**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM 13**

Tên lớp: An Toàn Và Bảo Mật Thông Tin – 20241IT6001002 Khóa: K16

Họ và tên sinh viên: Nguyễn Xuân Sơn, Dương Văn Chung, Lê Trung Hiếu, Nguyễn Minh Quang, Nguyễn Lương Chiến

Tên nhóm: 13

Tên chủ đề: Tìm hiểu về hệ chữ ký DSA và viết ứng dụng minh họa (Sử dụng ngôn ngữ C++, C#)

| **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 cần) |
| --- | --- | --- | --- | --- |
| 1 | Nguyễn Xuân Sơn | Tìm hiểu lý thuyết về hệ chữ ký số DSA, nguyên lý hoạt động và ứng dụng trong bảo mật | Đọc tài liệu, hiểu các khái niệm cơ bản về DSA |  |
| Lê Trung Hiếu | Tìm hiểu về các thuật toán sinh khoá trong DSA, các phép toán số học cơ bản (nghịch đảo modulo, a^b mod n) | Đọc tài liệu và tài liệu tham khảo |  |
| Nguyễn Minh Quang | Tìm hiểu lý thuyết về kiểm tra tính hợp lệ chữ ký và các ứng dụng trong thực tế. | Nắm được các cách thức kiểm tra chữ ký DSA |  |
| Dương Văn Chung | Tìm hiểu về các phép toán số học trong DSA (GCD, kiểm tra số nguyên tố, sinh số nguyên tố ngẫu nhiên) | Nghiên cứu các thuật toán số học trong DSA |  |
| Nguyễn Lương Chiến | Tìm hiểu về giao diện người dùng và các yêu cầu giao tiếp cho hệ thống chữ ký số DSA | Xác định yêu cầu giao diện người dùng |  |
| 2 | Nguyễn Xuân Sơn | Code hàm sinh khoá công khai và khoá bí mật (DSA) | Hoàn thành hàm sinh khoá |  |
| Lê Trung Hiếu | Code hàm sinh số nguyên tố ngẫu nhiên, các phép toán số học trong DSA (nghịch đảo modulo, GCD, a^b mod n) | Hoàn thành các hàm sinh số nguyên tố và tính toán số học |  |
| Nguyễn Minh Quang | Code hàm kiểm tra chữ ký và tính hợp lệ chữ ký DSA | Hoàn thành chức năng kiểm tra chữ ký |  |
| Dương Văn Chung | Code các phép toán số học phức tạp trong DSA | Hoàn thành các phép toán số học |  |
| Nguyễn Lương Chiến | Thiết kế giao diện người dùng | Hoàn thành giao diện người dùng, test chức năng mã hoá và giải mã |  |
| 3 | Nguyễn Xuân Sơn | Code hàm mã hoá và giải mã chữ ký số DSA | Hoàn thành mã hoá và giải mã chữ ký |  |
| Lê Trung Hiếu | Code các phép toán số học trong DSA (tính nghịch đảo modulo, a^b mod n) học cơ bản (nghịch đảo modulo, a^b mod n) | Hoàn thành các phép toán |  |
| Nguyễn Minh Quang | Hoàn thiện tính năng kiểm tra chữ ký và tải lên chữ ký (C++) | Hoàn thiện tính năng kiểm tra chữ ký |  |
| Dương Văn Chung | Xử lý các thuật toán tối ưu hoá và kiểm tra bảo mật cho các phép toán trong DSA | Hoàn thiện thuật toán tối ưu hoá và bảo mật |  |
| Nguyễn Lương Chiến | Code giao diện tải lên và tải xuống chữ ký, kiểm tra tính năng | Hoàn thiện giao diện cho tính năng này |  |
| 4 | Nguyễn Xuân Sơn | Hoàn thiện các chức năng mã hoá và giải mã chữ ký | Hoàn thiện các chức năng mã hoá và giải mã |  |
| Lê Trung Hiếu | Tối ưu hoá các phép toán số học trong DSA, kiểm tra tính chính xác và bảo mật các thuật toán | Tối ưu hoá thuật toán DSA |  |
| Nguyễn Minh Quang | Kiểm tra và tối ưu mã nguồn cho phần kiểm tra chữ ký số DSA | Hoàn thiện kiểm tra tính hợp lệ chữ ký |  |
| Dương Văn Chung | Tối ưu hoá phần mềm, kiểm tra bảo mật và hiệu suất của các thuật toán DSA | Tối ưu mã nguồn C++ và cải thiện hiệu suất |  |
| Nguyễn Lương Chiến | Kiểm tra và sửa lỗi giao diện người dùng, đảm bảo các chức năng hoạt động ổn định | Kiểm tra tính năng giao diện và sửa lỗi |  |
| 5 | Nguyễn Xuân Sơn | Hoàn thiện phần báo cáo về nguyên lý hoạt động chữ ký số DSA, ứng dụng thực tế và các vấn đề bảo mật | Hoàn thành báo cáo nguyên lý hoạt động |  |
| Lê Trung Hiếu | Hoàn thiện báo cáo về các thuật toán sinh khoá, các phép toán số học trong DSA | Hoàn thành báo cáo thuật toán sinh khoá |  |
| Nguyễn Minh Quang | Hoàn thiện báo cáo về cách kiểm tra tính hợp lệ chữ ký và giải mã chữ ký DSA | Hoàn thiện báo cáo kiểm tra chữ ký |  |
| Dương Văn Chung | Hoàn thiện báo cáo về các phép toán số học trong DSA (GCD, nghịch đảo modulo) | Hoàn thành báo cáo về phép toán số học |  |
| Nguyễn Lương Chiến | Hoàn thiện báo cáo tổng quan và giao diện người dùng của hệ thống | Hoàn thành báo cáo giao diện và tổng quan |  |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp

**PHIẾU HỌC TẬP CÁ NHÂN/NHÓM**

1. **Thông tin chung**
2. Tên lớp: … Khóa: ….
3. Họ và tên sinh viên (nếu giao phiếu học tập cá nhân)…….
4. Tên nhóm (nếu giao phiếu học tập nhóm)……. Họ và tên thành viên trong nhóm ……….
5. **Nội dung học tập**
6. Tên chủ đề:
7. 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 …
* Hoạt động/ Nội dung 2: Cài đặt thuật toán, xây dựng chương trình mô phỏng hoạt động của …
* Hoạt động/ Nội dung 3: Viết báo cáo tổng kết …

1. Sản phẩm nghiên cứu (Bản thuyết minh, bài thu hoạch, mô hình, sơ đồ, bản vẽ, trang website, bài báo khoa học …)

* Báo cáo thực nghiệm
* Chương trình demo

1. **Nhiệm vụ học tập**
2. Hoàn thành Bài tập lớn theo đúng thời gian quy định (từ ngày 11/11/2024 đến ngày 15/12/2024)
3. Báo cáo sản phẩm nghiên cứu theo chủ đề được giao trước giảng viên và những sinh viên khác
4. **Học liệu thực hiện Bài tập lớn**
5. Tài liệu học tập:

[1]. Bùi Doãn Khanh, Nguyễn Đình Thúc, *Mã hóa thông tin – Lý thuyết và ứng dụng*, NXB Lao động xã hội, 2011.

[2] …

[3] …

1. Phương tiện, nguyên liệu thực hiện Bài tập lớn (nếu có):….

* Máy tính, …

**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: ….. Khóa: …

Họ và tên sinh viên (nếu cá nhân thực hiện): …

Tên nhóm:…

Tên chủ đề: ….

| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| --- | --- | --- | --- |
| 1 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |
| 2 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |
| 3 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |
| 4 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |
| 5 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp