

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

LÊ THỊ THANH VÂN

**NGHIÊN CỨU MỘT SỐ KỸ THUẬT AN TOÀN
THÔNG TIN DÙNG TRONG RÚT TIỀN ĐIỆN TỬ**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: PGS.TS TRỊNH NHẬT TIẾN

Thái Nguyên - 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này của tự bản thân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của PGS.TS Trịnh Nhật Tiến. Các chương trình thực nghiệm do chính bản thân tôi lập trình, các kết quả là hoàn toàn trung thực. Các tài liệu tham khảo được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Lê Thị Thanh Vân

LỜI CẢM ƠN

Tôi xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã dạy dỗ chúng em trong quá trình học tập chương trình cao học tại trường.

Đặc biệt em xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo PGS.TS Trịnh Nhật Tiên, Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội đã nhiệt tình chỉ bảo, định hướng, hướng dẫn em hoàn thiện luận văn cao học này.

Cuối cùng, em xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với em trong quá trình làm luận văn cũng như trong quá trình học cao học.

Thái Nguyên, ngày 20 tháng 8 năm 2015

HỌC VIÊN

Lê Thị Thanh Vân

MỤC LỤC

	Trang
LỜI CAM ĐOAN	i
LỜI CẢM ƠN.....	ii
MỤC LỤC.....	iii
DANH MỤC HÌNH VẼ.....	vi
DANH MỤC BẢNG BIỂU.....	vi
MỞ ĐẦU	1
Chương 1: TỔNG QUAN VỀ GIAO DỊCH BẰNG TIỀN ĐIỆN TỬ VÀ AN TOÀN BẢO MẬT THÔNG TIN	3
1.1. TỔNG QUAN VỀ GIAO DỊCH BẰNG TIỀN ĐIỆN TỬ	3
1.1.1. Khái niệm tiền	3
1.1.2. Khái niệm tiền điện tử	3
<i>1.1.3. Cấu trúc, tính chất của tiền điện tử</i>	4
<i>1.1.3.1. Cấu trúc</i>	4
<i>1.1.3.2. Tính chất của tiền điện tử</i>	5
1.1.4. Mô hình giao dịch bằng tiền điện tử	7
1.1.5. Giao dịch bằng tiền điện tử tại Việt Nam	9
<i>1.1.5.1. Thẻ phone card</i>	9
<i>1.1.5.2. Thẻ Flexicard</i>	10
<i>1.1.5.3. Thẻ ATM</i>	11
<i>1.1.5.4. Yếu tố ảnh hưởng đến tiền điện tử tại Việt Nam</i>	11
1.2. MÃ HÓA	12
1.2.1. Tổng quan về mã hóa dữ liệu	12
<i>1.2.1.1. Hệ mã hóa</i>	12
<i>1.2.1.2. Mã hóa và giải mã</i>	13
<i>1.2.2. Phân loại hệ mã hóa</i>	13
<i>1.2.3. Một số thuật toán mã hóa khóa công khai</i>	15

1.3. CHỮ KÝ SỐ	15
1.3.1. Khái niệm chữ ký số	15
1.3.1.1. Giới thiệu	15
1.3.1.2. Sơ đồ chữ ký số	16
1.3.2. Một số vấn đề liên quan đến chữ ký số	17
1.3.2.1. Đại diện tài liệu	17
1.3.2.2. Hàm băm	18
1.3.3. Một số sơ đồ ký số	18
1.3.3.1. Sơ đồ ký số RSA	18
1.3.3.2. Sơ đồ ký số Schnorr	19
1.3.4. Chữ ký mù	20
1.3.4.1. Giới thiệu về chữ ký mù	20
1.3.4.2. Một số sơ đồ ký mù	21
1.4. NGUY CƠ MẤT AN TOÀN THÔNG TIN TRONG GIAI ĐOẠN RÚT TIỀN ĐIỆN TỬ	22
1.4.1. Mạo danh chủ tài khoản	22
1.4.2. Tiền giả	23
1.4.3. Tính riêng tư của người tiêu tiền	23
1.4.4. Mất “cấp” tiền điện tử	24
1.4.5. Khai man giá trị đồng tiền	24
1.4.6. Xâm phạm có sự kết hợp của nhân viên ngân hàng	24
Chương II: MỘT SỐ KỸ THUẬT ĐẢM BẢO AN TOÀN THÔNG TIN ỨNG DỤNG TRONG GIAI ĐOẠN RÚT TIỀN ĐIỆN TỬ	26
2.1. KỸ THUẬT “CHỨNG MINH KHÔNG TIẾT LỘ THÔNG TIN”	27
2.2. KỸ THUẬT CHỮ KÝ MÙ THEO SƠ ĐỒ KÝ SỐ RSA VỚI NHIỀU KHÓA KÝ	30
2.2.1. Chữ ký số “mù” theo sơ đồ ký RSA	30
2.2.2. Ứng dụng của chữ ký mù RSA trong giai đoạn rút tiền	32
2.2.2.1. Kiểm tra tính hợp pháp của đồng tiền	33

2.2.2.2. <i>Đảm bảo tính riêng tư</i>	33
2.2.2.3. <i>Bảo vệ đồng tiền</i>	36
2.2.2.4. <i>Phòng tránh khai man giá trị đồng tiền</i>	38
2.3. KỸ THUẬT CHIA SẺ BÍ MẬT	41
2.3.1. Chia sẻ khóa bí mật K	43
2.3.2. Khôi phục khóa bí mật K	44
Chương 3: CÀI ĐẶT THỬ NGHIỆM	45
3.1. ỨNG DỤNG CHỮ KÝ MÙ RSA TRONG GIAI ĐOẠN RÚT TIỀN ĐIỆN TỬ	46
3.1.1. Sinh khóa	47
3.1.2. Ký “mù” lên đồng tiền	47
3.1.3. Xóa mù	47
3.1.4. Kiểm tra chữ ký	48
3.2. CHỨNG MINH KHÔNG TIẾT LỘ THÔNG TIN TRONG XÁC THỰC CHỦ TÀI KHOẢN	48
3.2.1. Khởi tạo các thông số ban đầu	48
3.2.2. Chủ tài khoản gửi yêu cầu xác minh	48
3.2.3. Ngân hàng gửi thử thách	48
3.2.4. Chủ tài khoản gửi chứng minh	48
3.2.5. Ngân hàng kiểm tra tính hợp pháp của chủ tài khoản	49
3.3. CHƯƠNG TRÌNH THỬ NGHIỆM	49
3.3.1. Chương trình thử nghiệm chữ ký mù RSA	49
3.3.2. Chương trình “Chứng minh không tiết lộ thông tin” trong xác thực chủ tài khoản	52
3.3.3. Đánh giá	56
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN ĐỀ TÀI	57
TÀI LIỆU THAM KHẢO	58

DANH MỤC HÌNH VẼ

	Trang
Hình 1.1 : Mô hình giao dịch tiền điện tử.....	7
Hình 1.2: Sơ đồ mã hóa	13
Hình 1.3: Sơ đồ mã hóa khóa đối xứng	14
Hình 1.4: Sơ đồ mã hóa khóa bí mật	14
Hình 1.5: Sơ đồ tổng quát về quá trình ký mù	20
Hình 2.1: Khởi tạo tài khoản người dùng	28
Hình 2.2: Sơ đồ quá trình xác thực tính hợp pháp của chủ tài khoản.....	30
Hình 2.3: Ứng dụng chữ ký mù trong giai đoạn rút tiền điện tử	32
Hình 2.4: Sơ đồ chia sẻ bí mật khóa ký	41
Hình 3.1: Sơ đồ tổng quan giao dịch điện tử	45
Hình 3.2: Sơ đồ luồng dữ liệu khi ký mù lên đồng tiền	46
Hình 3.3: Đồng tiền	49
Hình 3.4: Thực hiện ký mù lên đồng tiền	50
Hình 3.5: Đồng tiền đã làm mù và chữ ký mù của ngân hàng trên đồng tiền..	50
Hình 3.6: Thực hiện xóa mù cho đồng tiền	51
Hình 3.7: Chữ ký trên đồng tiền của ngân hàng	51
Hình 3.8a: Kiểm tra chữ ký - chữ ký đúng: tiền thật	52
Hình 3.8b: Kiểm tra chữ ký - chữ ký sai: tiền “giả”	52
Hình 3.9: Khởi tạo các thông số ban đầu	53
Hình 3.10: Chủ tài khoản gửi yêu cầu xác minh.....	53
Hình 3.11: Giá trị y được gửi lại cho ngân hàng	54
Hình 3.12: Ngân hàng gửi thử thách	54
Hình 3.13: Giá trị thử thách r_1, r_2	55
Hình 3.14: Xác thực đúng chủ tài khoản - tiếp tục giao dịch	55

DANH MỤC BẢNG BIỂU

	Trang
Bảng 2.1: Các bước kiểm tra tính hợp pháp của đồng tiền.....	31
Bảng 2.2: Các bước ký mù lên đồng tiền sử dụng nhiều khóa ký	39
Bảng 3.1: Những thông số cần có của chủ tài khoản và ngân hàng	53

MỞ ĐẦU

Trong thời đại công nghệ thông tin và Internet phát triển như hiện nay, giao dịch điện tử đã trở nên phổ biến. Người ta có thể sử dụng tiền điện tử để thanh toán cho các giao dịch điện tử này. Tiền điện tử là phương tiện của thanh toán điện tử được bảo mật bằng chữ ký điện tử, và cũng như tiền giấy nó có chức năng là phương tiện trao đổi và tích lũy giá trị. Nếu như giá trị của tiền giấy được đảm bảo bởi chính phủ phát hành thì đối với tiền điện tử, giá trị của nó được tổ chức phát hành đảm bảo bằng việc cam kết sẽ chuyển đổi tiền điện tử sang tiền giấy theo yêu cầu của người sở hữu.

Quá trình dùng tiền điện tử có sự tham gia của Ngân hàng, người trả tiền, người được trả tiền và chia làm ba giai đoạn:

Giai đoạn 1: Người tiêu tiền rút tiền điện tử từ ngân hàng

Giai đoạn 2: Người tiêu tiền thanh toán tiền điện tử (tiêu tiền) cho bên người được trả tiền

Giai đoạn 3: Người được trả tiền gửi tiền điện tử vào ngân hàng

Tiền điện tử mang lại lợi ích không chỉ cho phía người dùng mà còn cho cả phía ngân hàng cũng như phía nhà cung cấp. Tiền điện tử làm tăng tốc độ cũng như hiệu quả của các phiên giao dịch. Tuy nhiên để tiền điện tử thực sự trở thành một phương thức thanh toán hữu hiệu, các nhà công nghệ, các nhà phát triển và các chuyên gia an toàn thông tin còn đứng trước nhiều thách thức như: yêu cầu rút tiền có thể bị mạo danh, sửa đổi. Khi đó đòi hỏi ngân hàng phải thẩm định xem yêu cầu rút tiền đó có đúng không (đúng tài khoản, đúng số tiền, đúng chủ tài khoản). Và đặc biệt khi “tiêu tiền”, làm thế nào có thể ẩn danh người tiêu tiền với tiền vì đây là tiền điện tử chứ không phải là tiền giấy. Đặc biệt, làm thế nào người tiêu tiền không thể tiêu một đồng tiền nhiều lần, hay khai man giá trị của đồng tiền cũng như trong quá trình chuyển tiền từ người này sang người khác thì tiền được “an toàn”, ...

Từ những nhận định trên và sự gợi ý của giáo viên hướng dẫn, tôi quyết định chọn đề tài: **“Nghiên cứu một số kỹ thuật an toàn thông tin dùng trong rút tiền điện tử”**

Nội dung chính của luận văn gồm có ba chương

Chương 1: Tổng quan về giao dịch bằng tiền điện tử và an toàn bảo mật thông tin

Trong chương này luận văn trình bày về tiền điện tử, giao dịch bằng tiền điện tử, nguy cơ mất an toàn thông tin khi người dùng rút tiền điện tử từ ngân hàng và kiến thức cơ bản về mã hóa, chữ ký số, chia sẻ bí mật.

Chương 2: Một số kỹ thuật đảm bảo an toàn thông tin ứng dụng trong giai đoạn rút tiền điện tử

Nội dung chương 2 trình bày về một số kỹ thuật để đảm bảo an toàn bảo mật thông tin trong giai đoạn rút tiền điện tử từ tài khoản trong ngân hàng của người dùng như: chữ ký mù, mã hóa, chia sẻ bí mật...

Chương 3: Cài đặt thử nghiệm

Toàn chương 3 trình bày phương pháp chữ ký “mù” trong ký xác thực lên đồng tiền và chứng minh không tiết lộ thông tin trong xác thực chủ tài khoản khi rút tiền điện tử từ ngân hàng và xây dựng chương trình thử nghiệm. Chương trình thử nghiệm được viết bằng ngôn ngữ lập trình C#.