hiện khi có một khách hàng (Customer) chấp nhận mua hàng, và một yêu cầu thanh toán được gửi từ khách hàng tới Server thanh toán. Trong yêu cầu thanh toán chứa số ID của người mua, ID của người bán và tổng số tiền cần thanh toán. Payment Server sẽ chuyển số tiền cần thanh toán từ tài khóa n của khách hàng sang tài khóa n của nhà cung cấp. Sau đó, Payment Server gửi một chứng thực xác nhận đã thanh toán cho khách hàng (Customer). Chứng thực này sẽ được khách hàng gửi tới nhà cung cấp làm bằng chứng cho việc thanh toán để nhận sản phẩm.

❖ *Nhận sản phẩm.*

Chức năng này được khách hàng dùng để nhận sản phẩm đã được thanh toán. Sau khi kiểm tra chứng thực thanh toán, nhà cung cấp sẽ gửi một thông báo tới khách hàng. Mặt hàng được chuyển giao tới cho khách hàng.

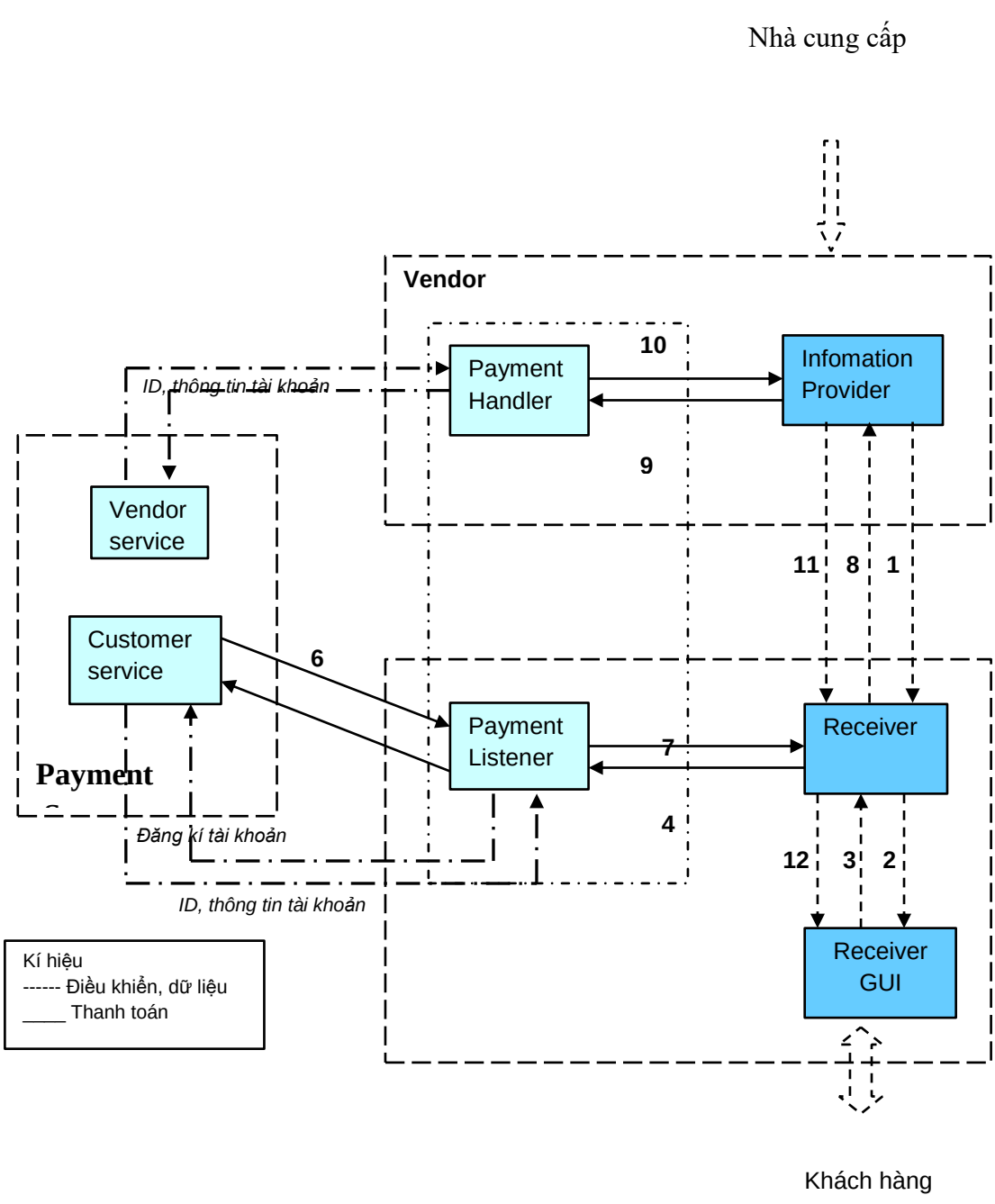
Các thông điệp trao đổi giữa các thành phần tham gia các chức năng trên đều được ký số bằng khóa bí mật của bên gửi và bên nhận kiểm tra bằng khóa công khai tương ứng của bên gửi sử dụng thuật toán DSA.

3.3.3. Kiến trúc module của hệ thống

Mỗi module của hệ thống sẽ thực hiện chức năng của một node trong mô hình hệ thống trong hình 5.1

Toàn bộ hệ thống có thể được chia làm ba module chính sau:

- VendorServer – Module này gồm hai thành phần là Payment Handler và Information Provider
- Customer – Module này gồm ba thành phần là Payment Listenner, Receiver và Receiver GUI.
- Payment Server – Module này gồm hai thành phần là Vendor Service và Customer Servive



Hình 4.2: Kiến trúc Module tổng thể của hệ

Quá trình tương tác giữa các module để thực hiện một giao dịch thanh toán trong mô hình như sau:

2. Information Provider gửi hàng mẫu (ví dụ thumbnail của một ảnh, thông tin của sách...) tới Receiver.

3. Người dùng chọn mặt hàng muốn mua thông qua một GUI.

4. Khi người dùng chấp nhận mua hàng, yêu cầu mua hàng được gửi tới Receiver.

5. Receiver tạo thông tin thanh toán chuyển tới Payment Listenner.

6. Payment Listenner liên lạc với Payment Server, gửi yêu cầu thanh toán tới Payment Server.

7. Payment Server gửi lại cho Payment Listenner một chứng thực đã thanh toán và thông tin về tài khóa n sau khi thanh toán của khách hàng.

8. Payment Listenner gửi xác nhận lại cho Receiver.

9. Receiver gửi yêu cầu chuyển hàng và chứng thực thanh toán cho Information Provider.

10. Information Provider gửi chứng thực cho Payment Handler.

11. Payment Handler kiểm tra chứng thực thanh toán, nếu là đúng thì gửi thông báo cho Information Provider yêu cầu chuyển giao sản phẩm cho Receiver.

12. Information Provider chuyển mặt hàng tới Receiver

13. Thông qua GUI khách hàng nhận sản phẩm (thực hiện download file hoặc xem).

3.3.4. Các module của hệ thống

- **Module Customer**

Đây là module do khách hàng dùng để nhận thông tin, như mẫu sản phẩm, sản phẩm chuyển giao từ phía nhà cung cấp. Customer có hai chức năng:

- ✔ Đăng ký người dùng với hệ thống
- ✔ Đăng nhập hệ thống.
- ✔ Thực hiện mua hàng.

Để đăng ký người dùng với hệ thống, Customer cần phải gửi một số thông tin trong đó có:

- Username: Định danh cho người sử dụng
- Password: Mật khẩu.

Hai thông tin này được người dùng đưa vào khi đăng nhập hệ thống. Customer sẽ đóng gói yêu cầu đăng nhập để gửi lên Vendor.

Để thực hiện mua hàng, Customer phải gửi yêu cầu thanh toán tới Payment Server. Yêu cầu thanh toán bao gồm các thông tin sau:

- CustomerID: ID của khách hàng
- VendorID: ID của nhà cung cấp
- Value: Tổng số tiền thanh toán

Module này gồm các thành phần sau:

Payment Listenner – Thành phần này cung cấp dịch vụ thanh toán cho phía người mua và hỗ trợ các hoạt động sau:

- Đăng ký tài khóa n và dịch vụ thanh toán với một Payment Server.
- Tạo và chuyển yêu cầu thanh toán tới Payment Server.
- Nhận chứng thực thanh toán từ Payment Server và chuyển tới cho Vendor.

Receiver – Thành phần này thực hiện chức năng truyền thông với Vendor và hỗ trợ các hoạt động sau:

- Tạo thông tin đăng ký từ người dùng và gửi yêu cầu đăng ký tới Vendor.
- Tạo thông tin đăng nhập và gửi yêu cầu đăng nhập tới Vendor
- Nhận thông tin mẫu sản phẩm từ phía Vendor
- Gửi yêu cầu chuyển hàng và chứng thực thanh toán tới Vendor
- Nhận mặt hàng đã thanh toán do Vendor chuyển tới.

Receiver GUI – Thành phần này thực hiện chức năng giao tiếp với khách hàng, hỗ trợ các hoạt động sau:

- Hiển thị thông tin về sản phẩm cho người dùng
- Nhận yêu cầu người dùng.
- Hiển thị các thông báo.

- **Module VendorServer**

Đây là module được dùng bởi nhà cung cấp thông tin hay người bán để phân phối sản phẩm. Vendor có các chức năng:

✔ Xử lý các yêu cầu gửi lên từ Customer

✔ Quản lý các Customer.

✔ Thực hiện bán hàng.

Các yêu cầu gửi lên từ Customer được đóng gói thành các thông điệp – message. Các yêu cầu bao gồm:

- Thông điệp yêu cầu đăng ký

- Thông điệp yêu cầu đăng nhập

- Thông điệp yêu cầu chuyển giao sản phẩm.

Đối với một Vendor, có rất nhiều Customer do đó, Vendor quản lý các Customer theo từng tiến trình tương ứng. Để quản lý các Customer, Vendor sẽ ghi lại thời điểm đăng nhập và thoát khỏi hệ thống của mỗi Customer. Khi có một Customer đăng nhập hệ thống, Vendor sẽ lấy và chuyển cho Customer này thời gian đăng nhập hệ thống lần cuối cùng tương ứng với username.

Để thực hiện bán hàng, Vendor kiểm tra tính hợp lệ của chứng thực bằng cách kiểm tra chữ ký của Payment Server dùng khóa công khai của Payment Server.

Module này gồm các thành phần sau:

Payment Handler – Thành phần này cung cấp dịch vụ thanh toán cho phía nhà cung cấp và hỗ trợ các hoạt động sau:

- Đăng ký tài khóa n và dịch vụ thanh toán với một Payment Server.

- kiểm tra chứng thực do Payment Server tạo ra và Receiver gửi đến làm bằng chứng cho việc thanh toán.

Information Provider – Thành phần này thực hiện chức năng truyền thông với Receiver và hỗ trợ các hoạt động sau:

- Xử lí yêu cầu đăng ký: kiểm tra trong CSDL đã có username như người dùng đăng ký chưa.

- Xử lí thông tin đăng nhập: kiểm tra Username và Password nhập vào.

- Chuyển mẫu sản phẩm tới Receiver.
- Nhận yêu cầu mặt hàng từ phía Receiver.
- Chuyển mặt hàng đã được thanh toán tới Receiver.

● **Module Payment Server**

Đây là module thực hiện chức năng thanh toán. Module này gồm hai thành phần sau:

Vendor Service: Thành phần này thực hiện các dịch vụ thanh toán phía người bán, hỗ trợ các hoạt động sau:

- Đăng ký tài khóa n cho người bán.
- Trao đổi khóa công khai giữa người bán và Payment Server nhằm kiểm tra tính toàn vẹn của chứng thực thanh toán do khách hàng gửi đến.

Customer Service: Thành phần này thực hiện các dịch vụ thanh toán phía người mua, hỗ trợ các hoạt động sau:

- Đăng ký tài khóa n tài khóa n cho người mua.
- Thực hiện thanh toán theo yêu cầu của khách hàng.
- Gửi chứng thực thanh toán cho khách hàng.

3.3.5. Các thông điệp được ký số

Thông tin trao đổi giữa các module được đóng gói dưới dạng các thông điệp. Tính bảo mật của các thông điệp được bảo đảm bằng cách gửi thông điệp đó kèm theo chữ ký của nó. Chữ ký này được tính bằng cách sử dụng hàm băm bảo mật SHA để thu được bản tin thu gọn (Message Digest) và thuật toán mã chữ ký điện tử DSA để mã hóa Message Digest này thu được chữ ký.

Đơn vị dữ liệu truyền đi có dạng sau:

Protocol Data Unit PDU = message + DSA [SHA(message)]

Bên nhận có thể xác minh chữ ký sử dụng khóa công khai của bên gửi.

Trong hệ thống thanh toán được xây dựng, ta chỉ thực hiện ký số lên các thông điệp quan trọng bao gồm:

✔ Thông điệp yêu cầu thanh toán từ Customer đến Payment Server

- ✔ Thông điệp trả lời chứa chứng thực thanh toán từ Payment Server đến Customer
- ✔ Thông điệp yêu cầu chuyển giao sản phẩm chứa chứng thực thanh toán từ Customer đến Vendor.

Để mô hình hóa các thông điệp, ta sử dụng các ký hiệu sau:

Mục dữ liệu – Data Item

Giá tri băm – Hash Value

Chữ kí

Phép toán mã hóa

Các chữ viết tắt sau được sử dụng:

Ký hiệu viết tắt	Mô tả
S_V	Chữ ký của người bán hay Vendor
S_{CP}	Chữ ký của Customer dùng trong trao đổi với Payment Server
S_{CV}	Chữ ký của Customer dùng trong trao đổi với Vendor
S_P	Chữ ký của Payment Server
V_{ID}	ID duy nhất của Vendor
C_{ID}	ID duy nhất của Customer
PK_C	khóa công khai của Customer
SK_C	khóa bí mật của Customer
PK_V	khóa công khai của Vendor
SK_V	khóa bí mật của Vendor
PK_P	khóa công khai của Payment Server
SK_P	khóa bí mật của Payment Server
Oid	ID duy nhất của một mẫu chào hàng – Offer
	ID duy nhất của một chứng thực thanh toán (Receipt)

rid	do Payment Server tạo ra cho phép xác định một giao dịch thanh toán
value	Tổng số tiền phải chuyển từ tài khóa n của Customer sang tài khóa n của Vendor
t_xc t_xp	Nhãn thời gian do Customer tạo để nhận biết khóa được dùng để ký tại một thời điểm cụ thể Nhãn thời gian tạo bởi Payment Server
$props_{vc}$	Thông tin tùy chọn trao đổi giữa Vendor và Customer như thông tin mô tả sản phẩm, thông tin giao hàng...

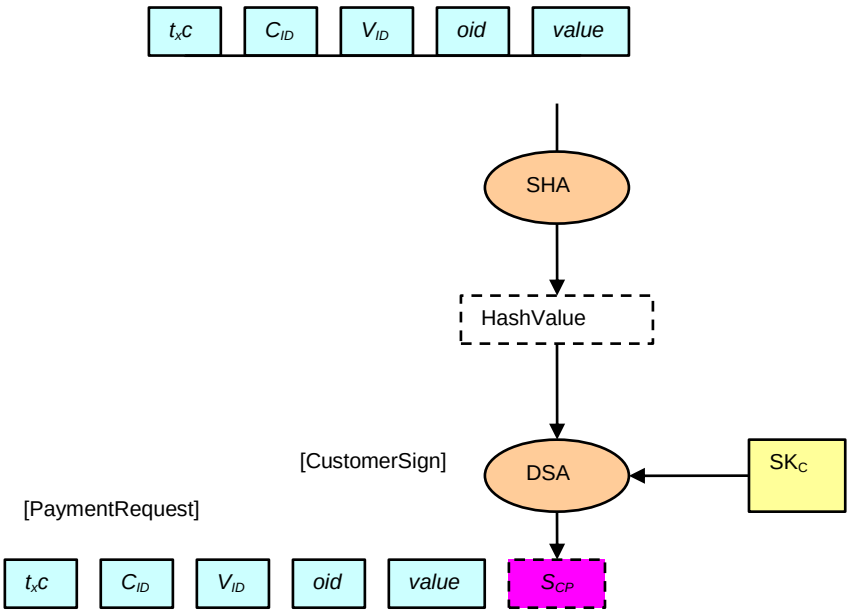
Ta chỉ xem xét việc trao đổi thông điệp để thực hiện một quá trình thanh toán. Do đó ta giả thiết các bước sau đã được thực hiện:

1. Khách hàng đã đăng ký với hệ thống, đã trao đổi khóa công khai với Vendor và Payment Server. Customer có C_{ID} hợp lệ và biết được V_{ID}**.**
2. Tài khóa n của Customer đủ để thực hiện thanh toán.
3. Customer nhận được một mẫu chào hàng từ Vendor chứa *oid* và *value*, đã lựa chọn mua sản phẩm.
4. Vendor đã đăng ký dịch vụ thanh toán với Payment Server và trao đổi khóa công khai với nhau.

- **Yêu cầu thanh toán** [Customer]:Để thực hiện thanh toán cho một sản phẩm đã chọn, Customer tạo thông điệp yêu cầu thanh toán, ký số lên thông điệp và gửi cho Payment Server:

  $PaymentRequest = [(t_xc + C_{ID} + V_{ID} + oid + value) + S_C)]$

  $S_{CV} = DSA\ [\ SHA\ (t_xc + C_{ID} + V_{ID} + oid + value)]$

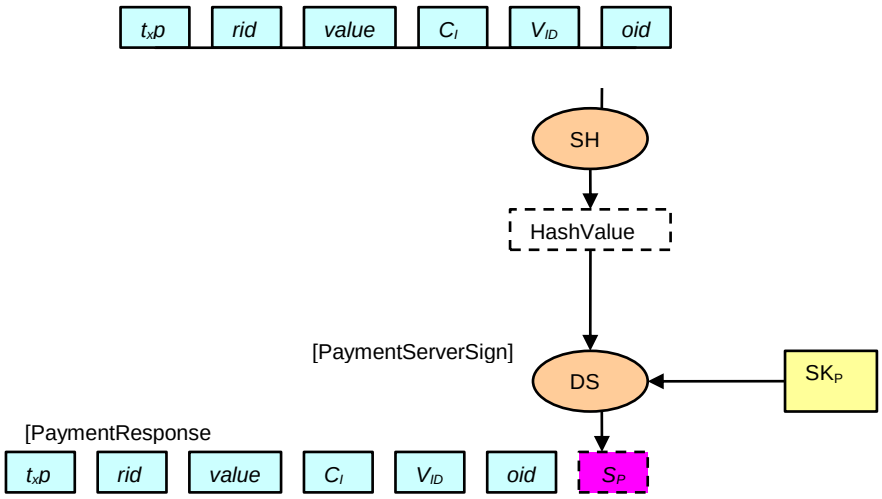


Hình 4.3:Thông điệp yêu cầu thanh toán [Customer Payment Server]

- **Xác nhận thanh toán** [Payment Server]**:** Sau khi thực hiện một thanh toán, Payment Server trả lại cho Customer một xác nhận thanh toán chứa chữ ký của Payment Server:

$PaymentResponse = [(t_xp + rid + value + C_{ID} + V_{ID} + oid) + S_P]$

$S_P = DSA [SHA (t_xp + rid + value + C_{ID} + V_{ID} + oid)]$

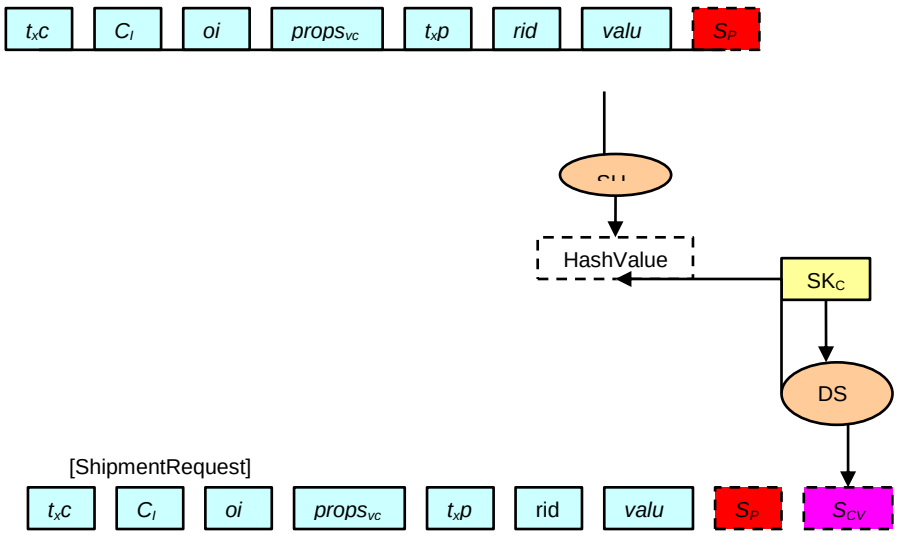


Hình 4.4: Thông điệp xác nhận thanh toán [Payment Server Customer]

- **Yêu cầu chuyển hàng** [Customer]: Customer nhận được PaymentResponse từ Payment Server, thực hiện kiểm tra chữ ký S_P sử dụng khóa công khai của Payment Server. Nếu chữ ký được kiểm tra là đúng, Customer tạo một yêu cầu chuyển hàng chứa C_{ID}, t_xc, *oid* một số thông tin phụ $props_{vc}$ và thông tin từ xác nhận thanh toán (t_xp, *rid*, *value*, S_P) gửi cho Vendor.

  $ShipmentRequest = [(t_xc + C_{ID} + oid + props_{vc} + t_xp + rid + value + S_P) + S_{CV}]$

  $S_{CV} = DSA\ [\ SHA\ (t_xc + C_{ID} + oid + props_{vc} + t_xp + rid + value + S_P)]$



Hình 4.5: Thông điệp yêu cầu chuyển hàng [CustomerVendor]

3.4. Cài đặt hệ thống

3.4.1. Một số hàm phương thức được sử dụng:

- **Hàm tạo cặp khóa riêng/khóa công khai *Taokhóa ()***:

Khi người dùng đăng ký tài khoản, hệ thống sẽ tự động Random hai số **p** và **q** lớn (Trong đoạn code minh họa là **x** và **y**), để tạo không gian khóa lớn. Hai số này sẽ phải thỏa mãn điều kiện là hai số nguyên tố phân biệt (kích cỡ mỗi số khoảng 512 bits $\rightarrow$ 1024 bits).

Tiếp theo tính số hàm Modulo của hệ thống N theo hai số nguyên tố đã tìm được. Hai số nguyên tố này chính là thừa số nguyên tố của N, nghĩa là $N = p_1^{e1}$, p_2^{e2}, …p_k^{ek} , với p_i là những số nguyên tố phân biệt và $e_i \geq 1$ (với i = 1,..., k). Trong bài toán RSA, cụ thể N = p * q. Tiếp tục tính toán hàm số Euclide ϕ(N) = (p – 1) * (q – 1).

Sau khi tính được hàm số Euclide ϕ(N), chọn một số ngẫu nhiên **E** (Trong đoạn code minh họa là **e**) trong khoản từ 17 < E < ϕ(N) với điều kiện E và ϕ(N) là hai số nguyên tố cùng nhau có cùng ước chung lớn nhất bằng 1. Để đáp ứng lượng người dùng lớn, tránh trùng lặp cặp khóa công khai, kiểm tra lại cặp khóa công khai giữa các người dùng. Nếu trùng thì tiến hàng Random lại khóa.

// hàm tạo cặp khóa riêng – khóa công khai

```
public List<long> Taokhóa ()
{
ReRadom://Radom để chọn lại khóa
//Radom để chọn khóa
Random r = new Random();
long x = r.Next(1001,9997);
long y = r.Next(1001,9997);
while (CHECK_SNT(x) == false || CHECK_SNT(y) == false)
{
Random rr = new Random();
x = rr.Next(1001,9997);
```

```
    y = rr.Next(1001, 9997);
    }
    List<long> khoa = new List<long>(); // khai báo mảng chứa
khóa 1,2 PriKey 3,4 PubKey
    long N = x * y; //Tính số hàm modulo của hệ thống
    long phi = (x - 1) * (y - 1); //Tính giá trị hàm số Ơ-le
    long E = 0;
    for (long i = 17; i < phi; i++) //Tìm số nguyên tố cùng
nhau của E vs phi trong khóa ng từ 1 <= E <= phi
    {
    if (UOC_CHUNG_LON_NHAT(i, phi) == 1)
    {
    E = i;
    break;
    }
    }
    //kiểm tra có lặp khóa công khai không.
    if (!CheckKeyPublic(N, E))
    goto ReRadom;
    //long k = nd(soE, phi);
    //Tính khóa giải mã D sao cho D*E = 1(mod phi(n))
    long k = 1;
    while (((phi * k + 1) % E != 0))
    { k++; }
    long soD = (phi * k + 1) / E; //tính số D
    khoa.Add(soD);
    khoa.Add(N);
    khoa.Add(E);
    khoa.Add(N);
```

```
return khoa ;
}
```

Tiếp đến là tính khóa bí mật **d** (trong đoạn code minh hoạ là **soD**). **d** được tính là nghịch đảo của e modulo N), cụ thể: $E * d \equiv 1 \bmod \phi(N)$. Cặp số (E, N) là khóa công khai, còn (D, N) là khóa bí mật

- **Hàm tạo chữ ký *TINHA(long, long, long)***

Trong đoạn code bên dưới,

- **a** là mỗi ký tự trong chuỗi Message đã được băm bởi hàm Hash.
- **b** là Private key **d** đã được tạo sẵn trong quá trình đăng ký tài khoản và mã hóa.
- **p** là **N** đã được tạo bởi hai số nguyên tố **p** và **q**.

```
// dùng PublicKey ký lên Message dùng thuật toán DSA và SHA
public long TINHA(long a, long b, long p)
{
long ret = 1;
a %= p;
b %= p - 1;
while (b > 0) //vòng lặp phân tích b thành cơ số 2
{
if (b % 2 > 0)  //ở vị trí có số 1 thì nhân với a^(2^i) tương ứng. Tất cả các phép nhân đều có phép mod p theo sau.
ret = ret * a % p;
a = a * a % p;  //tính tiếp a^(2^(i+1)), a^1 -> a^2 -> a^4 -> a^8 -> a^16 v.v...
b /= 2;
}
return (long)ret;
}
```

- **Hàm kiểm tra chữ ký bằng khóa công khai *CheckSignal(string, string, long, long)***

- **message:** thông điệp đã được băm và mã hóa.

- **signal:** chữ ký đã được tạo từ thông điệp **message** và cặp khóa bí mật **d**

- **so_n, so_e:** Cặp khóa công khai để giải mã chữ ký số.

Thông điệp message sẽ được kiểm tra xác thực cùng chữ ký. Giải mã thông điệp đã được mã hóa trước đó ra được thông điệp đã băm descrypt_message (bản tóm lược 1). Chữ ký số signal được giải mã cùng với khóa công khai tạo ra bản tóm lược Decrypt_signal (bản tóm lược 2). So sánh từng ký tự ở cả hai bản tóm lược: nếu có bất kỳ sự thay đổi nào ở cả hai bản tóm lược thì thông điệp gửi đi không được bảo toàn.

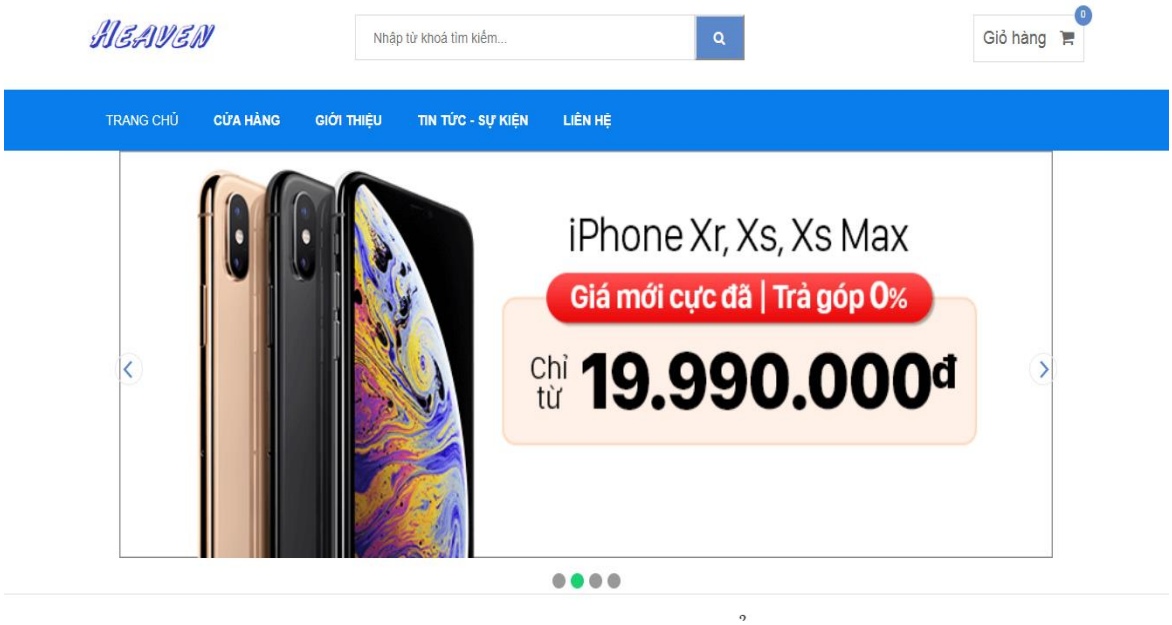
```
// kiểm tra chữ ký bằng khóa công khai
//Xác thực chữ ký
public int CheckSignal(string message, string signal, long so_n, long so_e)
{
List<long> Mang1 = new List<long>();
List<long> Mang2 = new List<long>();
//Giải mã bản tin thành hàm băm tạo ra bản tóm lược 1
string decrypt_message = sig.Decrypt_MD5(message);
//Xác thực chữ ký
string[] chuoi = signal.Split(' ');
for (int i = 0; i < chuoi.Length; i ++)
{
if(chuoi[i] == "")
continue;
Mang1.Add(long.Parse(chuoi[i]));
}
```

```
        //Xác thực chữ ký
        foreach (long i in Mang1)
        {
        long tam;
        //Giải mã chữ ký số cùng với khóa công khai và tạo ra
bản tóm lược 2
        tam = sig.TINHA(i, so_e, so_n);
        Mang2.Add(tam);
        }
        //Chuyển thành chuỗi để so sánh
        string Decrypt_signal = String.Join("", Mang2);
        int k = 0;
        if(decrypt_message.Length == Decrypt_signal.Length)
        {
        for(int i = 0; i < decrypt_message.Length; i ++)
        {
        if (Decrypt_signal[i] != decrypt_message[i])
        {
        k++;
        break;
        }
        }
        }
        else
        {
        k++;
        }
        if (k == 0)
        return 1; //Bản tin đc bảo toàn
```

```
else
return 0;//Bản tin đã bị thay đôi
}
```

3.4.2. Một số giao diện cài đặt

Hình 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 5.12 trình bày một số giao diện cài đặt của hệ thống. Với điều kiến khách hàng đã đăng ký tài khóa n và đăng nhập trong hệ thống. Các bước để khách hàng tiến hành mua sắm như sau:

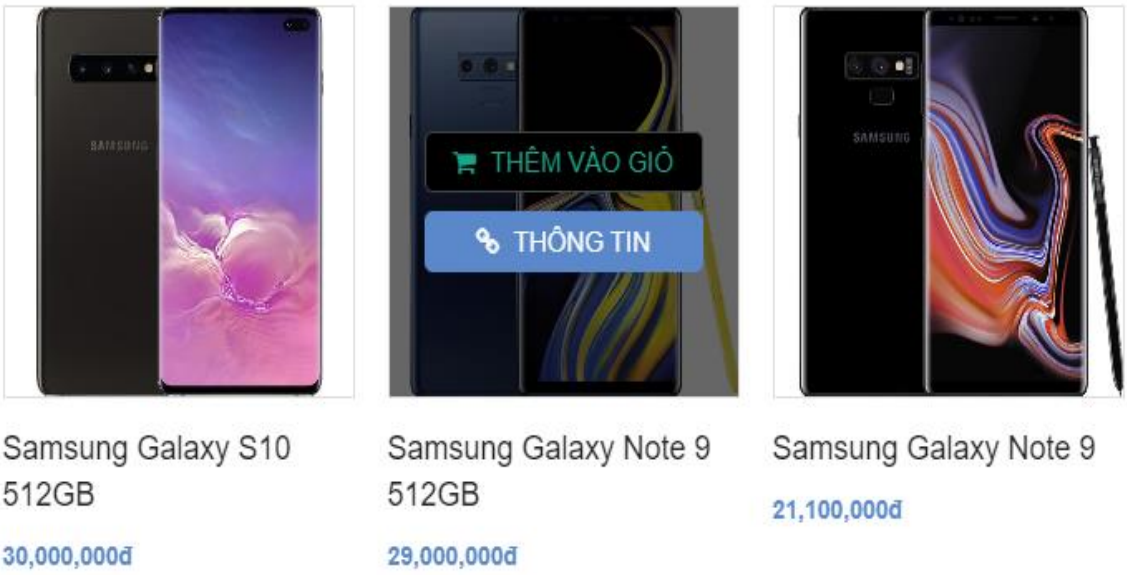


Hình 3.6: Giao diện trang WEB

Mỗi người mua hàng sẽ có sẵn 100.000.000 trong tài khoản. Ứng dụng của chữ kí điện tử sẽ được áp dụng trong chứng thực thanh toán. Mỗi khách hàng khi tạo tài khoản sẽ được cấp một khóa riêng ngẫu nhiên và khóa này sẽ được lưu trữ trong cơ sở dữ liệu và sẽ được sử dụng khi khách hàng muốn thanh toán một mặt hàng nào đó. Hóa đơn sẽ là một bản tin và chữ kí sẽ được tạo từ hóa đơn và khóa riêng tư của khách hàng. Sau đó được chuyển về server để xử lí đơn hàng. Tại server đơn hàng sẽ được xác thực chữ kí của người dùng. Nếu chính xác thì hóa đơn sẽ được chấp nhận và khi đó số dư tài khoản của người dùng mới bị trừ và thông báo đến đơn hàng đã được thanh toán thành công. Còn nếu không đơn hàng sẽ bị hủy bỏ.

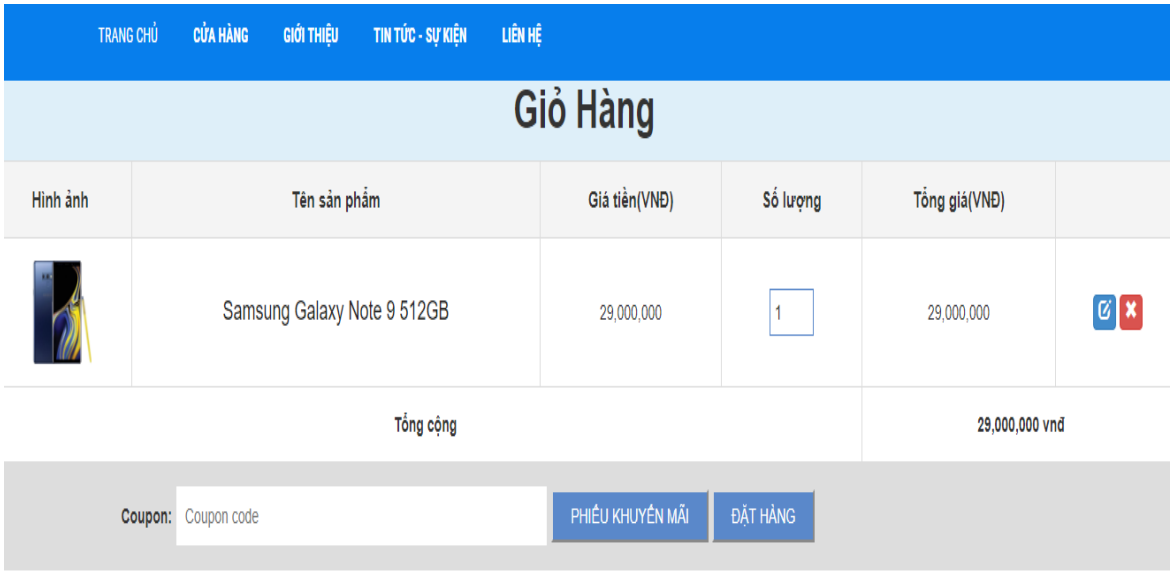
Các bước để mua hàng trên trang WEB:

Đầu tiên thêm sản phẩm bạn muốn mua vào giỏ hàng:



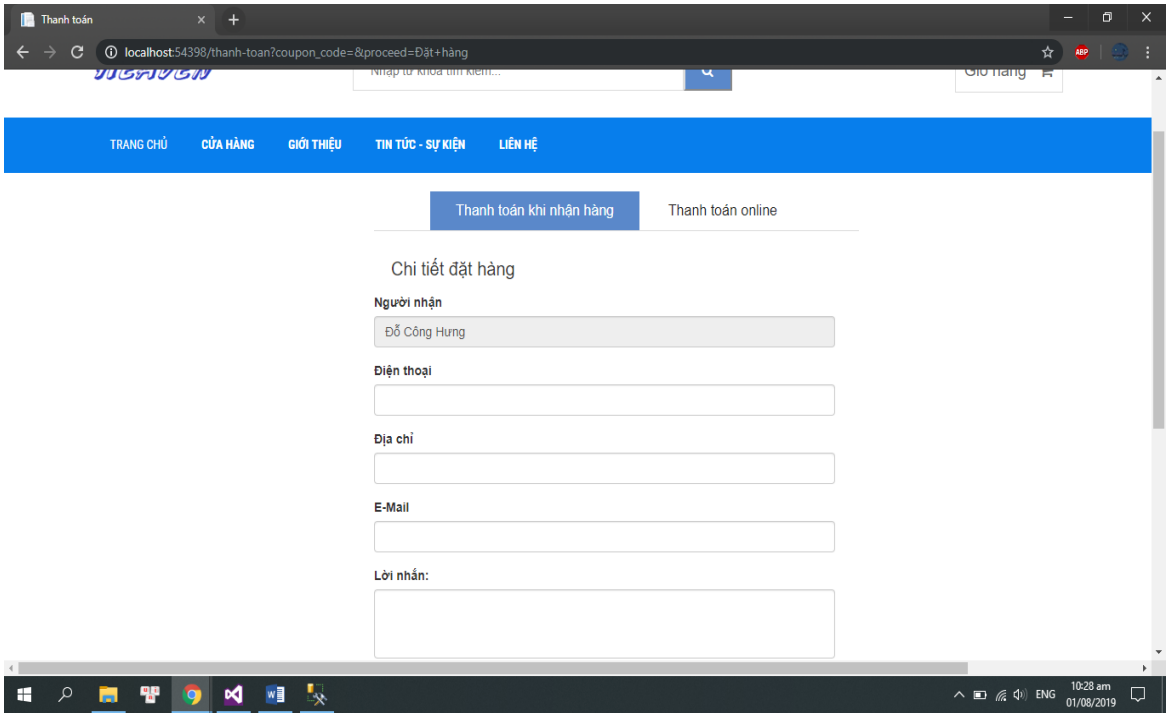
Hình 3.7: Giao diện thêm sản phẩm

Trong giỏ hàng, click vào nút đặt hàng để đi đến mục thanh toán:



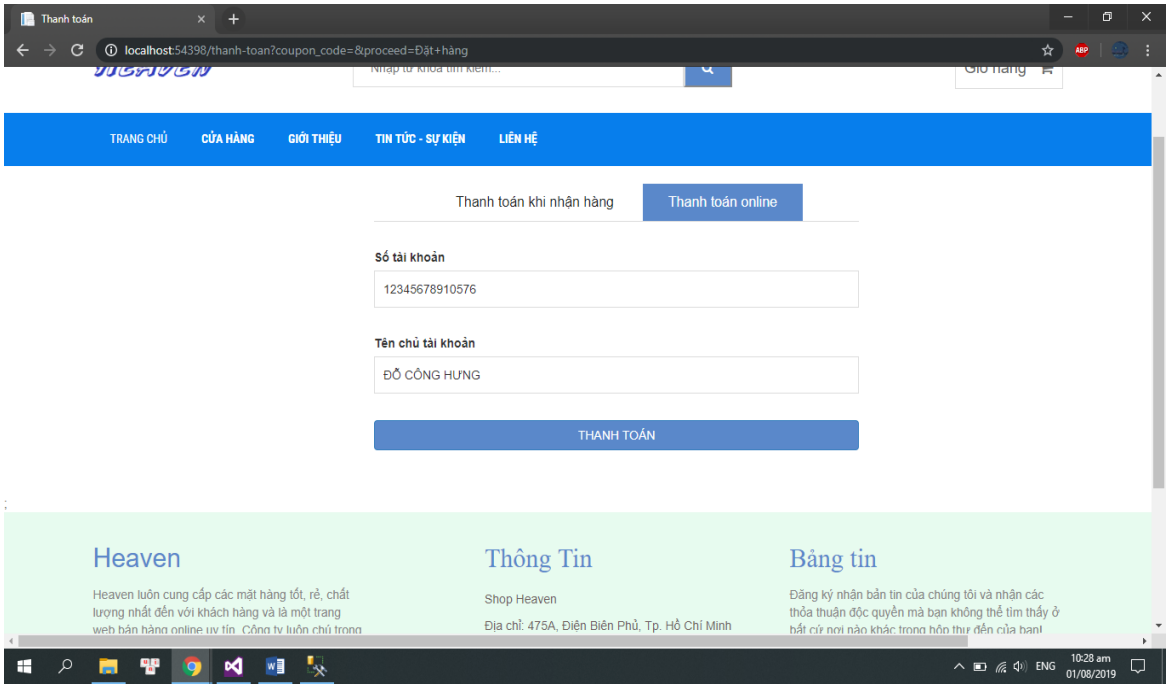
Hình 3.8: Giao diện đặt hàng

Nhấn nút đặt hàng. Hệ thống sẽ hiển thị thông báo đang xử lý giao dịch: nhận hàng rồi thanh toán hoặc thanh toán online.



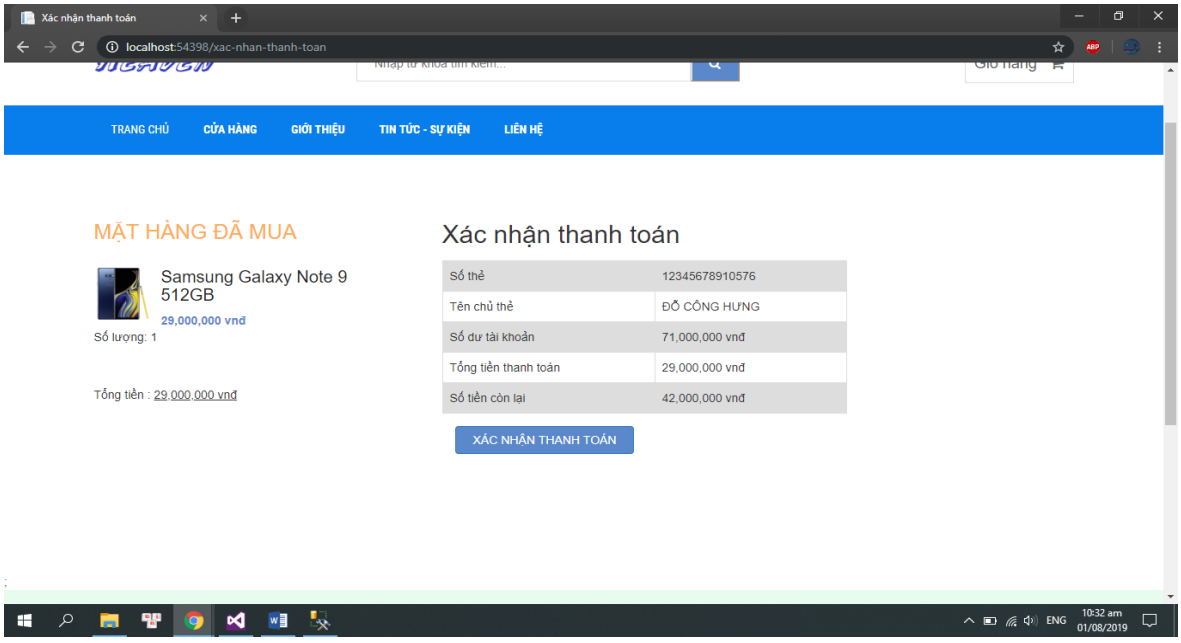
Hình 4.9: Giao diện đặt hàng

Khi thực hiện thanh toán online, thông tin chủ tài khóa n và chủ thẻ sẽ tự động được điền vào thanh input



Hình 4.10 : Giao diện thanh toán online

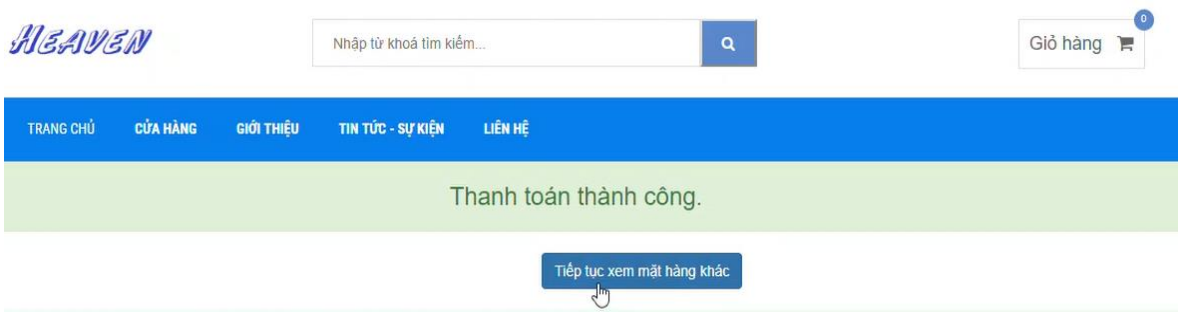
Khi nhấn nút thanh toán, hệ thống sẽ gửi xác nhận yêu cầu thanh toán cho khách hàng bao gồm: thông tin thẻ, số dư tài khóa n, tổng tiền thanh toán và số tiền còn lại trong thẻ.



Hình 3.11 : Giao diện xác nhận thanh toán

VendorServer (Server nhà cung cấp) gửi thông điệp yêu cầu thanh toán cho PaymentServer (Ngân hàng). PaymentServer sau khi kiểm tra thấy thông điệp là hợp lệ, nó sẽ trừ tiền trong tài khóa n của khách hàng và gửi thông báo xác nhận. Thông điệp này cũng được mã hóa. Sau khi kiểm tra tính hợp lệ của thông điệp nhận được, Vendor Server ghi yêu cầu mua hàng của khách hàng vào cơ sở dữ liệu của mình. Các thông điệp đều được ký bằng thuật toán RSA

Sau khi xác nhận thanh toán. VendorServer thông báo đã thực hiện giao dịch thành công.



Hình 3.12: Xác nhận thanh toán thành công

3.5 Kết luận

Hệ thống được xây dựng nhằm mục đích ứng dụng chữ ký điện tử trong quá trình truyền thông giữa các đối tác tham gia một giao dịch mua – bán qua mạng. Giao thức dùng trong chương trình đã được đơn giản hóa so với giao thức đang được dùng trong các hệ thống thương mại điện tử thực tế trên Internet. Điểm mấu chốt trong giao thức này đó là việc sử dụng một chứng thực điện tử - Receipt làm bằng chứng cho một quá trình thanh toán thành công. Đây là cơ sở để người bán chuyển giao sản phẩm cho người mua. Chương trình được xây dựng bằng ngôn ngữ C#, sử dụng kiến trúc mã hóa C# để thực hiện mã hóa và ký số lên các thông điệp.

KẾT LUẬN

Hiện nay, Đảng và Chính phủ Việt Nam rất quan tâm và đã có nhiều việc làm thiết thực nhằm thiết lập cơ sở hạ tầng cho Thương mại điện tử như chữ ký điện tử, thanh toán điện tử... Trong thời gian gần đây, nhiều hệ thống ứng dụng chữ ký điện tử đã ra đời như:(i) Sử dụng chữ ký điện tử trong thanh toán liên ngân hàng, (ii) Hệ thống khai báo hải quan điện tử, (iii) Các Website Thương mại điện tử như http://www.tienphong-vdc.com.vn, http://vdcsieuthi.vnn.vn, http://yes.com ... Tuy nhiên thực tế cho thấy các Website này còn thiếu một khâu rất quan trọng của Thương mại điện tử theo nghĩa hoàn chỉnh của nó là Thanh toán điện tử - một ứng dụng cần đến hệ thống chứng thực điện tử.

Qua một thời gian làm việc nghiêm túc và khẩn trương cùng với sự giúp đỡ tận tình của thầy giáo TS. Hồ Văn Canh. Đến nay, đồ án của tôi đã hoàn thành đúng hạn và đảm bảo được nội dung, yêu cầu đề ra theo kế hoạch. Đồ án đã giải quyết được một số vấn đề sau:

Thứ nhất: Tìm hiểu tổng quan về an toàn thông tin và thực trạng an toàn thông tin trong tình hình hiện nay

Thứ hai: Tìm hiểu các cơ sở toán học được sử dụng trong các thuật toán mã hóa, các hệ mã hóa khóa công khai và chữ ký số.

Thứ ba: Xây dựng lược đồ chữ ký số mới dựa trên bài toán mã khóa công khai RSA.

Một số vấn đề tiếp tục nghiên cứu và đề xuất:

- Mở rộng chức năng của chứng thực, ngoài xác nhận thanh toán còn xác định một số quyền cho chủ sở hữu chứng thực như quyền truy nhập tới một tài nguyên...v.v.
- Khách hàng và nhà cung cấp đăng ký với hai hệ thống thanh toán khác nhau.
- Trong thực tế các hệ thống thanh toán dùng giao thức HTTP. Chương trình được cài đặt bằng C#, chứng thực thanh toán là một đối tượng C#.

Để nâng cao khả năng tương tác cần chuyển sang XML cho việc trao đổi dữ liệu.

Do thời gian và năng lực bản thân còn hạn chế nên đồ án không tránh khỏi những thiếu sót, rất mong được sự góp ý và giúp đỡ của các thầy và các bạn để đồ án của tôi được hoàn thiện và có tính ứng dụng thực tiễn hơn. Trong thời gian tiếp theo, tôi sẽ tiếp tục hoàn thiện, nâng cao hiệu quả thuật toán. Và tôi mong thuật toán sẽ được ứng dụng rộng rãi hơn nữa vào các thanh toán điện tử.

TÀI LIỆU THAM KHẢO

[1] Q. X. WU, Y. X. Yang and Z. M. HU, "New signature schemes based on discrete logarithms and factoring", *Journal of Beijing University of Posts and Telecommunications*, vol. 24, pp. 61-65, January 2001.

[2] Z. Y. Shen and X. Y. Yu, "Digital signature scheme based on discrete logarithms and factoring", *Information Technology*, vol. 28,pp. 21-22, June 2004.

[3] Shimin Wei, "Digital Signature Scheme Based on Two Hard Problems", *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.12, December 2007.

[4] Eddie Shahrie Ismail, Tahat N.M.F., Rokiah. R. Ahmad, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms", *Journal of Mathematics and Statistics*, 04/2008; 12(3). DOI: 10.3844/jmssp.2008.222.225, Source:DOAJ.

[5] Qin Yanlin, Wu Xiaoping,"New Digital Signature Scheme Based on both ECDLP and IFP", *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, 8-11 Aug. 2009, E-ISBN: 978-1-4244-4520-2, pp 348 - 351.

[6] Swati Verma1, Birendra Kumar Sharma, "A New Digital Signature Scheme Based on Two Hard Problems", *International Journal of Pure and Applied Sciences and Technology*, ISSN 2229 - 6107, Int. J. Pure Appl. Sci. Technol., 5(2) (2011), pp. 55-59.

[7] Sushila Vishnoi, Vishal Shrivastava, "A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem", *International Journal of Computer Trends and Technology*, volume 3, Issue 4, 2012.

[8] A.N. Berezin, N.A. Moldovyan, V.A. Shcherbacov, "Cryptoschemes Based on Difficulty ofSimultaneous Solving Two Different DifficultProblems", Computer Science Journal of Moldova, vol.21, no.2(62), 2013.

[9] N.A. Moldovyan, “Digital Signature Scheme Based on a New Hard Problem”, Computer Science Journal of Moldova, vol.16, no.2(47), 2008.

[10] T. ElGamal, *“ A public key cryptosystem and a signature scheme based on discrete logarithms*”, IEEE Transactions on Information Theory. 1985, Vol. IT-31, No. 4. pp.469–472.