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

LUẬN VĂN THẠC SỸ 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 SỸ 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 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 thày 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

DANH MỤC BẢNG BIỂU

DANH MỤC HÌNH VẼ

MỞ ĐẦU

1. Lý do lựa chọn đề tài

Tiền mặt là một công cụ tài chính rất đỗi 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