

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	Mật mã hạng nhẹ (<i>Lightweight Cryptography</i>)	66
2.5	Câu hỏi, bài tập và thực hành	67
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
