

**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 cảm 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

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	ii
MỤC LỤC .....	iii
DANH MỤC CÁC CHỮ VIẾT TẮT .....	vi
DANH MỤC HÌNH VẼ.....	vii
<b>MỞ ĐẦU .....</b>	<b>1</b>
<b>Chương 1. MỘT SỐ KIẾN THỨC CƠ BẢN VỀ BẢO MẬT THÔNG TIN.....</b>	<b>3</b>
1.1. Giới thiệu về an toàn và bảo mật thông tin .....	3
1.1.1. Các khái niệm cơ bản .....	3
1.1.2. Mục tiêu của an toàn bảo mật thông tin .....	3
1.1.3. Các chiến lược an toàn hệ thống .....	4
1.1.4. An toàn thông tin bằng mật mã .....	5
1.2. Một số hệ mã hóa thông dụng .....	8
1.2.1. Hệ mã RSA .....	8
1.2.2. Hệ mã Rabin.....	9
1.2.3. Hệ mã Elgamal.....	10
1.2.4. Hệ mã MHK (Merkle -Hellman Knapsack).....	11
1.2.5. Hệ mật mã Rabin.....	12
1.2.6. Hệ mật mã McEliece .....	13
1.3. Giới thiệu về mật khẩu .....	15
1.3.1. Định nghĩa .....	15
1.3.2. Phương pháp xác thực .....	16
1.3.3. Độ an toàn .....	17
<b>Chương 2. MỘT SỐ KHÁI NIỆM VỀ OTP CÁC PHƯƠNG PHÁP .....</b>	<b>26</b>
2.1. Giới thiệu về OTP .....	26
2.1.1. Định nghĩa về OTP.....	26
2.1.2. Ưu điểm.....	26
2.1.3. Nhược điểm.....	27
2.2. Ứng dụng của OTP .....	27
2.2.1. Ứng dụng trong xác thực.....	27
2.2.2. Ứng dụng trong đăng nhập.....	28

2.3. Giới thiệu về hàm băm mật mã, các thuật toán .....	29
2.3.1. Giới thiệu.....	29
2.3.2. Cấu trúc, vai trò của hàm băm mật mã .....	29
2.3.3. Một số hàm băm mật mã thông dụng.....	36
2.3.4. Các ứng dụng cơ bản của hàm băm .....	37
2.4. Một số phương pháp sinh OTP .....	41
2.4.1. Phương pháp sinh theo thời gian.....	41
2.4.2. Phương pháp sinh theo thuật toán .....	42
2.4.3. Phương pháp sinh theo giải pháp S/KEY .....	44
2.4.4. Phương pháp sinh sử dụng HOTP.....	44
2.4.5. Phương pháp sinh sử dụng Security token.....	44
2.4.6. Phương pháp sinh bằng giao thức .....	44
2.5. Các phương pháp chuyển giao OTP .....	45
2.5.1. Chuyển giao OTP bằng giấy .....	45
2.5.2. Chuyển giao OTP bằng tin nhắn SMS .....	46
2.5.3. Tạo OTP sử dụng token .....	47
2.5.4. Tạo OTP sử dụng điện thoại di động .....	49
2.5.5. Chuyển giao OTP sử dụng gmail .....	51
<b>Chương 3. XÂY DỰNG CHƯƠNG TRÌNH ỨNG DỤNG XÁC THỰC SỬ</b>	
<b>DỤNG OTP TRONG GIAO DỊCH NGÂN HÀNG TRỰC TUYẾN .....</b>	<b>53</b>
3.1 Đặt vấn đề .....	53
3.2 Mô hình sử dụng giao dịch trực tuyến của ngân hàng Eximbank.....	54
3.2.1. Giới thiệu Mobile OTP .....	55
3.2.1. Hướng dẫn sử dụng Mobile OTP.....	56
3.3. Kết quả xây dựng mô hình thực nghiệm .....	56
3.4. Cài đặt .....	56
3.5. Kết chương.....	56
<b>KẾT LUẬN .....</b>	<b>57</b>
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>58</b>
<b>PHỤ LỤC .....</b>	<b>59</b>

**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

Hình 1:	Mã hoá với khoá mã và khoá giải giống nhau.....	6
Hình 2:	Minh họa xác thực mật khẩu .....	15
Hình 3:	Minh họa đăng nhập một lần .....	16
Hình 4:	Mô hình đăng nhập duy nhất SSO.....	26
Hình 5:	Cơ chế hoạt động của openSSO .....	30
Hình 6:	Người dùng truy cập vào ứng dụng khi.....	32
Hình 7:	Người dùng truy cập ứng dụng mà chưa .....	32
Hình 8:	Sơ đồ phân loại hàm băm .....	34
Hình 9:	Cấu trúc tổng quát của hàm băm .....	35
Hình 10:	Mô hình sinh mã OTP theo thời gian .....	39
Hình 11:	Thiết bị sinh OTP - OTP Token .....	40
Hình 12:	Ứng dụng Mobile OTP - IOS .....	40
Hình 13:	Ứng dụng Mobile OTP - Window Phone 8.....	42
Hình 14:	Mô hình xác thực người dùng dựa trên giao thức .....	44
Hình 15:	Thẻ mật khẩu OTP với mật khẩu in sẵn của VinaGame .....	45
Hình 16:	Chuyển giao OTP bằng tin nhắn SMS .....	46
Hình 17:	Minh họa thẻ EMV .....	48
Hình 18:	Minh họa thiết bị E-Token .....	49
Hình 19:	Mô hình kết nối SSL VPN đến Vigor2950 có điện thoại.....	49
Hình 20:	Cài đặt phần mềm sinh OTP trên iPhone với Vigor2950.....	51
Hình 21:	Mô hình nhận OTP qua gmail .....	53
Hình 22:	Hướng dẫn cài đặt ứng dụng Mobile OTP .....	54
Hình 23:	Hướng dẫn đăng nhập và kích hoạt dịch vụ .....	54
Hình 24:	Hướng dẫn sử dụng Mobile OTP để xác thực giao dịch .....	55
Hình 25:	Hướng dẫn chức năng đồng bộ OTP .....	55
Hình 26:	Hướng dẫn cấp lại mật khẩu.....	56
Hình 27:	Hướng dẫn đổi mật khẩu .....	56
Hình 28:	Người dùng đăng nhập vào hệ thống.....	56
Hình 29:	Người dùng nhập thông tin chuyển khoản .....	56
Hình 30:	Người dùng chấp nhận chuyển khoản .....	56
Hình 31:	Người dùng chuyển khoản thành công.....	56
Hình 32:	Mô tả lịch sử giao dịch .....	56



## MỞ ĐẦU

Trong kỹ 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