**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 Tiến, 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**

# DANH MỤC HÌNH VẼ

**Trang**

# DANH MỤC BẢNG BIỂU

**Trang**

# 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#.