



Mục lục

Chương 1. Tổng quan về an toàn dữ liệu	11
1.1 Sơ lược lịch sử về khoa học mật mã	11
1.2 Sự cần thiết phải đảm bảo an toàn dữ liệu	14
1.2.1 Những nguy cơ tiềm ẩn mất an toàn dữ liệu	14
1.2.2 Các bài toán về an toàn dữ liệu	15
1.3 Mật mã và tính an toàn của các hệ mã	16
1.3.1 Một số thuật ngữ	16
1.3.2 Định nghĩa hệ mật mã	16
1.3.3 Những yêu cầu đối với hệ mật mã	17
1.3.4 Phân loại phương pháp mã hóa	17
1.3.5 Thám mã và tính an toàn của hệ mật mã	18
1.4 Cơ sở toán học	20
1.4.1 Số nguyên tố	20
1.4.2 Phần tử nghịch đảo	22
1.4.3 Phương trình đồng dư tuyến tính	24
1.4.4 Định lý số dư Trung hoa	25
1.4.5 Bài toán Logarit rời rạc	25
1.4.6 Phân tích thành thừa số nguyên tố	26
1.4.7 Thuật toán tính $y = x^k \bmod N$	27

1.4.8	Bài toán về tổng các tập con	27
1.4.9	Hàm một phía và hàm cửa sập một phía	28
1.5	Câu hỏi, bài tập và thực hành	29

Chương 2. Các hệ mã hóa dữ liệu 31

2.1	Nguyên tắc chung của các hệ mã hóa	31
2.2	Các hệ mã hóa khóa cổ điển	32
2.2.1	Mã dịch vòng	32
2.2.2	Mã thay thế	33
2.2.3	Mã Affine	34
2.2.4	Mã Vigenère	34
2.2.5	Mã Hill	35
2.2.6	Mã hoán vị	36
2.2.7	Mã Playfair	37
2.2.8	Mã Rail Fence	38
2.3	Các hệ mã hóa khóa hiện đại	38
2.3.1	Mã DES-Data Encryption System	38
2.3.2	Mã AES-Advanced Encryption Standard	47
2.4	Hệ mã khoá công khai	53
2.4.1	Hệ mã hóa RSA	54
2.4.2	Hệ mã hóa Rabin	58
2.4.3	Hệ mã hóa Elgamal	59
2.4.4	Hệ mã hóa Merkle-Hellman	60
2.4.5	Hệ mã hóa McEliece	61
2.4.6	Hệ mã hóa trên đường cong Elliptic	63
2.4.7	Một mã hạng nhẹ (<i>Lightweight Cryptography</i>)	66
2.5	Câu hỏi, bài tập và thực hành	67

Chương 3. An toàn trong giao dịch điện tử 71

3.1	Hàm băm	71
3.1.1	Hàm băm Chaum-van Heijst-Pfitzmann	73
3.1.2	Hàm băm MD5	73
3.1.3	Hàm băm SHA-1	74
3.1.4	Phân tích, đánh giá hàm băm MD5 và SHA-1	76
3.2	Chữ ký số	77
3.2.1	Định nghĩa và phân loại sơ đồ ký	78
3.2.2	Sơ đồ ký RSA	79
3.2.3	Sơ đồ chữ ký Rabin	81
3.2.4	Sơ đồ chữ ký ElGamal	81
3.2.5	Sơ đồ chữ ký Schnorr	82
3.2.6	Chuẩn chữ ký số DSS	83

