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

——————o0o——————

ĐỀ CƯƠNG LUẬN VĂN THẠC SĨ

***Đề tài*:**

SƠ ĐỒ CHIA SẺ BÍ MẬT VÀ ỨNG DỤNG

Chuyên ngành: **KHOA HỌC MÁY TÍNH**

Giảng viên hướng dẫn: **PGS.TS XYZ**

Học viên: **NGUYỄN QUANG HUY**

Lớp: **KHOA HỌC MÁY TÍNH**

HỒ CHÍ MINH, 12/2019

1. Tên đề tài

"Sơ đồ chia sẻ bí mật và ứng dụng "

2. Lý do chọn đề tài

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. Những công ty phát triển và kinh doanh trên môi trường Internet/Intranet họ phải đối diện với những khó khăn lớn là làm thế nào để bảo vệ những dữ liệu quan trọng, ngăn chặn những hình thức tấn công, truy xuất dữ liệu bất hợp pháp từ bên trong (Intranet) lẫn bên ngoài (Internet). 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. Khoá luận này tập trung vào nghiên cứu các khái niệm cơ bản, cơ sở lý thuyết toán học modulo sử dụng trong bảo mật thông tin, các phương pháp phân phối khoá và các cách tạo khoá. Đặc biệt là áp dụng các sơ đồ chia sẻ bí mật vào

việc quản lý các khóa bí mật. Vấn đề chia sẻ bí mật được đã được nghiên cứu từ những năm 70. Ý tưởng chính của chia sẻ bí mật dựa trên nguyên tắc đơn giản là không tin vào bất cứ ai. Một thông tin nào đó để đảm bảo an toàn thì ta không thể trao nó cho một người nắm giữ mà phải chia nhỏ thành các mảnh và chỉ trao cho mỗi người một hoặc một số mảnh sao cho một người với một số mảnh mình có không thể tìm ra thông tin bí mật. Việc phân chia các mảnh phải theo một sơ đồ chia sẻ bí mật nhất định thì mới có thể khôi phục lại thông tin bí mật. 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.

3. Mục tiêu nghiên cứu

4. Đối tượng và phạm vi nghiên cứu

5. Nội dung, địa điểm, vật liệu và phương pháp nghiên cứu

5.1 Nội dung nghiên cứu

5.2 Phương pháp nghiên cứu

5.2.1 Thời gian nghiên cứu.

5.2.2 Địa điểm nghiên cứu

5.2.3 Vật liệu nghiên cứu

5.2.4 Phương pháp nghiên cứu

5.2.5 Phương pháp xử lý số liệu

6. Dự kiến kết quả

Nghiên cứu lý thuyết

Nghiên cứu thực tiễn

7. Kế hoạch thực hiện

8. Kết cấu chi tiết các chương của luận văn

Tài liệu tham khảo