

Nghiên cứu hệ mật mã khoá công khai trong giao dịch điện tử : Luận văn ThS / Nguyễn Thị Tuyết Minh ; Nghd. : GS.TS. Nguyễn Đình Thông . - H. : ĐHCN, 2006 . - 80 tr. + CD-ROM

Tóm tắt: Nghiên cứu cơ sở lý thuyết của việc đảm bảo an ninh dữ liệu trong các giao dịch trên mạng bao gồm cả hai vấn đề cơ bản: bảo mật dữ liệu và xác thực dữ liệu (xác minh người gửi và xác minh tính nguyên vẹn, không bị can thiệp trái phép trong khi truyền) thông qua các hệ mã hoá như: khoá công khai, RSA, chữ ký số, mã xác thực bản tin...Đồng thời đề cập đến các phương pháp tiêu biểu nhằm phá vỡ hệ thống an ninh dữ liệu tạo bởi các hệ mã. Đưa ra nhận xét, đánh giá, phân tích mật mã khoá công khai trong các giao dịch điện tử và xây dựng chương trình mô phỏng một số hệ mã RSA, MD5, SHA - 1..

Mở đầu	3
1.2 Quy trình giao dịch điện tử	8
1.3 Những kiến thức toán học nền tảng	14
1.3.1 Xác suất	14
1.3.2 Số học.....	15
1.3.2 Các định lý áp dụng cho phép toán chia lấy phần dư (mod).....	16
Chương 2: Các hàm băm	24
2.1 Các ký hiệu chung	24
2.2 Các định nghĩa, khái niệm và tính chất căn bản	24

2.2.1 Định nghĩa.....	25
2.2.2 Các tính chất căn bản.....	26
2.3 Phương pháp xây dựng các hàm băm.....	26
2.3.1 Hàm nén.....	26
2.3.2 Bộ mở rộng miền.....	27
2.4 Các hàm băm cơ bản.....	27
2.4.1 MD5.....	28
2.4.2 SHA-1.....	30
2.5 Hàm băm có khoá.....	31
2.6 Tấn công các hàm băm.....	32
2.6.1 Dạng tấn công căn bản.....	33
2.6.1.1 Tấn công không gian khoá của MAC.....	33
2.6.1.2 Tấn công kích thước bit trên MAC.....	34
2.6.1.3 Tấn công tính toán trước.....	34
2.6.1.4 Tấn công các mục tiêu song song trên OWHFs.....	34
2.6.1.5 Tấn công bản tin dài dành cho tiền ảnh thứ 2.....	34
2.6.1.6 Tấn công từng bit trên MDC.....	35
2.6.2 Tấn công ngày sinh nhật.....	36
Chương 3: Hệ mật mã khoá công khai.....	41
3.1 Hệ mật mã khoá công khai RSA.....	42
3.2 Các thuật toán phân tích thừa số.....	48
3.2.1 Một số phương pháp truyền thống.....	48
3.2.2 Một số phương pháp hiện đại.....	52
Chương 4: Các sơ đồ chữ ký số, sơ đồ định danh.....	.59

4.1 Sơ đồ chữ ký số.....	59
4.1.1 Sơ đồ chữ ký số có phụ lục.....	61
4.1.2 Sơ đồ chữ ký số khôi phục bản tin.....	62
4.1.3 Sơ đồ chữ ký RSA.....	64
4.1.3.1 Định nghĩa và giải thuật.....	64
4.1.3.2 Tiêu chuẩn mật mã khoá công khai sử dụng sơ đồ chữ ký RSA.....	66
4.1.4 Sơ đồ chữ ký Elgama.....	70
4.1.5 Chuẩn chữ ký số.....	72
4.1.6 Sơ đồ chữ ký Schnorr.....	73
4.2 Sơ đồ định danh.....	74
4.3 ứng dụng hệ mật mã RSA cho bài toán GDĐT.....	78
Kết luận	82
Phụ lục A: Các thuật ngữ viết tắt.....	83
Phụ lục B: Các thuật ngữ tiếng anh dịch sang tiếng việt	.84
Tài liệu tham khảo.....	.87