ĐẠI HỌC THÁI NGUYÊN
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

VŨ QUỐC THỊNH

TÌM HIỂU MỘT SỐ PHƯƠNG PHÁP THÁM MÃ HỆ MẬT MÃ KHÓA CÔNG KHAI ỨNG DỤNG TRONG BẢO MẬT DỮ LIỆU

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - NĂM 2014

ĐẠI HỌC THÁI NGUYÊN
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

VŨ QUỐC THỊNH

TÌM HIỂU MỘT SỐ PHƯƠNG PHÁP THÁM MÃ HỆ MẬT MÃ KHÓA CÔNG KHAI ỨNG DỤNG TRONG BẢO MẬT DỮ LIỆU

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số: 60.48.01

Người hướng dẫn khoa học: TS. NGUYỄN DUY MINH

Thái Nguyên, 2014

LỜI CẢM ƠN

Lời đầu tiên, em xin được gửi lời cảm ơn sâu sắc đến TS.Nguyễn Duy Minh, người thầy đã giúp đỡ em trong suốt quá trình làm khóa luận, đồng thời cũng là người thầy đã hướng dẫn em những bước đi đầu tiên để khám phá một lĩnh vực đầy bí ẩn và thách thức – lĩnh vực an toàn và bảo mật dữ liệu.

Em xin được cảm ơn các thầy, các cô đã giảng dạy em trong suốt quá trình học tập. Những kiến thức mà các thầy các cô đã dạy sẽ mãi là hành trang giúp em vững bước trong tương lai.

Em cũng xin được gửi lời cảm ơn đến tập thể lớp CK11G, một tập thể lớp đoàn kết với những người bạn không chỉ học giỏi mà còn luôn nhiệt tình, những người bạn đã giúp đỡ em trong suốt quá trình học tập.

Cuối cùng em xin được gửi lời cảm ơn sâu sắc tới gia đình em, những người luôn kịp thời động viên, khích lệ em, giúp đỡ em vượt qua những khó khăn trong cuộc sống.

Thái Nguyên, tháng 08 năm 2014

Học viên

Vũ Quốc Thịnh

ĐỊNH NGHĨA, VIẾT TẮT

Advanced Encryption Standard (AES)	Tiêu chuẩn tiên tiến
Asymmetric key cryptography	Mã hóa bất đối xứng
Authentication	Tính xác thực
Cipher text	Bản mã
Concatenate frequency of pairs	Tần số bộ đôi móc xích
Confidentiality	Tính bảo mật
Cryptannalysis	Thám mã
Cryptography	Mật mã
Cryptology	Mật mã học
Data Encryption Standard (DES)	Tiêu chuẩn mã hóa dữ liệu
Decryption	Giải mã
Encryption	Mã hóa
Frequency	Tấn số
Integrity	Tính toàn vẹn
Key seed	Mầm khóa
Most Likelihood Ratio (MLR)	Tỷ số hợp lý cực đại
Non – repudation	Tính không thể chối bỏ
Plain text	Bản rõ
Private key	Khóa bí mật
Public key	Khóa công khai
Relative frequency	Tần số tương đối
Rivest, Shamir, & Adleman (RSA)	
Symmetric - key cryptography	Mã hóa đối xứng

MỤC LỤC

DANH MỤC HÌNH VẼ

LỜI NÓI ĐẦU

Từ khi con người có nhu cầu trao đổi thông tin, thư từ với nhau thì nhu cầu giữ bí mật và bảo mật tính riêng tư của những thông tin, thư từ đó cũng nảy sinh. Hình thức thông tin trao đổi phổ biến sớm nhất là dưới dạng các văn bản, để giữ bí mật của thông tin người ta đã sớm nghĩ đến cách che dấu nội dung các văn bản bằng các biến dạng các văn bản đó để người ngoài đọc nhưng không hiểu được, đồng thời có cách khôi phục lại nguyên dạng ban đầu để người trong cuộc vẫn hiểu được; theo cách gọi ngày nay thì dạng biến đổi của văn bản được gọi là mật mã của văn bản, cách lập mã cho một văn bản được gọi là phép lập mã, còn cách khôi phục lại nguyên dạng ban đầu gọi là phép giải mã. Phép lập mã và phép giải mã được thực hiện nhờ một chìa khóa riêng nào đó mà chỉ những người trong cuộc được biết và nó được gọi là khóa lập mã. Người ngoài dù có lấy được bản mật mã trên đường truyền mà không có khóa mật mã thì cũng không thể hiểu được nội dung của văn bản truyền đi.

Trong số các phương pháp đảm bảo an toàn thông tin thì phương pháp mật mã hóa (Cryptography) được sử dụng rộng rãi và đảm bảo an toàn nhất. Tuy nhiên phương pháp mật mã hóa không tốt (mặc dù việc quản lý khóa mã được giả thiết là an toàn) thì rất nguy hiểm. Vậy làm thế nào để đánh giá được chất lượng của một hệ mã là tốt? Có nhiều phương pháp đánh giá chất lượng của một hệ mật như phương pháp Entropy của Shannon, nhưng phương pháp tốt nhất và trực quan nhất, đó là phương pháp phân tích trực tiếp bản mã khi không có khóa mã trong tay mà người ta thường gọi là thám mã (Cryptannalysis).

Hiện nay thám mã cũng là một lĩnh vực cũng thường được quan tâm nghiên cứu nhưng ít khi được công khai, hoặc công khai không đầy đủ. Sự hiểu biết về các phương pháp thám mã hiện nay ở trong nước nói chung đang còn rất hạn chế. Tuy đã có nhiều công trình nghiên cứu về thám mã nhưng việc đưa ra hệ quy trình thám mã và chương trình thám mã vẫn ở mức độ hẹp và khó khăn trong ứng dụng thực tế.

Xuất phát từ thực tế đó, để góp phần tăng cường độ an toàn cho các hệ mật mã hiện đại nhằm góp phần bảo vệ an ninh thông tin trong tình hình mới nên em đã chọn đề tài ***"Tìm hiểu một số phương pháp thám mã hệ mật mã khóa công khai ứng dụng trong bảo mật dữ liệu"*** nhằm nghiên cứu và ứng dụng.

Trong khuôn khổ đề tài được giao, luận văn được trình bày trong 3 chương. Có phần mở đầu, phần kết luận, phần mục lục, tài liệu tham khảo. Các nội dung cơ bản của luận văn được trình bày như sau:

Chương 1: ***"Tổng quan về mật mã khóa công khai và thám mã"***. Ở chương này, luận văn trình bày chi tiết về lịch sử cũng như các khái niệm về các hệ mã thuộc dòng mã truyền thống cũng như dòng mã đối xứng, mã bất đối xứng giúp chúng ta hiểu cơ sở lý thuyết về các hệ mật mã. Vấn đề thám mã nói chung và thám mã đối với hệ mật RSA cũng được em trình bày kỹ trong chương này.

Chương 2: **"Các phương pháp thám mã hệ mật mã khóa công khai"**. Trên cơ sở hiểu các hệ mật được trình bày ở chương 1, để có cái nhìn tổng quan về vấn đề thám mã đối với hệ mật RSA và trên cơ sở trình bày các phương pháp thám mã đã tổng kết lại các phương pháp và đánh giá kết quả của phương pháp như: các tấn công cơ bản - modul chung, tấn công vào số mũ công khai hoặc số mũ bí mật nhỏ, giao thức công chứng...

Chương 3: **"Thử nghiệm phương pháp thám mã với hệ RSA"**. Qua nghiên cứu các phương pháp thám mã trong chương 2, chương 3 đề xuất phương pháp tấn công giao thức sử dụng hệ mật mã RSA có modul n chung. Để minh chứng cho phương pháp này, luận văn xây dựng thuật toán và cài đặt chương trình thử nghiệm trong hệ bảo mật.

Do mức độ phức tạp của công việc thám mã là rất lớn nên bài toán đặt ra với giả thiết người thám mã biết được các thông tin và bản mã được mã hóa bởi RSA từ bản rõ tương ứng là một thông điệp dạng Text. Từ giả thiết này xây dựng thuật toán để xác định khóa mật K đã sử dụng để mã hóa cũng như tìm ra bản rõ tương ứng.