**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: An ninh mạng

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

1. Nguyễn Bá Thuận Mã SV: 2022603360

2. Đỗ Tuấn Đạt Mã SV: 2022602884

3. Nguyễn Văn Dũng Mã SV: 2023601938

4. Nguyễn Mạnh Hùng Mã SV: 2021608268

5. Lê Đăng Dương Mã SV: 2021607148

Tên nhóm: 2

Tên chủ đề: **Chữ ký số Elgmal 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 | Nguyễn Bá Thuận | Tổng quan về an ninh mạng | Hoàn thành |  |
| Lê Đăng Dương | Lý do chọn đề tài |
| Đỗ Tuấn Đạt | Nội dung nghiên cứu |
| Nguyễn Văn Dũng | Sự cần thiết của an toàn bảo mật thông tin |
| Nguyễn Mạnh Hùng | Kiến thức cơ sở |
| 2 | Nguyễn Bá Thuận | Nghiên cứu tìm hiểu về hệ mật Elgamal | Hoàn thành |  |
| Lê Đăng Dương |
| Đỗ Tuấn Đạt | Nghiên cứu tìm hiểu về hệ mã khóa công khai |
| Nguyễn Mạnh Hùng | Tìm hiểu về chữ ký số |
| Nguyễn Văn Dũng | Tìm hiểu về hàm băm |
| 3 | Nguyễn Bá Thuận | Nghiên cứu tìm hiểu về chữ ký số Elgamal | Hoàn thành |  |
| Lê Đăng Dương |
| Đỗ Tuấn Đạt | Kịch bản chương trình |
| Nguyễn Mạnh Hùng |
| Nguyễn Văn Dũng | Giới thiệu ngôn ngữ lập trình sử dụng để triển khai ứng dụng |
| 4 | Nguyễn Bá Thuận | Tạo chữ ký, giải mã chữ ký bằng Java |  |  |
| Đỗ Tuấn Đạt | Làm giao diện bằng ngôn ngữ java |
| Nguyễn Mạnh Hùng | Tạo khóa bằng ngôn ngữ Java |
| Lê Đăng Dương | Tạo khóa, tạo chữ ký, kiểm tra chữ ký bằng ngôn ngữ C# |
| Nguyễn Văn Dũng | Làm giao diện bằng ngôn ngữ C# |
| 5 | Nguyễn Bá Thuận | Tổng hợp và hoàn thành báo cáo thực nghiệm | Hoàn Thành |  |
| Đỗ Tuấn Đạt |
| Nguyễn Mạnh Hùng |
| Lê Đăng Dương |
| Nguyễn Văn Dũng |

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: An ninh mạng Khóa: K17
3. Họ và tên sinh viên (nếu giao phiếu học tập cá nhân)
4. Tên nhóm 2. Họ và tên thành viên trong nhóm:

1. Nguyễn Bá Thuận Mã SV: 2022603360

2. Đỗ Tuấn Đạt Mã SV: 2022602884

3. Nguyễn Văn Dũng Mã SV: 2023601938

4. Nguyễn Mạnh Hùng Mã SV: 2021608268

5. Lê Đăng Dương Mã SV: 2021607148

1. **Nội dung học tập**
2. Tên chủ đề: Chữ ký số Elgmal và ứng dụng trong xác thực tính toàn vẹn của dữ liệu.
3. 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: Lập kế hoạch về triển khai báo cáo thực nghiệm, tìm hiểu vể chủ đề
* Hoạt động/ Nội dung 2: Cài đặt thuật toán, xây dựng chương trình mô phỏng hoạt động của chữ ký số elgama
* 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

[4]. TS Thái Thanh Tùng, giáo trình mật mã học an toàn thông tin.

[5].<https://mawgoud.medium.com/digital-signature-vs-electronic-signature-concept-applications-and-security-2cac54aace59>

[6]. <https://luanvan.co/luan-van/he-elgamal-45318/>

[7].<https://www.researchgate.net/publication/220709516_A_Comparative_Study_of_Elgamal_Based_Cryptographic_Algorithms>

[8].https://www.geeksforgeeks.org/elgamal-encryption-algorithm/

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

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

* Máy tính, …

**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: An ninh mạng Khóa: K17

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

1. Nguyễn Bá Thuận Mã SV: 2022603360

2. Đỗ Tuấn Đạt Mã SV: 2022602884

3. Nguyễn Văn Dũng Mã SV: 2023601938

4. Nguyễn Mạnh Hùng Mã SV: 2021608268

5. Lê Đăng Dương Mã SV: 2021607148

Tên nhóm: 2

Tên chủ đề: ….

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| 1 | Nguyễn Bá Thuận | Tổng quan về an ninh mạng | * Giáo trình an ninh mạng, kiến thức đã học. * Tài liệu tham khảo các khóa trước * Họp Online * Tài liệu tham khảo trên mạng |
| Lê Đăng Dương | Lý do chọn đề tài |
| Đỗ Tuấn Đạt | Nội dung nghiên cứu |
| Nguyễn Văn Dũng | Sự cần thiết của an toàn bảo mật thông tin |
| Nguyễn Mạnh Hùng | Kiến thức cơ sở |
| 2 | Nguyễn Bá Thuận | Nghiên cứu tìm hiểu về hệ mật Elgamal | * Giáo trình an ninh mạng, kiến thức đã học. * Tài liệu tham khảo các khóa trước * Họp Online * Tài liệu tham khảo trên mạng |
| Lê Đăng Dương |
| Đỗ Tuấn Đạt | Nghiên cứu tìm hiểu về hệ mã khóa công khai |
| Nguyễn Mạnh Hùng | Tìm hiểu về chữ ký số |
| Nguyễn Văn Dũng | Tìm hiểu về hàm băm |
| 3 | Nguyễn Bá Thuận | Nghiên cứu tìm hiểu về chữ ký số Elgamal | * Giáo trình an ninh mạng, kiến thức đã học. * Tài liệu tham khảo các khóa trước * Họp Online * Tài liệu tham khảo trên mạng |
| Lê Đăng Dương |
| Đỗ Tuấn Đạt | Kịch bản chương trình |
| Nguyễn Mạnh Hùng |
| Nguyễn Văn Dũng | Giới thiệu ngôn ngữ lập trình sử dụng để triển khai ứng dụng |
| 4 | Nguyễn Bá Thuận | Tạo chữ ký, giải mã chữ ký bằng Java | * Giáo trình an ninh mạng. * Tài liệu tham khảo các khóa trước * Họp Online * Tài liệu tham khảo trên mạng * Công cụ sử dụng visual studio, Net beans |
| Đỗ Tuấn Đạt | Làm giao diện bằng ngôn ngữ java |
| Nguyễn Mạnh Hùng | Tạo khóa bằng ngôn ngữ Java |
| Lê Đăng Dương | Tạo khóa, tạo chữ ký, kiểm tra chữ ký bằng ngôn ngữ C# |
| Nguyễn Văn Dũng | Làm giao diện bằng ngôn ngữ C# |
| 5 | Nguyễn Bá Thuận | Tổng hợp và hoàn thành báo cáo thực nghiệm | * Tài liệu thầy gửi, kiến thức, kinh nghiệm, trải nghiệm qua năm tháng. |
| Đỗ Tuấn Đạt |
| Nguyễn Mạnh Hùng |
| Lê Đăng Dương |
| Nguyễn Văn Dũng |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp