ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

PHẠM THỊ THANH THỦY

NGHIÊN CỨU MỘT SỐ BÀI TOÁN VỀ AN TOÀN THÔNG TIN TRONG THỎA THUẬN VÀ KÝ KẾT HỢP ĐỒNG CỦA THƯƠNG MẠI ĐIỆN TỬ

Ngành: Công nghệ thông tin
Chuyên ngành: Hệ thống thông tin
Mã số: 60480104

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS. TS. TRỊNH NHẬT TIẾN

Học viên thực hiện Giáo viên hướng dẫn Chủ tịch hội đồng

Hà Nội – 2016

LỜI CẢM ƠN

Trong khoảng thời gian nghiên cứu và học tập tại trường Đại học Công Nghệ - Đại học Quốc Gia Hà Nội, bản thân tôi đã được sự động viên và giúp đỡ rất lớn của gia đình, thầy cô và bạn bè, đặc biệt là Thầy PGS. TS. Trịnh Nhật Tiến - Thầy là người trực tiếp hướng dẫn luận văn cho tôi, Thầy luôn chỉ dạy mỗi khi tôi gặp khó khăn trong việc tìm hiểu đề tài của mình. Thầy đã giúp tôi vững vàng và trưởng thành hơn rất nhiều trên con đường nghiên cứu và học tập. Thầy ơi, em muốn gửi tới Thầy lời tri ân chân thành và sâu sắc nhất, em chúc Thầy luôn mạnh khỏe để tiếp tục sự nghiệp trồng người và tiếp tục hướng dẫn những thế hệ chúng em đạt được những thành quả cao hơn trên con đường mà mình đã chọn.

Tôi xin bày tỏ lòng biết ơn chân thành tới các Thầy - Cô giáo, các anh chị, các bạn trong chuyên ngành Hệ thống thông tin - khoa Công nghệ thông tin, những người luôn sát cánh bên tôi, nhiệt thành chỉ bảo, hướng dẫn và chia sẻ với tôi rất nhiều những kiến thức về công nghệ thông tin - đó là những kiến thức quý báu và bổ ích giúp tôi tự tin hơn trong công việc của mình. Hơn thế nữa, tình cảm tôi nhận được từ những người bạn trong khoảng thời gian học tập tại trường đã giúp chúng tôi thân thiết hơn và trở thành những người bạn tốt của nhau, đó là một điều tuyệt vời!!!

Tôi xin gửi lời cảm ơn chân thành tới Ban Giám hiệu Nhà trường, Phòng Đào tạo sau đại học, Đại học Công nghệ - Đại học Quốc gia Hà Nội đã tạo điều kiện tốt nhất giúp tôi trong suốt quá trình học tập.

Cuối cùng tôi muốn gửi đến gia đình những tình cảm thân thương nhất. Con cảm ơn bố mẹ đã luôn tin tưởng, động viên và giúp đỡ để con đạt được mơ ước của mình. Cảm ơn anh và con luôn là chỗ dựa vững chắc giúp em cố gắng phấn đấu, cảm ơn các em đã dành mọi điều kiện để giúp chị tập trung vào nghiên cứu.

Hà Nội, ngày ... tháng... năm 2016
Học viên

Phạm Thị Thanh Thủy

LỜI CAM ĐOAN

Tôi xin cam đoan nội dung trình bày trong luận văn này là do tôi tự nghiên cứu và tìm hiểu dưới sự hướng dẫn trực tiếp của Thầy PGS. TS. Trịnh Nhật Tiến. Luận văn này của tôi chưa từng được ai công bố trong bất cứ công trình nào trước đây. Trong quá trình nghiên cứu tôi có tham khảo đến các tài liệu của một số tác giả. Tôi đều có trích dẫn đầy đủ và liệt kê trong mục "TÀI LIỆU THAM KHẢO" ở cuối luận văn.

Hà Nội, ngày ... tháng ... năm 2016

Học viên

Phạm Thị Thanh Thủy

MỤC LỤC

LỜI CẢM ƠN i
LỜI CAM ĐOAN ii
LỜI MỞ ĐẦU 1
CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN 3
1.1. Tổng quan về thương mại điện tử 3
1.1.1. Khái niệm về TMĐT 3
1.1.2. Vai trò tác động của TMĐT 4
1.1.3. Các đặc trưng của TMĐT 6
1.1.4. Các loại hình giao dịch TMĐT 8
1.1.5. Ba giai đoạn hoạt động của TMĐT 10
1.2. Tổng quan về An toàn thông tin 12
1.2.1. An toàn thông tin là gì? Tại sao cần bảo đảm An toàn thông tin? 12
1.2.2. Mục tiêu của An toàn thông tin 13
1.2.3. Các giải pháp bảo đảm An toàn thông tin 13
1.3. Mã hóa dữ liệu 14
1.3.1. Khái niệm Mã hóa dữ liệu 15
1.3.2. Phân loại hệ mã hóa 16
1.3.3. Một số Hệ mã hóa tiêu biểu 18
1.4. Chữ ký số 23
1.4.1. Khái niệm "Chữ ký số" 23
1.4.2. Một số chữ ký số tiêu biểu 25
1.5. Đại diện tài liệu và hàm băm 27
1.5.1. Hàm băm (Hàm tạo đại diện tài liệu) 27
1.5.2. Các Hàm băm 28
1.6. Thủy vân số (Digital watermarking) 28
1.6.1 Phân loại Thủy vân số 29
1.6.2. Các ứng dụng của Thuỷ vân với ảnh số 30

CHƯƠNG 2. CÁC BÀI TOÁN VỀ ATTT TRONG THỎA THUẬN VÀ KÝ KẾT HỢP ĐỒNG CỦA TMĐT 31
2.1. Thỏa thuận và ký kết hợp đồng của TMĐT 31
2.1.1. Khái niệm về giao kết hợp đồng điện tử 31
2.1.2. Chủ thể của hợp đồng điện tử 31
2.1.3. Hình thức hợp đồng điện tử 33
2.1.4. Nội dung hợp đồng điện tử 33
2.2. Các bài toán về ATTT trong thỏa thuận và ký kết hợp đồng của TMĐT 34
2.2.1. Bảo đảm tính toàn vẹn thông tin hợp đồng trực tuyến 35
2.2.2. Bảo đảm tính xác thực 45
2.2.3. Chống chối bỏ hợp đồng giao dịch 47
CHƯƠNG 3. THỰC NGHIỆM CHƯƠNG TRÌNH 50
3.1. Giới thiệu chương trình 50
3.1.1. Chương trình mã hóa AES 50
3.1.2. Chương trình ký không thể phủ định 50
3.2. Cấu hình hệ thống 50
3.3. Hướng dẫn sử dụng 50
3.3.1. Chương trình mã hóa AES 50
3.3.2. Chương trình ký không thể phủ định 55
KẾT LUẬN 58
TÀI LIỆU THAM KHẢO 59

BẢNG CÁC CHỮ VIẾT TẮT

Từ viết tắt	Ý nghĩa
AES	Advance Encryption Standard (Chuẩn mã hóa tiên tiến)
DES	Data Encryption Standard (Chuẩn mã hóa dữ liệu)
RSA	Rivest, Shamir, & Adleman (Một công nghệ mã hóa khóa công khai)
UNCITRAL	The United Nations Commission on International Trade Law (Ủy ban về Luật Thương mại Quốc tế của Liên Hợp Quốc)
TMĐT	Thương mại điện tử
ATTT	An toàn thông tin

DANH SÁCH HÌNH VẼ VÀ BẢNG

Danh mục hình

Hình 1.1: Mô hình đơn giản thương mại điện tử 3
Hình 1.2: Khảo sát giá trị mua hàng trực tuyến của người dùng Việt Nam 2015 5
Hình 1.3: Biểu đồ Quy mô TMĐT Việt Nam (tỷ USD). 6
Hình 1.4: Biểu đồ so sánh mức độ ứng dụng TMĐT ở Việt Nam 6
Hình 1.5: Các loại giao dịch B2B trong TMĐT 8
Hình 1.6: Doanh thu bán lẻ TMĐT của Hoa Kỳ 9
Hình 1.7: Doanh thu bán lẻ TMĐT của Hàn Quốc 9
Hình 1.8: Doanh thu bán lẻ TMĐT của Indonesia 9
Hình 1.9: Doanh thu bán lẻ TMĐT của Úc 10
Hình 1.10: Doanh thu bán lẻ TMĐT của Ấn Độ 10
Hình 1.11: Sơ đồ mã hóa đơn giản. 15
Hình 1.12: Phân loại Thủy vân 29
Hình 1.13: Ví dụ về thuỷ vân hiện (trên trang web của Thư viện số liên bang Mỹ) 29
Hình 1.14: Giấu thông tin trong ảnh 30
Hình 2.1: Mô hình giải quyết bài toán 34
Hình 2.2: Sơ đồ thuật toán AES 38
Hình 2.3: Các phần tử biến đổi của S-box dưới dạng ma trận 39
Hình 2.4: Kết quả biến đổi của hàm SubBytes() với mảng trạng thái 39
Hình 2.5: Nội dung bảng S-box sau khi tính toán 40
Hình 2.6: Kết quả tính toán 40
Hình 2.7: Minh họa sự dịch vòng 41
Hình 2.8: Minh họa làm việc trên cột trạng thái 42
Hình 2.9: Thực hiện hàm AddRoundKey() 42
Hình 2.10: Quá trình thực hiện Expand Key 43
Hình 2.11: Minh họa thực hiện hàm InvShiftRows() 44
Hình 2.14: Kiểm tra tính đúng đắn của chữ ký 48
Hình 2.15: Giao thức kiểm thử chữ ký số 49
Hình 2.16: Giao thức chối bỏ chữ ký số. 49
Hình 3.1: Quá trình mã hóa văn bản 51
Hình 3.2: Quá trình giải mã văn bản 52
Hình 3.3: Quá trình mã hóa tệp tin 53
Hình 3.4: Quá trình giải mã tệp tin 54
Hình 3.5: Quá trình ký 56
Hình 3.6: Giao thức kiểm thử 56
Hình 3.7: Giao thức chối bỏ. 57

Danh mục bảng

Bảng 1: Qui ước một số từ viết tắt và thuật ngữ của AES *20*

Bảng 2: Các hàm, ký hiệu, các tham số của thuật toán *21*

Bảng 3: Các trạng thái của AES *36*

Bảng 4: Độ dài khóa AES *37*

LỜI MỞ ĐẦU

Như chúng ta đã biết, ngày nay thông tin trở thành một tài nguyên vô giá và không thể thiếu trong các hoạt động của con người. Nhu cầu trao đổi thông tin ngày càng lớn. Mạng máy tính ra đời giúp việc trao đổi và xử lý thông tin một cách dễ dàng và nhanh chóng.

Các cơ quan, tổ chức, cá nhân ở khắp mọi nơi trên thế giới biết đến nhau thông qua việc sử dụng Internet để trao đổi thông tin và dữ liệu. Internet đã tác động sâu sắc đến hoạt động sản xuất kinh doanh của các doanh nghiệp và tác động đến hầu hết mọi hoạt động của đời sống kinh tế xã hội. Trong đó, việc thỏa thuận và ký kết hợp đồng giữa các bên tham gia là một khâu rất quan trọng đòi hỏi các bên phải thực hiện hợp đồng theo đúng khuôn khổ pháp lý và được pháp luật công nhận. Trước tiên, ta phải hiểu Hợp đồng điện tử là gì? Theo [10] Luật Giao dịch điện tử Việt Nam 2005 chỉ ra rằng Hợp đồng điện tử là hợp đồng được thiết lập dưới dạng thông điệp dữ liệu, trong đó thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử[1]. Trước đây, các bên tham gia sẽ trực tiếp gặp nhau để giới thiệu, lựa chọn sản phẩm, bàn bạc và cùng thống nhất ký vào hợp đồng nhưng ngày nay nhờ Internet mà việc thỏa thuận hợp đồng giảm được nhiều thời gian trao đổi giữa doanh nghiệp với doanh nghiệp đối tác cũng như các khách hàng của họ và sau khi bàn bạc họ cũng đưa ra quyết định và ký vào hợp đồng nhưng khác với phương thức truyền thống ở chỗ là việc thỏa thuận và ký kết diễn ra trên mạng, đó chính là Hợp đồng điện tử.

Vấn đề đặt ra là trong môi trường mạng một lượng tin hay dữ liệu khi được gửi từ người gửi đến người nhận thường phải qua nhiều nút, nhiều trạm không ai đảm bảo rằng thông tin đến người nhận không bị sao chép, không bị đánh cắp hay không bị sửa đổi…Mục 1.3 [2] chỉ ra rằng bảo đảm an toàn thông tin trong thỏa thuận và ký kết hợp đồng của thương mại điện tử là bảo đảm việc xác minh nguồn gốc giao dịch, đảm bảo bí mật, toàn vẹn thông tin và chống chối bỏ giao dịch. Đây là một vấn đề cấp thiết cần phải được giải quyết hiện nay, xuất phát từ yêu cầu này mà tác giả đã lựa chọn đề tài ***"Nghiên cứu một số bài toán về an toàn thông tin trong thỏa thuận và ký kết hợp đồng của thương mại điện tử"*** làm đề tài nghiên cứu của mình.

Trên cơ sở làm rõ một số bài toán về an toàn thông tin trong giai đoạn thỏa thuận và ký kết hợp đồng điện tử, luận văn sẽ tập trung nghiên cứu một số kỹ thuật để đảm bảo việc xác minh nguồn gốc giao dịch, đảm bảo bí mật, toàn vẹn thông tin

[1] Phương tiện điện tử là phương tiện hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, điện từ hoặc công nghệ tương tự.

và chống chối bỏ giao dịch cũng như thử nghiệm chương trình thực hiện việc xác nhận đúng hợp đồng, đảm bảo thông tin hợp đồng không bị sửa đổi và tiến hành ký kết hợp đồng.

Nhiệm vụ cụ thể mà luận văn cần giải quyết đó là:

- Nêu rõ khái niệm, vai trò, đặc điểm, phân loại, phương pháp và các vấn đề gặp phải khi thực hiện thỏa thuận hợp đồng điện tử.
- Phân tích, nghiên cứu, tìm hiểu một số bài toán về ATTT trong thỏa thuận và ký kết hợp đồng điện tử.
- Nghiên cứu một số kỹ thuật đảm bảo an toàn thông tin trong giai đoạn thỏa thuận hợp đồng.
- Xây dựng chương trình thử nghiệm sử dụng các kỹ thuật trên để thực hiện việc giải quyết một số bài toán trong thỏa thuận và ký kết hợp đồng.

Đối tượng nghiên cứu của đề tài là những vấn đề liên quan đến giai đoạn thứ hai của quy trình TMĐT (giai đoạn thỏa thuận hợp đồng), trong đó đặc biệt chú trọng đến việc nghiên cứu các kỹ thuật đảm bảo An toàn thông tin trong giai đoạn này.

Phạm vi nghiên cứu của luận văn tập trung chủ yếu đến các kỹ thuật thủy vân số, mã hóa, chữ ký số để xác minh nguồn gốc giao dịch, đảm bảo tính toàn vẹn thông tin và chống chối bỏ giao dịch trong thỏa thuận và ký kết hợp đồng. Ngoài ra còn có một số kỹ thuật khác cũng được đề cập trong luận văn.

Về phương pháp tiếp cận của bài toán, tác giả sử dụng các phương pháp cơ bản như:

- Phương pháp phân tích và tổng hợp lý thuyết.
- Phương pháp chuyên gia khi tham khảo các giáo trình, bài giảng, tạp chí liên quan đến việc giải quyết bài toán.
- Phương pháp diễn giải các thuật toán.
- Phương pháp tổng hợp để đưa ra kết luận.

Luận văn được trình bày theo bố cục như sau:

Chương 1. Các khái niệm cơ bản. Trong chương này, tác giả sẽ nêu tổng quan về An toàn thông tin trong TMĐT, hướng tiếp cận, phương pháp giải quyết.

Chương 2. Các bài toán về ATTT trong thỏa thuận và ký kết hợp đồng của TMĐT. Chương này sẽ giới thiệu những bài toán về ATTT trong giai đoạn thỏa thuận hợp đồng. Tiếp theo là đưa ra các kỹ thuật cụ thể để giải quyết từng bài toán trong giai đoạn này bao gồm: Thủy vân số để xác nhận đúng hợp đồng, Mã hóa AES để mã hóa hợp đồng và chữ ký không thể phủ nhận để ký kết hợp đồng.

Chương 3. Thực nghiệm chương trình. Là chương cài đặt, thử nghiệm chương trình ứng dụng mã hóa AES và chữ ký không thể phủ nhận để giải quyết bài toán đặt ra.

TÀI LIỆU THAM KHẢO

- **Tài liệu tiếng Việt:**

[1] Trịnh Nhật Tiến. Giáo trình An toàn dữ liệu - Đại học Công Nghệ - ĐH Quốc Gia Hà Nội, 2008.

[2] Trịnh Nhật Tiến. Bài giảng Tổng quan về An toàn thông tin trong TMĐT - Đại học Công Nghệ - Đại học Quốc Gia Hà Nội.

[3] Phan Đình Diệu. Lý thuyết mật mã và An toàn thông tin, 2002.

[4] Nguyễn Đăng Hậu. Kiến thức thương mại điện tử, 11- 2004.

[5] Trần Phương Nam. Tiểu luận Mật mã và An toàn dữ liệu-ĐHCN-ĐHQGHN, 2014.

[6] Hoàng Thị Vân. Tiểu luận Mật mã và An toàn dữ liệu-ĐHCN-ĐHQGHN, 2013.

[7] Phạm Thành Luân. Đồ án tốt nghiệp: Tìm hiểu, nghiên cứu một số tình huống trong thỏa thuận hợp đồng điện tử - ĐHDL Hải Phòng, 2012.

[8] Lê Thị Thu. Luận văn thạc sĩ: Nghiên cứu một số giao thức bảo vệ thông tin trong thỏa thuận hợp đồng điện tử - ĐHCN - ĐHQGHN, 2011.

- **Website:**

[9] http://en.wikipedia.org/wiki/Thuong_mai_dien_tu

[10] http://www.moj.gov.vn

[11] http://vixra.org/pdf/1405.0049v1.pdf

[12] http://www.dynamicwebs.com.au/tutorials/e-commerce.htm#services

[13] http://ecommerce.httt.uit.edu.vn

[14] http://en.wikipedia.org/wiki/Digital_signature

[15] http://www.rsa.com/rsalabs/node.asp?id=2344

- **Tài liệu tiếng Anh:**

[16] Chaum, David, van Heijst, Eugene and Pfitzmann, Birgit, *Cryptographically strong undeniable signatures, unconditionally secure for the signer* (extended abstract)

[17] *Ecient Convertible Undeniable Signature Schemes* – D. Chaum, E. van Heys

[18] William Stallings (2007), *Cryptography and Network Security*, Third Edition.

[19] D. Stinson. *Cryptography: Theory and Practice*, CRT Press 1995.

[20] N. F. Johnson (2002), *Steganography*, George Mason University, pp 5-6.

[21] Bruce Schneier (1999), *Applied Cryptography*, Second Edition.

[22] Alfred J. Menezes Paul C. van Ooschot Scott A. Vanstone (1998): *Handbook of Applied Cryptography*, CRC press.

[23] Bart Van Rompay. *Analysis and Desigbn of Cryptographic Hash Functions*, MAC Algorithms and Block Ciphers, Juni 2004.

[24] Benoıt Libert Jean-Jacques Quisquater, *Identity Based Undeniable Signatures*, UCL Crypto Group, Belgium.

[25] David Chaum, Hans van Antwerpen. *Undeniable Signature*. CRYPTO.

[26] Moti Young : *Weaknesses of Undeniable Signature Schemes.*