

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

PHIẾU HỌC TẬP NHÓM

I. Thông tin chung

1. Tên lớp: 20231IT6001001

Khóa: 16

2. Tên nhóm: 7

4. Họ và tên thành viên trong nhóm: Tổng Khánh Linh, Nguyễn Hồng Ánh, Lê Thị Ngọc Mai, Phan Thị Sao Mai, Quách Thị Hồng Minh

II. Nội dung học tập

1. Tên chủ đề: Chữ ký số và ứng dụng trong thương mại điện tử.

2. Hoạt động của sinh viên (xác định các hoạt động chính của sinh viên trong quá trình thực hiện Bài tập lớn)

- Hoạt động/Nội dung 1: Tìm tài liệu, nghiên cứu lý thuyết về an toàn bảo mật thông tin, lý do chọn đề tài, sơ lược các nội dung trình bày và kiến thức cơ sở áp dụng vào đề tài nghiên cứu. Mục tiêu/chuẩn đầu ra: Hoàn thành chương 1: Tổng quan về an toàn bảo mật thông tin và chữ ký số.

- Hoạt động/Nội dung 2: Tìm hiểu về kỹ thuật sử dụng chữ ký số. Mục tiêu/chuẩn đầu ra: Hoàn thành chương 2: Kỹ thuật sử dụng gồm cơ sở lý thuyết và nền tảng toán học

- Hoạt động/Nội dung 3: Cài đặt thuật toán và xây dựng chương trình mô phỏng hoạt động của chữ ký số. Mục tiêu/chuẩn đầu ra: Hoàn thiện chương 2

- Hoạt động/Nội dung 4: Đưa ra kết quả nghiên cứu và tiến hành viết báo cáo tổng kết. Mục tiêu/chuẩn đầu ra: Hoàn thành báo cáo

3. Sản phẩm nghiên cứu

-Báo cáo thực nghiệm

-Chương trình demo

III. Nhiệm vụ học tập

1. Hoàn thành Bài tập lớn theo đúng thời gian quy định (từ ngày 25/10/2023 đến ngày 25/11/2023)

2. Báo cáo sản phẩm nghiên cứu theo chủ đề được giao trước giảng viên và những sinh viên khác

IV. Học liệu thực hiện Tiểu luận, Bài tập lớn, Đồ án/Dự án

1. Tài liệu học tập:

[1]. Bruce Schneiner, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, NXB Wiley, 1996

[2]. NIST (2013), Tiêu chuẩn chữ ký số, từ
<https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf>

[3]. Thư viện hashlib python, từ
<https://docs.python.org/3.10/library/hashlib.html>

2. Phương tiện, nguyên liệu thực hiện Bài tập lớn (nếu có): Máy tính, máy in.

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

KẾ HOẠCH BÀI TẬP LỚN

Tên lớp: 20231IT6001001

Khóa: 16

Tên nhóm: 7

Họ và tên thành viên trong nhóm: Tống Khánh Linh, Nguyễn Hồng Ánh, Lê Thị Ngọc Mai, Phan Thị Sao Mai, Quách Thị Hồng Minh

Tên đề tài: Chữ ký số và ứng dụng trong thương mại điện tử

Tuần	Người thực hiện	Nội dung công việc	Phương pháp thực hiện
1	Nguyễn Hồng Ánh	Tổng quan về an toàn và bảo mật thông tin	Tìm hiểu giáo trình và tài liệu Internet
	Tống Khánh Linh	Nội dung nghiên cứu đề tài và lời mở đầu	
	Lê Thị Ngọc Mai	Lý do chọn đề tài	Tìm hiểu Internet và tình hình thực tế
	Phan Thị Sao Mai	Tổng quan về chữ ký số	Tìm hiểu giáo trình và tài liệu Internet
	Quách Thị Hồng Minh	Chữ ký số trong thương mại điện tử	
2	Nguyễn Hồng Ánh	Tìm hiểu công cụ sử dụng	Tìm hiểu giáo trình và tài liệu Internet
	Tống Khánh Linh	Tìm hiểu cơ sở lý thuyết	Dựa vào nội dung đã học và tài liệu Internet
	Lê Thị Ngọc Mai	Tìm hiểu nền tảng toán học	
	Phan Thị Sao Mai	Tìm hiểu thuật toán chữ ký số	
	Quách Thị Hồng Minh		
3 - 4	Nguyễn Hồng Ánh	Viết thủ tục kiểm tra số nguyên tố, tạo số nguyên tố, tìm nghịch đảo module	Dựa vào nội dung đã học

	Tổng Khánh Linh	Tìm hiểu thuật toán ký và viết thủ tục ký tài liệu	Tìm hiểu giáo trình và tài liệu Internet
	Lê Thị Ngọc Mai	Viết thủ tục tạo và tìm tham số p,q,g,h	Dựa vào nội dung đã học và tìm hiểu trên Internet
	Phan Thị Sao Mai	Tìm hiểu và viết thủ tục tạo cặp khóa bí mật và khóa công khai	Tìm hiểu giáo trình và tài liệu Internet
	Quách Thị Hồng Minh	Tìm hiểu thuật toán xác minh chữ ký và viết thủ tục	Tìm hiểu giáo trình và tài liệu Internet
	Cả nhóm	Thảo luận và viết code hoàn chỉnh	Sử dụng Internet tìm hiểu lỗi sai
5	Nguyễn Hồng Ánh	Viết mô phỏng thuật toán	Dựa vào nội dung đã thực hiện
	Tổng Khánh Linh	Hoàn chỉnh báo cáo	Dựa vào nội dung đã thực hiện
	Lê Thị Ngọc Mai	Viết kết luận	Dựa vào nội dung đã thực hiện
	Phan Thị Sao Mai	Đánh giá độ phức tạp	Tìm hiểu Internet và qua quá trình thực hiện
	Quách Thị Hồng Minh	Đánh giá tính bảo mật	Tìm hiểu Internet và qua quá trình thực hiện

Ngày tháng năm

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO HỌC TẬP NHÓM

Tên lớp: 20231IT6001001

Khóa: 16

Tên nhóm: 7

Họ và tên thành viên trong nhóm: Tống Khánh Linh, Nguyễn Hồng Ánh, Lê Thị Ngọc Mai, Phan Thị Sao Mai, Quách Thị Hồng Minh

Tên đề tài: Chữ ký số và ứng dụng trong thương mại điện tử

Tuần	Người thực hiện	Nội dung công việc	Kết quả đạt được	Kiến nghị với giảng viên hướng dẫn (Nêu những khó khăn, hỗ trợ từ phía Giảng viên... nếu có)
1	Nguyễn Hồng Ánh	Tổng quan về an toàn và bảo mật thông tin	Hoàn thành	Nhóm mới đang học Python cơ bản nên gặp khá nhiều khó khăn về kiến thức code, phải tham khảo nhiều. Trong quá trình học, giảng viên chỉ dạy và giảng rất chi tiết nên nhóm nắm bắt khá ổn.
	Tống Khánh Linh	Nội dung nghiên cứu đề tài và lời mở đầu	Hoàn thành	
	Lê Thị Ngọc Mai	Lý do chọn đề tài	Hoàn thành	
	Phan Thị Sao Mai	Tổng quan về chữ ký số	Hoàn thành	
	Quách Thị Hồng Minh	Chữ ký số trong thương mại điện tử	Hoàn thành	
2	Nguyễn Hồng Ánh	Tìm hiểu công cụ sử dụng	Hoàn thành	
	Tống Khánh Linh	Tìm hiểu cơ sở lý thuyết	Hoàn thành	

	Lê Thị Ngọc Mai	Tìm hiểu nền tảng toán học	Hoàn thành	
	Phan Thị Sao Mai	Tìm hiểu thuật toán chữ ký số	Hoàn thành	
	Quách Thị Hồng Minh		Hoàn thành	
3-4	Nguyễn Hồng Ánh	Viết thủ tục kiểm tra số nguyên tố, tạo số nguyên tố, tìm nghịch đảo module	Hoàn thành	
	Tổng Khánh Linh	Tìm hiểu thuật toán ký và viết thủ tục ký tài liệu	Hoàn thành	
	Lê Thị Ngọc Mai	Viết thủ tục tạo và tìm tham số p, q, g, h	Hoàn thành	
	Phan Thị Sao Mai	Tìm hiểu và viết thủ tục tạo cặp khóa bí mật và khóa công khai	Hoàn thành	
	Quách Thị Hồng Minh	Tìm hiểu thuật toán xác minh chữ ký và viết thủ tục	Hoàn thành	
	Cả nhóm	Thảo luận và viết code hoàn chỉnh	Hoàn thành	
5	Nguyễn Hồng Ánh	Viết mô phỏng thuật toán	Hoàn thành	
	Tổng Khánh Linh	Tổng hợp và hoàn thành tất cả nội dung báo cáo	Hoàn thành	

	Lê Thị Ngọc Mai	Đánh giá độ phức tạp	Hoàn thành	
	Phan Thị Sao Mai	Làm powerpoint	Hoàn thành	
	Quách Thị Hồng Minh	Đánh giá tính bảo mật	Hoàn thành	

Ngày tháng năm

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)