

105-V
BU-K

2015



NGUYỄN ĐÌNH THỨC · BÙI DOÃN KHANH

MÃ HÓA THÔNG TIN VỚI JAVA

Tập 2:

MÃ HÓA - MẬT MÃ

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRUNG TÂM THÔNG TIN THƯ VIỆN

V-DO/15126

NHÀ XUẤT BẢN LAO ĐỘNG XÃ HỘI

MỤC LỤC

LỜI NÓI ĐẦU	3
THƯ NGỎ	3
MỤC LỤC	5
Chương 1: KIẾN THỨC CƠ SỞ.....	9
I. ÁNH XẠ BIẾN ĐỔI	9
II. SỐ NGUYÊN	12
II.1. Phép chia Euclid.....	12
II.2. Số nguyên tố	13
II.3. Phép tính trên vành $\mathbb{Z}_n$	14
III. ĐỊNH LÝ FERMAT NHỎ	16
IV. ĐỊNH LÝ EULER.....	17
V. ĐỊNH LÝ SỐ DƯ TRUNG HOA.....	20
BÀI TẬP CHƯƠNG 1	22
Chương 2: TRƯỜNG HỮU HẠN.....	23
I. CẤU TRÚC NHÓM	23
I.1. Phép toán 2 ngôi	23
I.2. Nhóm và Nhóm con.....	24
I.3. Nhóm đơn sinh.....	26
II. VÀNH, MIẾN NGUYÊN, TRƯỜNG	26
II.1. Cấu trúc Vành.....	27
II.2. Miến nguyên	27
II.3. Vành chia và Trường.....	28

II.4. Đặc số nguyên tố của trường.....	29
III. TÍNH CHẤT CỦA TRƯỜNG HỮU HẠN.....	30
IV. VÍ DỤ ÁP DỤNG.....	34
IV.1. Định lý Fermat nhỏ.....	34
IV.2. Mã hóa dựa vào nhóm.....	34
BÀI TẬP CHƯƠNG 2.....	36
Chương 3: TÍNH TOÁN SỐ LỚN.....	37
I. CÁC PHÉP TOÁN SỐ HỌC DỰA TRÊN BIỂU DIỄN NHỊ PHÂN.....	37
I.1. Biểu diễn nhị phân.....	37
I.2. Thuật giải biểu diễn cơ sở nhị phân.....	38
I.3. Thuật giải cộng hai số nguyên dương.....	38
I.4. Thuật giải trừ hai số nguyên dương.....	38
I.5. Phép cộng và trừ [mod].....	39
I.6. Phép nhân [mod].....	39
I.7. Phép lũy thừa [mod].....	40
II. CÁC PHÉP TOÁN SỐ HỌC DỰA TRÊN CƠ SỞ B.....	41
II.1. Cộng hai số nguyên.....	41
II.2. Trừ 2 số nguyên.....	42
II.3. Nhân hai số nguyên.....	43
III. MỘT SỐ PHƯƠNG PHÁP TÍNH NHANH TRÊN SỐ LỚN.....	44
III.1. Nhân số lớn.....	44
III.2. Phép mod và phép chia.....	45
III.3. Phương pháp số dư Trung Hoa.....	46
BÀI TẬP CHƯƠNG 3.....	48
Chương 4: CÁC BÀI TOÁN QUAN TRỌNG TRONG LÝ THUYẾT SỐ VÀ MÃ HÓA THÔNG TIN.....	49
I. BÀI TOÁN SỐ NGUYÊN TỐ.....	49

1.1. Phép thử Miller.....	49
1.2. Phép thử Rabin-Miller.....	51
1.3. Tạo số nguyên tố lớn.....	52
II. BÀI TOÁN PHÂN TÍCH RA THỪA SỐ NGUYÊN TỐ.....	52
II.1. Phương pháp Fermat.....	53
II.2. Phương pháp Monte Carlo.....	56
II.3. Phương pháp Rho.....	57
III. BÀI TOÁN LOGARITHM RỜI RẠC.....	59
III.1. Một số khái niệm cơ bản.....	59
III.2. Tìm phần tử sinh.....	63
III.3. Tính logarithm rời rạc.....	63
BÀI TẬP CHƯƠNG 4.....	72
Chương 5: MÃ HÓA THÔNG TIN.....	73
I. MÃ TUYẾN TÍNH.....	73
1.1. Mã Caesar.....	73
1.2. Mã Affine.....	74
1.3. Mã Vigenere.....	76
1.4. Mã khối.....	77
1.5. Mã ma-trận.....	79
1.6. Mã hoán vị.....	80
1.7. Mã kết hợp thay thế/hoán vị.....	81
II. CÁC HỆ MÃ BẬC HAI.....	82
II.1. Mã Rabin.....	82
II.2. Mã xích khối.....	84
II.3. Mã xác suất Blum-Goldwasser.....	85
III. MÃ LŨY THỪA.....	88
III.1. Trao đổi khóa Diffie-Hellman.....	88

III.2. Mã Pohlig-Hellman.....	89
III.3. Mã hồi tác.....	90
III.4. Mã RSA.....	93
BÀI TẬP CHƯƠNG 5.....	96
Chương 6: CHỮ KÝ SỐ VÀ BẢO MẬT CƠ SỞ DỮ LIỆU.....	97
I. THÔNG ĐIỆP CÓ KÝ.....	97
I.1. Ký bằng RSA.....	97
I.2. Ký bằng mã Rabin.....	98
II. CHỮ KÝ SỐ.....	98
II.1. Khái niệm.....	98
II.2. Hàm băm MASH-2.....	99
II.3. Ký bằng ElGamal.....	100
II.4. Tấn công hàm ký số.....	101
II.5. Định danh tri thức trị không.....	102
III. BẢO MẬT CSDL.....	103
III.1. Mở đầu.....	103
III.2. Nghi thức mã CSDL.....	104
BÀI TẬP CHƯƠNG 6.....	104