**BÁO CÁO HỌC TẬP CÁ NHÂN/NHÓM**

Tên lớp: An Ninh Mạng - 202411T6070001

Họ và tên sinh viên trong nhóm :

Trần Gia Hoàng - 2021605995

Phạm Việt Hưng - 2021603253

Phạm Đức Toản – 2021606942

Trần Xuân Đức - 2022600490

Đỗ Trọng Thích – 2021604318

Tên nhóm: Nhóm 1

Tên chủ đề: **CHỮ KÝ SỐ RSA VÀ ỨNG DỤNG TRONG XÁC THỰC TÍNH TOÀN VẸN CỦA DỮ LIỆU**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | Trần Gia Hoàng | Tổng quan về an toàn thông tin | **Hoàn thành** |  |
| Phạm Việt Hưng | Lý do chọn đề tài |
| Phạm Đức Toản | Tìm hiểu sự cần thiết của an toàn và bảo mật thông tin |
| Trần Xuân Đức | Tìm hiểu mục đích của an toàn và bảo mật thông tin |
| Đỗ Trọng Thích | Kiến thức cơ sở |
| 2 | Đỗ Trọng Thích | Tìm hiểu về chữ ký số | **Hoàn thành** |  |
| Phạm Việt Hưng | Nghiên cứu tìm hiểu hệ mã hóa công khai |
| Trần Xuân Đức | Tìm hiểu nội dung thuật toán RSA |
| Trần Gia Hoàng |
| Phạm Đức Toản | Tìm hiểu ứng dụng của chữ ký số RSA |
| 3 | Phạm Đức Toản | Chữ ký số và ứng dụng trong thực tế | **Hoàn thành** |  |
| Đỗ Trọng Thích | Giới thiệu ngôn ngữ lập trình sử dụng để cài đặt thuật toán  Thiết kế kịch bản chương trình |
| Phạm Việt Hưng | Kiến thức đã học được trong quá trình thực hiện đề tài |
| Trần Xuân Đức | Cài đặt thuật toán |
| Trần Gia Hoàng | Bài học kinh nghiệm |
| 4 | Phạm Đức Toản | Giao diện và tạo khóa (Java) | **Hoàn thành** |  |
| Đỗ Trọng Thích | Tạo khóa (Java) |
| Phạm Việt Hưng | Giao diện (C#) |
| Trần Xuân Đức | Giao diện, tạo chữ kí kiểm tra chữ kí bổ sung tạo khóa thủ công. |
| Trần Gia Hoàng | Tạo chữ kí, kiểm tra chữ kí (C#) |
| 5 | Phạm Đức Toản | Tổng hợp và hoàn chỉnh bài tập lớn. | **Hoàn thành** |  |
| Đỗ Trọng Thích |
| Phạm Việt Hưng |
| Trần Xuân Đức |
| Trần Gia Hoàng |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp

**PHIẾU HỌC TẬP NHÓM**

1. **Thông tin chung**
2. Tên lớp: An Ninh Mạng - 202411T6070001 Khóa: 16,17
3. Tên nhóm: Nhóm 1
4. Họ và tên sinh viên trong nhóm :   
    Trần Gia Hoàng – 2021605995

Phạm Việt Hưng – 2021603253

Phạm Đức Toản – 2021606942

Trần Xuân Đức – 2022600490

Đỗ Trọng Thích – 2021604318

1. **Nội dung học tập**
2. Tên chủ đề: **CHỮ KÝ SỐ RSA VÀ ỨNG DỤNG TRONG XÁC THỰC TÍNH TOÀN VẸN CỦA DỮ LIỆU**
3. Hoạt động của sinh viên

* Hoạt động/ Nội dung 1: Tìm tài liệu, nghiên cứu lý thuyết về an ninh mạng, an toàn và bảo mật thông tin.
* Hoạt động/ Nội dung 2: Cài đặt thuật toán, xây dựng chương trình mô phỏng hoạt động của chữ ký số RSA và ứng dụng trong xác thực tính toàn vẹn của dữ liệu.
* 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]. Nguyễn Xuân Dũng, *Bảo mật thông tin – Mô Hình và ứng dụng*, NXB thống kê, 2009.

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

[3]. William Stallings**,** *Cryptography and Network Security Principles and Practices***,** Fourth Edition, Prentice Hall, 2005.

1. Phương tiện, nguyên liệu thực hiện Bài tập lớn : Laptop.

**BÁO CÁO HỌC TẬP NHÓM**

Tên lớp: An Ninh Mạng - 202411T6070001

Họ và tên sinh viên trong nhóm :

Trần Gia Hoàng - 2021605995

Phạm Việt Hưng - 2021603253

Phạm Đức Toản – 2021606942

Trần Xuân Đức - 2022600490

Đỗ Trọng Thích – 2021604318

Tên nhóm: Nhóm 1

Tên chủ đề: **CHỮ KÝ SỐ RSA VÀ ỨNG DỤNG TRONG XÁC THỰC TÍNH TOÀN VẸN CỦA DỮ LIỆU**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| 1 | Trần Gia Hoàng | Tổng quan về an toàn thông tin | Tài liệu tham khảo trên mạng |
| Phạm Việt Hưng | Lý do chọn đề tài | Họp Online |
| Phạm Đức Toản | Tìm hiểu sự cần thiết của an toàn và bảo mật thông tin | Giáo trình an ninh mạng, kiến thức đã học. |
| Trần Xuân Đức | Tìm hiểu mục đích của an toàn và bảo mật thông tin | Giáo trình an ninh mạng, kiến thức đã học. |
| Đỗ Trọng Thích | Kiến thức cơ sở | Giáo trình an ninh mạng, kiến thức đã học. |
| 2 | Đỗ Trọng Thích | Tìm hiểu về chữ ký số | Giáo trình an ninh mạng, kiến thức đã học và tài liệu tham khảo trên mạng |
| Phạm Việt Hưng | Nghiên cứu tìm hiểu hệ mã hóa công khai | Giáo trình an ninh mạng, kiến thức đã học và tài liệu tham khảo trên mạng |
| Trần Xuân Đức | Tìm hiểu nội dung thuật toán RSA | Giáo trình an ninh mạng, kiến thức đã học và tài liệu tham khảo trên mạng  Giáo trình an ninh mạng, kiến thức đã học và tài liệu tham khảo trên mạng |
| Trần Gia Hoàng |
| Phạm Đức Toản | Tìm hiểu ứng dụng của chữ ký số RSA |
| 3 | Phạm Đức Toản | Chữ ký số và ứng dụng trong thực tế | Tài liệu tham khảo trên mạng |
| Đỗ Trọng Thích | Giới thiệu ngôn ngữ lập trình sử dụng để cài đặt thuật toán  Thiết kế kịch bản chương trình | Tài liệu tham khảo trên mạng |
| Phạm Việt Hưng | Kiến thức đã học được trong quá trình thực hiện đề tài | Giáo trình an ninh mạng, kiến thức đã học và tài liệu tham khảo trên mạng |
| Trần Xuân Đức | Cài đặt thuật toán | Sử dụng công cụ Visual Studio, Eclipse IDE |
| Trần Gia Hoàng | Bài học kinh nghiệm | Tài liệu tham khảo trên mạng |
| 4 | Phạm Đức Toản | Giao diện và tạo khóa (Java) | IntelliJ IDEA |
| Đỗ Trọng Thích | Tạo khóa (Java) | IntelliJ IDEA |
| Phạm Việt Hưng | Giao diện (C#) | Visual Studio Code |
| Trần Xuân Đức | Giao diện, tạo chữ kí kiểm tra chữ kí bổ sung tạo khóa thủ công. | IntelliJ IDEA |
| Trần Gia Hoàng | Tạo chữ kí, kiểm tra chữ kí (C#) | Visual Studio Code |
| 5 | Phạm Đức Toản | Tổng hợp và hoàn chỉnh bài tập lớn. | Họp Online |
| Đỗ Trọng Thích |
| Phạm Việt Hưng |
| Trần Xuân Đức |
| Trần Gia Hoàng |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp