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

ĐINH THỊ HẢI YẾN

TÌM HIỂU KHẢ NĂNG AN TOÀN CỦA HỆ MẬT MÃ RSA

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, 2017

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

ĐINH THỊ HẢI YẾN

TÌM HIỂU KHẢ NĂNG AN TOÀN CỦA HỆ MẬT MÃ RSA

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. HỒ VĂN CANH

THÁI NGUYÊN, 2017

LỜI CAM ĐOAN

Tôi xin cam đoan kết quả nghiên cứu trong luận văn là sản phẩm của riêng cá nhân tôi, không sao chép lại của người khác. Trong toàn bộ nội dung của luận văn, những điều đã trình bày là của cá nhân tôi hoặc là được tôi tổng hợp từ nhiều nguồn tài liệu. Tất cả các nguồn tài liệu tham khảo có xuất xứ rõ ràng và được trích dẫn hợp pháp.

Tôi xin chịu toàn bộ trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đoan của tôi.

Thái Nguyên, tháng 6 năm 2017

Đinh Thị Hải Yến

LỜI CÁM ƠN

Để hoàn thành luận văn "Tìm khả năng an toàn của hệ mật mã RSA" em đã nhận được sự hướng dẫn và giúp đỡ nhiệt tình của nhiều tập thể và cá nhân.

Trước hết, em xin bày tỏ lòng biết ơn chân thành đến ban lãnh đạo cùng quý thầy cô trong khoa Công nghệ thông tin – Trường Đại học Công nghệ và truyền thông, Đại học Thái Nguyên đã tạo tình dạy dỗ, truyền đạt kiến thức, kinh nghiệm và tạo điều kiện thuận lợi cho em trong suốt thời gian học tập và thực hiện đề tài.

Đặc biệt, em xin bày tỏ lòng biết ơn sâu sắc đến thầy hướng dẫn TS. Hồ Văn Canh, người đã gợi cho em những ý tưởng về đề tài, đã tận tình hướng dẫn và giúp đỡ để đề tài được thực hiện và hoàn thành.

Xin chân trọng gửi đến gia đình, bạn bè và người thân những tình cảm tốt đẹp nhất đã giúp đỡ động viên trong suốt khóa học và hoàn thành luận văn.

Thái Nguyên, tháng 6 năm 2017

Tác giả

Đinh Thị Hải Yến

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CÁM ƠN ii
MỤC LỤC iii
DANH MỤC HÌNH vi
DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT vii
MỞ ĐẦU 1
1. Lý do chọn đề tài 1
2. Những đóng góp của luận văn 1
3. Bố cục của luận văn 1
Chương 3. Các phương pháp tấn công vào hệ mã hóa RSA 2
NỘI DUNG 3
CHƯƠNG 1. TỔNG QUAN VỀ LÝ THUYẾT MẬT MÃ 3
1.1. CÁC KHÁI NIỆM CƠ BẢN 3
1.2. PHÂN LOẠI CÁC HỆ MẬT MÃ 4
1.2.1. Mã hoá đối xứng 5
1.2.2. Mã hoá bất đối xứng 5
1.3. MỘT SỐ KHÁI NIỆM TOÁN HỌC 5
1.3.1. Ước chung lớn nhất 5
1.3.2. Số nguyên tố và số nguyên tố cùng nhau 5
1.4. ĐỒNG DƯ THỨC 6
1.4.1. Định nghĩa đồng dư thức 6
1.4.2. Tính chất đồng dư thức 6
1.5. KHÔNG GIAN Z_n VÀ Z_n^* 7
1.5.1. Không gian Z_n 7
1.5.2. Không gian Z_n^* 7
1.6. PHẦN TỬ NGHỊCH ĐẢO 7
1.6.1. Định nghĩa 7
1.6.2. Tính chất 7

1.7. KHÁI NIỆM NHÓM, NHÓM CON VÀ NHÓM CYCLIC 8
1.7.1. Khái niệm nhóm 8
1.7.2. Khái niệm nhóm con 8
1.7.3. Khái niệm nhóm Cyclic 8
1.8. HÀM PHI EULER Φ(n) 8
1.8.1. Định nghĩa 8
1.8.2. Tính chất 8
1.9.3. Định lý Euler 9
1.9. CÁC PHÉP TOÁN CƠ BẢN TRONG MODULO 9
1.9.1. Thuật toán Euclid 9
1.9.2. Thuật toán Euclid mở rộng 11
1.9.3. Định lý đồng dư Trung Hoa 13
1.10. HÀM MỘT PHÍA VÀ HÀM MỘT PHÍA CÓ CỬA SẬP 14
1.10.1. Hàm một phía 14
1.10.2. Hàm một phía có cửa sập 15
1.11. ĐỘ PHỨC TẠP TÍNH TOÁN 15
1.11.1. Độ phức tạp tính toán 15
1.11.2. Các lớp độ phức tạp 16
CHƯƠNG 2. TỔNG QUAN VỀ HỆ MÃ HÓA KHÓA CÔNG KHAI RSA 18
2.1. MÃ HÓA KHÓA CÔNG KHAI 18
2.2. MÃ HÓA KHÓA CÔNG KHAI RSA 18
2.2.1. Định nghĩa hệ mã hóa RSA 18
2.2.2. Định lý (The Correctness of RSA) 20
2.2.3. Một số nhận xét 22
2.3. CÁC VẤN ĐỀ AN TOÀN HỆ MÃ HÓA RSA 25
2.4. CÁC BÀI TOÁN LIÊN QUAN TỚI HỆ MÃ HÓA RSA 26
2.4.1. Bài toán phân tích số nguyên thành tích các thừa số nguyên tố 27
2.4.2. Bài toán tìm căn bậc hai module n 29
CHƯƠNG 3. CÁC PHƯƠNG PHÁP TẤN CÔNG VÀO HỆ MÃ HÓA RSA 31

3.1. PHÂN TÍCH NHÂN TỬ SỐ NGUYÊN LỚN 31
3.1.1. Mệnh đề 1.....31
3.1.2. Mệnh đề 2.....31
3.1.3. Mệnh đề 3.....32
3.2. TẤN CÔNG DỰA TRÊN VIỆC PHÂN TÍCH SỐ NGUYÊN n THÀNH TÍCH THỪA SỐ NGUYÊN TỐ.....34
3.2.1. Phương pháp phân tích n thành tích thừa số nguyên tố của Fermat (Fermat Factoring Attack).....34
3.2.2. Phương pháp phân tích $\boldsymbol{p \pm 1}$ và đường cong Elliptic 35
3.2.3. Phương pháp phân tích tổng quát.....37
3.2.4. Phương pháp sàng toàn phương – QS (Quadratic Sieve) 38
3.2.5. Phương pháp sành trường số tổng quát – GNFS (General Number Field Sieve).....40
3.3. TẤN CÔNG DỰA TRÊN SỐ MŨ CÔNG KHAI BÉ.....41
3.4. TẤN CÔNG DỰA TRÊN SỐ MŨ RIÊNG BÉ.....43
3.5. CÀI ĐẶT MỘT SỐ THUẬT TOÁN.....45
3.5.1. Cơ sở toán học.....45
3.5.2. Xây dựng thuật toán demo 49
3.5.3. Giao diện của chương trình.....56
KẾT LUẬN.....58
TÀI LIỆU THAM KHẢO.....59

DANH MỤC HÌNH

Hình 1.1 Lược đồ Mã hóa và giải mã thông tin 3
Hình 2.1 Sơ đồ mã hóa khóa công khai 18
Hình 2.2 Sơ đồ thuật toán mã hóa RSA 19
Hình 2.3 Sơ đồ thuật toán RSA 20
Hình 2.4 Sơ đồ chữ ký số RSA 24

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Ký hiệu	Tiếng anh	Tiếng việt
N hoặc Z^+	Set of natural numbers or positive integers N = Z^+={1,2,3,…}	Tập hợp các số tự nhiên N hoặc các số nguyên dương Z^+
Q	Set of rational numbers: $Q = \left\{\frac{a}{b}, a, b \in Z \text{ and } b \neq 0\right\}$	Tập hợp các phân số: $Q = \left\{\frac{a}{b}, a, b \in Z \text{ và } b \neq 0\right\}$
Z_n hoặc $\frac{Z}{nZ}$	Residue classes modulo n: $Z_n = \frac{Z}{nZ} = \{0,1,2,\dots,n-1\}$	
Z_n^*	Multiplicative group: $Z_n^* = \{a \in Z_n, \gcd(a,n) = 1\}$	
kP	$kP = P \oplus P \oplus \dots \oplus P$, where P is a point (x,y) on an elliptic curve E: $y^2 = x^3 + ax + b$	$kP = P \oplus P \oplus \dots \oplus P$, trong đó P là một điểm có tọa độ (x,y) trên đường cong Elliptic E: $y^2 = x^3 + ax + b$
O_E	Point at infinity on an elliptic curve E	O là điểm tại vô cực trên đường cong Elliptic E
gcd(a,b)	Greatest common divisor of (a,b)	
lcm(a,b)	Least common multiple of (a,b)	
$\lfloor x \rfloor or [x]$	Greatest integer less than or equal to x	Lấy cận trên của x
$\lceil x \rceil$	Least integer greater than or equal to x	Lấy cận dưới của x
$(\frac{a}{n})$	Jacobi symbol, where n is composit	Ký hiệu Jacobi
J_n	$J_n = \{a \in Z_n^* : \left(\frac{a}{n}\right) = 1\}$	
ECM	Elliptic Curve Method (for factoring)	Đường cong elliptic

LLL	Lenstra- Lenstra-Lovasz lattice reducation algorithm	Giải thuật Lenstra- Lenstra-Lovaszlattice
P	Class of problems solvable in polynomial –time by a deterministic Turing machine	
$A \overset{P}{\Leftrightarrow} B$	A and B are deterministic polynomial-time equivalent	