**CHƯƠNG 3: KẾT LUẬN VÀ BÀI HỌC KINH NGHIỆM**

**3.1. Kiến thức và kĩ năng đã học được trong quá trình thực hiện đề tài**

Trong quá trình thực hiện đề tài, chúng em đã hiểu được:

- Tìm hiểu về an ninh mạng và tầm quan trọng của an ninh mạng trong đời sống; vai trò của an ninh mạng: Trong bảo mật cá nhân, trong doanh nghiệp và chính phủ - quốc phòng

- Các mối hiểm họa trên không gian mạng: Malware, phishing, DDoS,…; các phương pháp bảo vệ an ninh mạng: sử dụng tường lửa, mã hóa dữ liệu, xác thực 2 yếu tố,…

- Tìm hiểu về Tiêu chuẩn mã hóa dữ liệu (DES): Khái niệm, thuật toán, quá trình sinh khóa con, quá trình mã hóa DES và giải mã DES

- Các ngôn ngữ lập trình phổ biến trong quá trình chuẩn hóa DES: Sử dụng ngôn ngữ C# và Java để thực hiện quá trình chuẩn hóa; về khái niệm, lịch sử ra đời, đặc điểm nổi bật, ưu điểm và ứng dụng của các ngôn ngữ lập trình

- Nghiên cứu, hiểu thế nào là mã hóa công khai, mã hóa bí mật

- Tầm quan trọng của chữ kí số và ứng dụng của nó trong thực tế

- Thiết kế kịch bản của chương trình trước khi cài đặt thuật toán

- Rèn luyện kĩ năng cài đặt chuẩn hóa DES vào mã hóa dữ liệu bằng ngôn ngữ Java và C#: Cài đặt thuật toán và giao diện chương trình

Ngoài ra, chúng em còn học được nhiều kĩ năng mềm trong quá trình làm việc nhóm như:

- Kỹ năng hợp tác:

+ Tôn trọng ý kiến khác biệt: Chấp nhận và học hỏi từ những quan điểm khác nhau.

+ Chia sẻ trách nhiệm: Phân công công việc hợp lý, hoàn thành nhiệm vụ đúng hạn.

+ Hỗ trợ lẫn nhau: Sẵn sàng giúp đỡ đồng đội khi cần thiết.

- Kỹ năng khác:

+ Quản lý thời gian: Lên kế hoạch, sắp xếp công việc hiệu quả.

+ Làm việc độc lập: Hoàn thành tốt phần việc được giao.

+ Khả năng thích ứng: Linh hoạt trước những thay đổi.

+ Khả năng chịu áp lực: Giữ bình tĩnh và làm việc hiệu quả trong những tình huống căng thẳng.

**3.2. Bài học kinh nghiệm**

**3.3. Đề xuất về tính khả thi của chủ đề nghiên cứu:**

Tính khả thi của chủ đề nghiên cứu:

Chủ đề nghiên cứu về tính khả thi của việc chuẩn hóa DES trong mã hóa dữ liệu là một chủ đề hết sức thú vị và có giá trị thực tiễn cao. Tuy nhiên, để đánh giá tính khả thi của chủ đề này, chúng ta cần xem xét một cách toàn diện các yếu tố sau:

+ Tính cấp thiết: DES là một tiêu chuẩn mã hóa đã lỗi thời và không còn đảm bảo được độ an toàn trong môi trường hiện nay. Việc đánh giá lại và chuẩn hóa DES là cần thiết để đảm bảo an ninh thông tin.

+ Tính mới lạ: Mặc dù DES đã được nghiên cứu rất nhiều, nhưng việc đánh giá lại tính khả thi của nó trong bối cảnh công nghệ hiện đại vẫn là một vấn đề mới mẻ và chưa được nghiên cứu sâu rộng.

+ Tính thực tiễn: Kết quả nghiên cứu này sẽ có ý nghĩa thực tiễn rất lớn, giúp các tổ chức, doanh nghiệp đánh giá lại hệ thống mã hóa hiện tại và đưa ra những quyết định phù hợp.

Chủ đề nghiên cứu này hoàn toàn khả thi và có giá trị khoa học cũng như thực tiễn cao.

Những thuận lợi khi chuẩn hóa DES:

+ Tiêu chuẩn hóa: Việc chuẩn hóa DES sẽ giúp cho việc triển khai và quản lý hệ thống mã hóa trở nên dễ dàng hơn.

+ Tương thích: Các hệ thống mã hóa hiện tại dựa trên DES có thể dễ dàng được nâng cấp để đáp ứng các tiêu chuẩn mới.

+ An toàn: Một tiêu chuẩn DES được chuẩn hóa sẽ giúp đảm bảo tính bảo mật của dữ liệu tốt hơn.

Những khó khăn khi chuẩn hóa DES

+ Độ dài khóa: Độ dài khóa 56 bit của DES quá ngắn và dễ bị tấn công bằng vũ lực.

+ Các cuộc tấn công khác: DES cũng dễ bị một số loại tấn công khác như tấn công tuyến tính và tấn công vi phân.

+ Tiêu chuẩn mới: Việc thay thế DES bằng một tiêu chuẩn mã hóa mới sẽ tốn kém và mất thời gian.

+ Kháng cự: Một số tổ chức có thể không muốn thay đổi hệ thống mã hóa hiện tại của họ.

Để khắc phục những khó khăn trên, có thể đưa ra một số đề xuất sau:

+ Không nên chuẩn hóa DES: Thay vào đó, nên khuyến khích các tổ chức sử dụng các thuật toán mã hóa hiện đại và mạnh mẽ hơn như AES.

+ Chuẩn hóa một phiên bản nâng cấp của DES: Có thể nâng cấp độ dài khóa của DES lên 128 bit hoặc 256 bit để tăng cường độ bảo mật. Tuy nhiên, giải pháp này chỉ là tạm thời và không giải quyết được các vấn đề về thiết kế của DES.

+ Kết hợp DES với các thuật toán mã hóa khác: Có thể kết hợp DES với các thuật toán mã hóa khác để tạo ra một hệ thống mã hóa hybrid, tăng cường độ bảo mật.

Việc chuẩn hóa DES là một vấn đề phức tạp và cần được cân nhắc kỹ lưỡng. Các nhà nghiên cứu cần đánh giá kỹ lưỡng các ưu và nhược điểm của việc chuẩn hóa DES trước khi đưa ra quyết định cuối cùng.