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

LÊ THU HƯƠNG

NGHIÊN CỨU VẤN ĐỀ XÁC THỰC GIAO DỊCH NGÂN HÀNG TRỰC TUYẾN SỬ DỤNG MẬT KHẨU DẠNG OTP

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, 2016

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

LÊ THU HƯƠNG

NGHIÊN CỨU VẤN ĐỀ XÁC THỰC GIAO DỊCH NGÂN HÀNG TRỰC TUYẾN SỬ DỤNG MẬT KHẨU DẠNG OTP

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: TS. VŨ VINH QUANG

THÁI NGUYÊN, 2016

LỜI CAM ĐOAN

Sau quá trình học tập tại **Trường Đại học công nghệ thông tin & truyền thông**, với những kiến thức lý thuyết và thực hành đã tích lũy được, với việc vận dụng các kiến thức vào thực tế, em đã tự nghiên cứu các tài liệu, các công trình nghiên cứu, đồng thời có sự phân tích, tổng hợp, đúc kết và phát triển để hoàn thành luận văn thạc sĩ của mình.

Em xin cam đoan luận văn này là công trình do bản thân em tự tìm hiểu, nghiên cứu và hoàn thành dưới sự hướng dẫn của thầy giáo **TS. Vũ Vinh Quang**.

Thái Nguyên, tháng 12 năm 2016

Học viên

Lê Thu Hương

LỜI CẢM ƠN

Trong thời gian hai năm của chương trình đào tạo thạc sỹ, trong đó gần một nửa thời gian dành cho các môn học, thời gian còn lại dành cho việc lựa chọn đề tài, giáo viên hướng dẫn, tập trung vào nghiên cứu, viết, chỉnh sửa và hoàn thiện luận văn. Với quỹ thời gian như vậy và với vị trí công việc đang phải đảm nhận, không riêng bản thân em mà hầu hết các sinh viên cao học muốn hoàn thành tốt luận văn của mình trước hết đều phải có sự sắp xếp thời gian hợp lý, có sự tập trung học tập và nghiên cứu với tinh thần nghiêm túc, nỗ lực hết mình; tiếp đến cần có sự ủng hộ về tinh thần, sự giúp đỡ về chuyên môn một trong những điều kiện không thể thiếu quyết định đến việc thành công của luận văn.

Để hoàn thành được luận văn này trước tiên em xin gửi lời cảm ơn đến thầy giáo hướng dẫn **TS. Vũ Vinh Quang**, người đã có những định hướng cho em về nội dung và hướng phát triển của đề tài, người đã có những đóng góp quý báu cho em về những vấn đề chuyên môn của luận văn, giúp em tháo gỡ kịp thời những vướng mắc trong quá trình làm luận văn.

Em cũng xin cám ơn các thầy cô giáo Trường Đại học Công nghệ thông tin và Truyền thông đã có những ý kiến đóng góp bổ sung cho đề tài luận văn của em.

Em xin hứa sẽ cố gắng hơn nữa, tự trau dồi bản thân, tích cực nâng cao năng lực chuyên môn của mình để sau khi hoàn thành luận văn này sẽ có hướng tập trung nghiên cứu sâu hơn, không ngừng hoàn thiện hơn nữa luận văn của mình để có những ứng dụng thực tiễn cao trong thực tế.

Thái Nguyên, tháng 12 năm 2016

Học viên

Lê Thu Hương

MỤC LỤC

DANH MỤC CÁC CHỮ VIẾT TẮT

OTP	One Time Password
DES	Data Encrypt Standar
RSA	R.Rivest A.Shamir L.Adleman
MHK	Merkle -Hellman Knapsack
SHA	Secure Hash Algorithm

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Trong kĩ thuật bảo mật thông tin, mật khẩu (password) được sử dụng rộng rãi trong quá trình đăng nhập (log-on) để xác thực người dùng khi truy nhập vào các hệ thống máy tính và mạng, các phần mềm ứng dụng trên máy tính cá nhân, máy chủ công ty và cả website của các tổ chức tài chính, ngân hàng. Phương pháp phổ thông thường hay dùng nhất để xác thực người dùng chỉ là mật khẩu (tên đăng nhập username - password). Tuy nhiên, hầu hết các chuyên gia bảo mật đều đánh giá là việc sử dụng password không còn an toàn trước các thủ đoạn tấn công tinh vi hiện nay. Mật khẩu có thể bị nghe lén, bị đánh cắp, hoặc bị phá mã. Một trong những hướng nghiên cứu để tăng cường độ an toàn của hệ thống là mật khẩu sử dụng một lần *OTP (One Time Password).* Đây là phương pháp được giới thiệu để tăng cường độ an toàn trong quá trình xác thực người dùng, xác thực các giao dịch, đặc biệt là các giao dịch thanh toán trực tuyến trong các hệ thống ngân hàng đang được sử dụng phổ biến hiện nay.

Đề tài "*Nghiên cứu vấn đề xác thực giao dịch ngân hàng trực tuyến sử dụng mật khẩu dạng OTP"* được lựa chọn với mục đích nghiên cứu sâu về mật khẩu sử dụng một lần, các phương pháp sinh và tạo mật khẩu sử dụng một lần và ứng dụng trong việc xác thực các giao dịch ngân hàng, cài đặt thử nghiệm ứng dụng mật khẩu sử dụng một lần để nâng cao an toàn cho xác thực các giao dịch ngân hàng trực tuyến. **Mục đích của luận văn**

Tìm hiểu nghiên cứu sâu về mật khẩu sử dụng một lần, các phương pháp sinh và tạo mật khẩu sử dụng một lần và ứng dụng trong xác thực giao dịch ngân hàng trực tuyến.

Đối tượng và phạm vi nghiên cứu

Luận văn tìm hiểu nghiên cứu về lý thuyết mật mã, các thuật toán mã hóa cơ bản, lý thuyết về hàm băm và thuật toán mã hóa SHA-1, lý thuyết về OTP và vấn đề xác thực các giao dịch ngân hàng trực tuyến. Xây dựng hệ thống xác thực các giao dịch ngân hàng bằng mật khẩu sử dụng 1 lần OTP trên ngôn ngữ Java.

Cấu trúc của luận văn gồm có

Phần mở đầu: Nêu lý do chọn đề tài và hướng nghiên cứu chính

Chương 1: Các kiến thức cơ bản về lý thuyết bảo mật thông tin, một số thuật toán mã hóa cơ bản, khái niệm về mật khẩu và ứng dụng.

Chương 2: Giới thiệu tổng quan về mật khẩu OTP, các ứng dụng cơ bản, các phương pháp sinh mật khẩu OTP, các phương pháp chuyển giao

Chương 3: Xây dựng chương trình ứng dụng xác thực trong giao dịch trực tuyến tại các ngân hàng Việt Nam dựa trên mật khẩu OTP