BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP
THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

—————o0o—————

KHÓA LUẬN TỐT NGHIỆP

SƠ ĐỒ CHIA SẺ BÍ MẬT VÀ ỨNG DỤNG

Chuyên ngành: **KHOA HỌC MÁY TÍNH**

Giảng viên hướng dẫn: **PGS.TS XYZ**

Sinh viên: **NGUYỄN QUANG HUY**

Lớp: **KHOA HỌC MÁY TÍNH**

HỒ CHÍ MINH, 12/2019

Lời nói đầu

Thế giới của chúng ta luôn sôi sục trong muôn vàn biến động được tạo ra bởi con người. Và trong thế kỷ 20, máy tính là một trong những sản phẩm vĩ đại nhất. Cùng với thời gian, người ta không muốn sử dụng một máy tính đơn lẻ nữa mà sẽ kết nối các máy này lại thành một mạng máy tính nhằm tăng khả năng làm việc, hiểu biết, trao đổi, cập nhật các thông tin. . . .Mạng Internet là xu hướng phát triển của thế giới ngày nay. Hiện nay Internet đã trở nên rất phổ biến trên toàn thế giới. Thông qua mạng Internet mọi người có thể trao đổi thông tin với nhau một cách nhanh chóng thuận tiện.Khi một người muốn trao đổi thông tin với một người hay một tổ chức nào đó thông qua mạng máy tính thì yêu cầu quan trọng là làm sao để đảm bảo thông tin không bị sai lệch hoặc bị lộ do sự xâm nhập của kẻ thứ ba. Trước các yêu cầu cần thiết đó, lý thuyết về mật mã thông tin đã ra đời nhằm đảm bảo tính an toàn dữ liệu tại nơi lưu trữ cũng như khi dữ liệu được truyền trên mạng.

Trong các hệ mật mã, khoá là vấn đề rất quan trọng. Ở đây chúng ta sẽ nghiên cứu các vấn đề về tạo khoá cho người dùng trong bảo mật dữ liệu. Mô hình server tạo khoá giải quyết các công việc như quản lý và phân phối khóa một cách an toàn, hiệu quả. Quản trị khoá là một vấn đề rất rộng trong mật mã học. Nó bao gồm mã hoá khoá trước khi truyền. Liên quan đến việc truyền khoá là vấn đề xác định danh tính cho người dùng, ký điện tử.

Ngành mật mã học vẫn đang phát triển không ngừng. Trong thời đại mọi thông tin đều mang giá trị thì việc bảo mật thông tin càng trở nên có ý nghĩa. Để có một cơ sở hạ tầng tốt nhằm xây dựng các hệ thống bảo mật thì mọi nghiên cứu liên quan đến bảo mật và mã hoá đều cần phải có những nỗ lực lớn và đòi hỏi sự làm việc nghiêm túc và thử nghiệm kỹ càng. Trong khuôn khổ khoá luận này, em chỉ tập trung vào một vấn đề nhỏ là truyền khoá bí mật và chia sẻ khoá bí mật đồng thời tìm ra các ứng dụng thực tế cho cơ sở lý thuyết đó.

Mục lục

Chương 1

CHƯƠNG 1: CÁC KHÁI NIỆM VÀ THUẬT TOÁN CƠ BẢN

1.1 Lý thuyết toán học modulo

1.1.1 Hàm phi Euler

Định nghĩa 1.1.1. *Cho được định nghĩa là số các số nguyên trong khoảng từ nguyên tố cùng nhau với n. Hàm được gọi là hàm phi Euler*

1.1.2 Đồng dư thức

1.1.3 Không gian Zn

1.2 Vấn đề mã hoá

1.2.1 Mã hoá đối xứng

1.2.2 Mã hoá không đối xứng

1.3 Các cách tạo khoá

1.4 Phân phối khoá

Chương 2

CHƯƠNG 2: ỨNG DỤNG CHIA SẺ BÍ MẬT

Kết luận

Phụ lục

Tài liệu tham khảo