ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ KIM HUỆ

CHỮ KÝ SỐ
TRONG GIAO DỊCH THƯƠNG MẠI ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2015

MỤC LỤC

LỜI CAM KẾT

Tài liệu được sử dụng trong luận văn được thu thập từ các nguồn kiến thức hợp pháp, có trích dẫn nguồn tài liệu tham khảo. Chương trình sử dụng mã nguồn mở, có xuất xứ.

Dưới sự giúp đỡ nhiệt tình và chỉ bảo chi tiết của giáo viên hướng dẫn, tôi đã hoàn thành luận văn của mình. Tôi xin cam kết luận văn này là của bản thân tôi làm và nghiên cứu, không hề trùng hay sao chép của bất kỳ ai.

LỜI CẢM ƠN

Để hoàn thành chương trình cao học và viết luận văn này, em đã nhận được sự giúp đỡ và đóng góp nhiệt tình của các thầy cô trường Đại học Công nghệ thông tin và Truyền thông, Đại học Thái Nguyên.

Trước hết, em xin chân thành cảm ơn các thầy cô trong khoa Đào tạo sau đại học, đã tận tình giảng dạy, trang bị cho em những kiến thức quý báu trong suốt những năm học qua.

Đặc biệt em xin gửi lời cảm ơn sâu sắc đến PGS.TS Đỗ Trung Tuấn - người đã dành nhiều thời gian, công sức và tận tình hướng dẫn cho em trong suốt quá trình làm luận văn.

Xin chân thành cảm ơn gia đình, bạn bè đã nhiệt tình ủng hộ, giúp đỡ, động viên cả về vật chất lẫn tinh thần trong thời gian học tập và nghiên cứu.

Trong quá trình thực hiện luận văn, mặc dù đã rất cố gắng nhưng cũng không tránh khỏi những thiếu sót. Kính mong nhận được sự cảm thông và tận tình chỉ bảo của các thầy cô và các bạn.

DANH MỤC CÁC TỪ VIẾT TẮT

ANSI	American National Standards Institute
B2B	Business to business
B2C	Business to customers
Client	Khách, Máy khách
Client/ server	Khách / chủ
CNTT	Công nghệ Thông tin
CSDL	Cơ sở dữ liệu
DB	Database
DC	Data Communication
IDE	Integrated Development Environment
ISO	International Organization for Standardization
LHQ	Liên hiệp quốc
Server	Máy chủ, phía máy chủ
SQL	Structured Query Language
TMĐT	Thương mại điện tử
XML	eXtensible Markup Language
DSS	Digital Signature Standard
CA	Xác thực, certificate authoring
RSA	Tên thuật toán khóa công khai , theo tên của ba người sáng lập. Ron Rivest, Adi Shamir và Leonard Adleman
PKI	Public Key Infrastructure
Digital Signature Scheme	Lược đồ ký số
DSA	Digital Signature Algorithm
SHA	Security Hash Algorithm, thuật toán băm an toàn SHA

DANH MỤC HÌNH VẼ VÀ BẢNG BIỂU

MỞ ĐẦU

Với sự phát triển nhanh chóng của Internet, cùng với sự phát triển của nền kinh tế theo hướng hiện đại thì việc trao đổi thông tin, giao dịch hay mua bán hàng hóa…theo phương thức trực tiếp ngày càng giảm mà thay vào đó là các dịch vụ qua Internet. Dịch vụ thương mại điện tử (TMĐT) (Electronic-Commerce) là một bước phát triển nhảy vọt trong việc ứng dụng Internet vào cuộc sống và kinh doanh. Thông qua TMĐT, nhiều loại hình kinh doanh mới được hình thành, trong đó có việc mua bán hàng hóa và dịch vụ trên mạng. Với hình thức này sẽ tiết kiệm thời gian cho người tiêu dùng trong việc tiếp cận, lựa chọn hàng hóa theo nhu cầu, sở thích và trong việc thanh toán. Đồng thời tăng tính cạnh tranh, mở rộng thị trường, giảm chi phí bán hàng và tiếp thị cho các doanh nghiệp kinh doanh.

Thương mại điện tử [14], hay còn gọi là e-commerce, e-comm hay EC, là sự mua bán sản phẩm hay dịch vụ trên các hệ thống điện tử như Internet và các mạng máy tính. Thương mại điện tử dựa trên một số công nghệ như chuyển tiền điện tử, quản lý chuỗi dây chuyền cung ứng, tiếp thị Internet, quá trình giao dịch trực tuyến, trao đổi dữ liệu điện tử (EDI), các hệ thống quản lý hàng tồn kho, và các hệ thống tự động thu thập dữ liệu. Thương mại điện tử hiện đại thường được thực hiện trên công nghệ World Wide Web, kèm theo các thiết bị công nghệ như: Email, điện thoại di động….

Thương mại điện tử là một phần không thể thiếu được trong môi trường kinh doanh điện tử (e-business), đảm bảo cho vấn đề trao đổi dữ liệu, thanh toán dịch vụ trên mạng Internet.

E-commerce có thể được phân chia thành [14]:

E-tailing (bán lẻ trực tuyến) hoặc "cửa hàng ảo" trên trang web với các danh mục trực tuyến, đôi khi được gom thành các "trung tâm mua sắm ảo".

Trao đổi dữ liệu điện tử (EDI), trao đổi dữ liệu giữa Doanh nghiệp với Doanh nghiệp.

Email và fax, cách sử dụng chúng như là phương tiện cho việc tiếp cận và thiếp lập mối quan hệ với khách hàng (ví dụ như bản tin - newsletters)

Việc mua và bán giữa Doanh nghiệp với Doanh nghiệp.

Bảo mật các giao dịch kinh doanh.

Tóm lại, thương mại điện tử chỉ xảy ra trong môi trường kinh doanh mạng Internet và các phương tiện điện tử giữa các nhóm (cá nhân) với nhau thông qua các công cụ, kỹ thuật và công nghệ điện tử.

Nhưng đồng nghĩa với việc bên mua và bên bán không gặp nhau trực tiếp mà chỉ trao đổi thông tin, giao dịch qua Internet và các phương tiện điện tử nên rất dễ xảy ra tình trạng lừa đảo, giả mạo thông tin, gây mất mát thông tin và tài sản. Vì vậy, điều quan trọng trong thương mại điện tử là tính ràng buộc pháp lý nhằm bảo đảm thông tin giữa các bên trong hoạt động kinh doanh, mua bán hàng hóa, dịch vụ. Chữ ký số là một thành tố rất quan trọng trong TMĐT, nhằm đảm bảo độ an toàn thông tin, tính toàn vẹn dữ liệu và chống chối bỏ trách nhiệm trên nội dung đã ký giữa các đối tác thực hiện hoạt động kinh doanh, nghiệp vụ, dịch vụ,… với các ràng buộc pháp lý. Thấy được lợi ích khi sử dụng chữ ký số trên các tài liệu khi giao dịch giữa các đối tác trong thương mại điện tử và được sự đồng ý của giáo viên hướng dẫn, tôi đã chọn đề tài "Chữ ký số trong giao dịch thương mại điện tử" làm nội dung nghiên cứu cho luận văn của mình.

Luận văn gồm 3 chương:

Chương 1: Tổng quan về thương mại điện tử

Chương 2: An toàn thông tin và chữ ký số trong giao dịch thương mại điện tử

Chương 3: Cài đặt và thử nghiệm chữ ký số trong giao dịch TMĐT

Cuối luận văn là phần kết luận và danh sách các tài liệu tham khảo.