

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CNTT&TT THÁI NGUYÊN

PHẠM MINH TUÂN

NGHIÊN CỨU CÁC LỢC ĐO CHỮ KÝ SỐ
DỰA TRÊN HỆ MẬT RSA, ỨNG DỤNG
TRONG HỆ THỐNG TIỀN ĐIỆN TỬ

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

THÁI NGUYÊN, 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CNTT&TT THÁI NGUYÊN

PHẠM MINH TUÂN

**NGHIÊN CỨU CÁC LƯỢC ĐỒ CHỮ KÝ SỐ
DỰA TRÊN HỆ MẬT RSA, ỨNG DỤNG
TRONG HỆ THỐNG TIỀN ĐIỆN TỬ**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. VŨ MẠNH XUÂN

THÁI NGUYÊN, 2014

LỜI CAM ĐOAN

Tên tôi là: Phạm Minh Tuân

Sinh ngày: 01/09/1983

Học viên lớp cao học CHK11G - Trường Đại học Công nghệ thông tin và Truyền thông – Thái Nguyên.

Xin cam đoan: Đề tài “*Nghiên cứu các lược đồ chữ ký số dựa trên hệ mật RSA, ứng dụng trong hệ thống tiền điện tử*” do thầy giáo TS. Vũ Mạnh Xuân hướng dẫn là công trình nghiên cứu của riêng tôi. Tất cả tài liệu tham khảo đều có nguồn gốc, xuất xứ rõ ràng.

Tác giả xin cam đoan tất cả những nội dung trong luận văn đúng như nội dung trong đề cương và yêu cầu của thầy giáo hướng dẫn. Nếu sai tôi hoàn toàn chịu trách nhiệm trước hội đồng khoa học và trước pháp luật.

Thái Nguyên, ngày .. tháng .. năm 2014

TÁC GIẢ LUẬN VĂN

LỜI CẢM ƠN

Sau một thời gian nghiên cứu và làm việc nghiêm túc, được sự động viên, giúp đỡ và hướng dẫn tận tình của Thầy giáo hướng dẫn TS. Vũ Mạnh Xuân, luận văn với đề tài “*Nghiên cứu các lược đồ chữ ký số dựa trên hệ mật RSA, ứng dụng trong hệ thống tiền điện tử*” đã hoàn thành.

Tôi xin bày tỏ lòng biết ơn sâu sắc đến:

Thầy giáo hướng dẫn TS. Vũ Mạnh Xuân đã tận tình chỉ dẫn, giúp đỡ tôi hoàn thành luận văn này.

Khoa sau Đại học Trường Đại học công nghệ thông tin và truyền thông đã giúp đỡ tôi trong quá trình học tập cũng như thực hiện luận văn.

Tôi xin chân thành cảm ơn bạn bè, đồng nghiệp và gia đình đã động viên, khích lệ, tạo điều kiện giúp đỡ tôi trong suốt quá trình học tập, thực hiện và hoàn thành luận văn này.

TÁC GIẢ LUẬN VĂN

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC.....	iii
DANH MỤC BẢNG BIỂU	iii
DANH MỤC HÌNH VẼ.....	iv
MỞ ĐẦU.....	1
CHƯƠNG 1. TỔNG QUAN VỀ TIỀN ĐIỆN TỬ	5
1.1 THANH TOÁN ĐIỆN TỬ.....	5
1.1.1 Khái niệm thanh toán điện tử	5
1.1.2 Các mô hình thanh toán điện tử.....	5
1.2 TIỀN ĐIỆN TỬ.....	7
1.2.1 Khái niệm	7
1.2.2 Mô hình giao dịch mua bán bằng tiền điện tử.....	8
1.2.3 Cấu trúc của Tiền điện tử	9
1.2.4 Tính chất của tiền điện tử	10
1.3 VẤN ĐỀ PHÁT SINH TRONG DÙNG TIỀN ĐIỆN TỬ	13
1.3.1 Vấn đề ẩn danh người sử dụng đồng tiền	13
1.3.2 Vấn đề gian lận giá trị đồng tiền	13
1.3.3 Vấn đề tiêu xài một đồng tiền hai lần.....	14
1.4 VẤN ĐỀ DÙNG TIỀN ĐIỆN TỬ Ở VIỆT NAM.....	14
1.4.1 Xây dựng “đường đi” an toàn cho đồng tiền điện tử.	14
1.4.2 Xây dựng các cơ sở bảo vệ “ví tiền” của người sử dụng.	15
KẾT LUẬN CHƯƠNG 1	16
CHƯƠNG 2. AN TOÀN THÔNG TIN BẰNG MẬT MÃ VÀ CHỮ KÝ SỐ.....	17
2.1. TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN	17
2.1.1. Sự cần thiết của bảo đảm an toàn thông tin.....	17
2.1.2. Khái niệm an toàn thông tin	18

2.1.3.	Các phương pháp bảo vệ thông tin	20
2.2.	MẬT MÃ VÀ CÁC YÊU CẦU BẢO MẬT THÔNG TIN.....	21
2.3.	MÃ HÓA.....	22
2.3.1.	Khái niệm hệ mật mã.....	22
2.3.2.	Phân loại các hệ thống mật mã	23
2.3.3.	Hệ mã hóa khóa đối xứng.....	23
2.3.4.	Hệ mã hóa khóa công khai	24
2.4.	CHỮ KÝ SỐ	26
2.4.1.	Giới thiệu	26
2.4.2.	Yêu cầu chữ ký số	26
2.4.3.	Đặc điểm của chữ ký số.....	26
2.4.4.	Tồn tại của chữ ký số.....	27
2.4.5.	Phân loại chữ ký theo mức an toàn.....	27
2.4.6.	So sánh chữ ký thông thường và chữ ký số.....	27
2.5.	TẠO ĐẠI DIỆN TÀI LIỆU VÀ HÀM BĂM.....	28
2.5.1.	Một số vấn đề với chữ ký số.....	29
2.5.2.	Phương thức quyết các vấn đề.....	29
2.5.3.	Tổng quan về hàm băm	30
	KẾT LUẬN CHƯƠNG	31
CHƯƠNG 3. ỨNG DỤNG CHỮ KÝ SỐ DỰA TRÊN HỆ MẬT RSA VÀO HỆ THỐNG TIỀN ĐIỆN TỬ.....		33
3.1.....		33
3.1.	HỆ MẬT RSA.....	33
3.1.1.	Tìm hiểu RSA	33
3.1.2.	Thuật toán RSA	34
3.1.3.	Chuyển đổi văn bản rõ.....	36
3.1.4.	Vấn đề an toàn với hệ mật RSA	37
3.1.4.1.	An ninh.....	37

3.1.4.2. Các phương thức tấn công.....	39
3.1.4.3. Các vấn đề đặt ra trong thực tế.....	40
3.1.5. Một số tính chất của hệ RSA	41
3.1.6. Ứng dụng hệ mã RSA trong chữ ký số.....	42
3.1.7. Sơ đồ chữ kí RSA	43
3.2. CHỮ KÝ MÙ RSA	441
3.2.1. Khái niệm chữ ký mù	44
3.2.2. Sơ đồ chữ ký mù RSA	44
3.3. ỨNG DỤNG CHỮ KÝ MÙ RSA TRONG HỆ THỐNG TIỀN ĐIỆN TỬ.....	45
3.3.1. Đặt vấn đề.....	45
3.3.2. Giải pháp thực hiện.....	46
3.3.3. Lược đồ Chaum - Fiat - Naor	46
3.3.4. Phân tích – đánh giá.....	48
3.4. ỨNG DỤNG CHỮ KÝ MÙ RSA TRONG BÀI TOÁN THANH TOÁN PHÍ ĐƯỜNG BỘ.....	49
3.4.1 Khảo sát thực trạng thu phí đường bộ tại Việt Nam	49
3.4.2 Phát biểu bài toán	51
3.4.3 Giải pháp thực hiện.....	53
3.4.4 Cấu trúc chương trình.....	55
3.4.1. Một số kết quả đạt được	55
KẾT LUẬN CHƯƠNG	58
KẾT LUẬN.....	60
TÀI LIỆU THAM KHẢO.....	Error! Bookmark not defined.

DANH MỤC BẢNG BIỂU

Bảng 2.2	Khởi tạo các tham số	36
Bảng 3.1	Các file chính đề trong chương trình Demo	55

DANH MỤC HÌNH VẼ

Hình 1.1	Mô hình giao dịch cơ bản của hệ thống Tiền điện tử	9
Hình 1.2	Mô hình phương thức thanh toán	9
Hình 1.3	Mô hình giao dịch có tính chuyển nhượng	12
Hình 2.1	Quá trình mã hóa và giải mã.....	22
Hình 3.1	Sơ đồ biểu diễn thuật toán mã hóa RSA.....	35
Hình 3.2	Khái quát lược đồ Chaum – Fiat – Naor.....	46
Hình 3.3	Mô hình giao dịch cơ bản của hệ thống thanh toán phí giao thông đường bộ sử dụng tiền điện tử.....	52
Hình 3.4	Giao diện chương trình chính	56
Hình 3.5	Giao diện cài đặt hệ thống	56
Hình 3.6	Giao diện khách hàng tạo đồng tiền	57
Hình 3.7	Trạm thu phí xác thực và gửi lịch sử thanh toán	58

MỞ ĐẦU

1. Lý do lựa chọn đề tài

Tiền mặt là một công cụ tài chính rất phổ biến quen thuộc, đã từng được ví như là một trong số những phát minh vĩ đại của loài người, tuy nhiên tại các quốc gia phát triển như Mỹ, EU, tiền mặt đang đứng trước nguy cơ “tuyệt chủng”!

Khi xã hội phát triển đến một mức nhất định, việc lạm dụng sử dụng tiền mặt lại làm cản trở sự phát triển của nền kinh tế. Đơn cử như việc huy động và vận chuyển tiền không những mất thời gian và chi phí vận chuyển, mà còn tạo ra cả rủi ro an ninh. Thêm vào đó, khi thực hiện giao dịch bằng tiền mặt, giao dịch viên phải bỏ nhiều thời gian để đếm và kiểm tra tính pháp lý của số tiền được đưa vào thanh toán (tiền thật hay giả, còn giá trị sử dụng hay không). Mặc dù tổng khối lượng giao dịch vừa và nhỏ không nhiều nhưng do trị giá mỗi giao dịch là thấp nên khi xét về số lượng thì những giao dịch đó lại vượt trội so với các giao dịch phi tiền mặt. Trong khi đó trên thực tế, tại các quốc gia phát triển, việc sử dụng tiền mặt là rất hạn chế. Đây cũng là những con số nói lên được phần nào nhu cầu cấp thiết hạn chế tiền mặt trong lưu thông để kích thích sự phát triển của kinh tế [1].

Ở Việt Nam, theo báo cáo mới nhất của bộ Công Thương thì tới năm 2014, trên phạm vi toàn quốc đã triển khai được 10.051 máy ATM và phát hành 19,4 triệu thẻ thanh toán. Tính đến tháng 7 năm 2014, dân số Việt Nam gần 91 triệu, như vậy trung bình cứ 6 người sở hữu 1 thẻ thanh toán. Một xã hội thanh toán không dùng tiền mặt không còn là điều mới mẻ ở Việt Nam. Người dân có cơ hội tiếp cận với các hình thức thanh toán không dùng tiền mặt. Tuy vậy, các giao dịch không dùng tiền mặt chủ yếu vẫn là qua hệ thống thẻ phát hành bởi ngân hàng cổ phần. Các hình thức thanh toán không dùng tiền mặt khác vẫn còn chưa phổ biến. Động thái gần đây nhất ghi lại được, mới chỉ là việc ra mắt thẻ Flexicard do Tổng Công ty Xăng dầu Việt Nam (Petrolimex) và Ngân hàng TMCP Xăng dầu Petrolimex (PG Bank).

Trong khi tại Việt Nam, việc thanh toán vẫn dừng ở hình thức thẻ, thì hiện nay trên thế giới, thanh toán bằng điện thoại di động đã trở nên phổ biến, nhất là những quốc gia phát triển. Tại Nhật, chỉ với chiếc điện thoại di động, người dân có thể dùng để mua vé tàu điện ngầm, vé xe bus, thanh toán vé máy bay hay là trả tiền