

## **Chương 1. Mở đầu**

1.1. Giới thiệu tổng quan môn học"

1.2 Một số khái niệm cơ bản

## **Chương 2. Mã hóa cổ điển**

2.1. Các khái niệm về mã hóa "

2.2. Mã thế

1. Mã Caesar
2. Mã cặp - playfair
3. [Tự học] Mã đơn bảng chữ & Mã đa bảng chữ
4. [Tự học] Mã Hill

2.3. Mã hoán vị và mã hoán vị cải tiến

## **Chương 3. Lý thuyết số**

3.1 Giới thiệu Modulo"

3.2 Các phép toán modulo

[Tự học] 3.3 Tính nghịch đảo modulo

3.4 Giải phương trình và hệ phương trình đồng dư

3.5 Tính lũy thừa modulo

[Tự học] 3.6 Căn nguyên thủy và Logarit rời rạc

## **Chương 4. Mã khối hiện đại**

4.1 Giới thiệu tổng quan"

[Tự học] 4.2 Chuẩn mã hóa dữ liệu (DES)

[Tự học] 4.3 Trường hữu hạn  $GF(2^8)$

#### 4.4. Chuẩn mã hóa dữ liệu nâng cao (AES)

[Tự học] 4.5. Mã dòng hiện đại

### **Chương 5. Mã công khai**

#### 5.1 Giới thiệu tổng quan

#### 5.2 Mã công khai RSA

#### 5.3 Trao đổi khóa Diffie-Hellman

[Tự học] 5.4 Mã công khai Elgamal

### **Chương 6. Xác thực thông điệp**

#### 6.1 Giới thiệu về xác thực thông điệp"

[Tự học] 6.2 Mã xác thực thông điệp

[Tự học] 6.3 Hàm băm

[Tự học] 6.4 SHA

#### 6.5 Chữ ký điện tử DSA

### **Chương 7. Một số ứng dụng bảo mật trên mạng**

#### 7.1 Giới thiệu một số ứng dụng bảo mật trên mạng

[Tự học] 7.2 Trao đổi khóa

[Tự học] 7.3. Xác thực người sử dụng Kerberos

[Tự học] 7.4 Một số giao thức an ninh

#### 7.5 An toàn thư điện tử & thanh toán điện tử

### **Chương 8. An ninh hệ thống**

8.1 Giới thiệu mô hình an ninh hệ thống"

[Tự học] 8.2 Kẻ xâm nhập

[Tự học] 8.3 Phần mềm có hại

[Tự học] 8.4 Bức tường lửa

8.5 Hệ thống thông tin an toàn

**Ôn tập**

**Nghiệm thu bài thực hành**