**BÁO CÁO HỌC TẬP CÁ NHÓM**

Tên lớp: 20241IT6070001 Khóa: K17

Tên nhóm Nhóm 9

Tên chủ đề: Tìm hiểu về hệ mật RSA và ứng dụng trong thực tế

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | 1. Nguyễn Hải Biên | Giới thiệu, tìm hiểu về chữ ký số và mục đích đề tài (Chương 1) | - Hoàn thành |  |
| 2. Phạm Việt Đức | Tìm hiểu phương pháp, đối tượng nghiên cứu, ý nghĩa khoa học và thực tiễn (Chương 1) |  |
| 3. Vũ Quang Huy | Tìm hiểu về hàm băm SHA-1-2-3 (Chương 2)  Tổng hợp nội dung word. |  |
| 4. Nguyễn Quỳnh Giao | Kiến thức cơ sở |  |
| 2 | 1. Nguyễn Hải Biên | Nghiên cứu, tìm hiểu hệ mã hóa khóa công khai (Chương 2)  Tìm hiều về công cụ NetBean | Hoàn thành |  |
| 2. Phạm Việt Đức | Tìm hiểu phương pháp mã hóa bất đối xứng ứng dụng chữ ký điện tử (Chương 2)  Tìm hiều về công cụ Visual Studio |  |
| 3. Vũ Quang Huy | Nghiên cứu, tìm hiểu chữ ký số, ứng dụng thực tế (Chương 2)   * Tìm hiều về công cụ Visual Studio |  |
| 4. Nguyễn Quỳnh Giao | Tìm hiểu phương pháp mã hóa RSA, thuật toán RSA (Chương 2) |  |
| 3 | 1. Nguyễn Hải Biên | * Thiết kế giao diện chương trình bằng Java | Hoàn thành |  |
| 2. Phạm Việt Đức | * Thiết kế kịch bản |  |
| 3. Vũ Quang Huy | * + Thiết kế giao diện chương trình bằng C# |  |
| 4. Nguyễn Quỳnh Giao | * + Giới thiệu ngôn ngữ lặp trình sử dụng cái đặt thuật toán |  |
| 4 | 1. Nguyễn Hải Biên | * Tạo chữ ký bằng Java | Hoàn thành |  |
| 2. Phạm Việt Đức | * Cài đặt thuật toán RSA và xác nhận chữ ký |  |
| 3. Vũ Quang Huy | * Tạo chữ ký bằng C# |  |
| 4. Nguyễn Quỳnh Giao | * Cài đặt thuật toán RSA và xác nhận chữ ký bằng Java |  |
| 5 | 1. Nguyễn Hải Biên | Kết luận kiến thức lĩnh hội  ( Chương 3)   * + Tổng hợp word, thực nghiệm bài báo cáo | Hoàn thành |  |
| 2. Phạm Việt Đức | * + Rút ra bài học kinh nghiệm |  |
| 3. Vũ Quang Huy | * + Hoàn thành báo cáo bản mềm, phiếu học tập, chương trình thực nghiệm. |  |
| 4. Nguyễn Quỳnh Giao | * + Đề xuất tính khả thi, khó khăn, thuận lợi của chủ đề nghiên cứu |  |

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: 20241IT6070001 Khóa: K17
3. Tên nhóm: Nhóm 9
4. Họ và tên thành viên trong nhóm:

Nguyễn Hải Biên

Phạm Việt Đức

Nguyễn Quỳnh Giao

Vũ Quang Huy

1. **Nội dung học tập**
2. Tên chủ đề: Tìm hiểu về hệ mật RSA và ứng dụng trong thực tế
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: Tìm tài liệu, nghiên cứu lý thuyết về an toàn bảo mật thông tin và mã hóa dữ liệu RSA
* Hoạt động/ Nội dung 2: Cài đặt thuật toán bằng ngôn ngữ C# và Java, xây dựng chương trình mô phỏng hoạt động mã hóa và giải mã RSA
* Hoạt động/ Nội dung 3: Viết báo cáo tổng kết

1. Sản phẩm nghiên cứu

* 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 (nếu có):

Máy tính, laptop.

**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: 20241IT6070001 Khóa: K17

Tên nhóm Nhóm 9

Tên chủ đề: Tìm hiểu về hệ mật RSA và ứng dụng trong thực tế

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | 1. Nguyễn Hải Biên | Giới thiệu, tìm hiểu về chữ ký số và mục đích đề tài (Chương 1) | - Hoàn thành |  |
| 2. Phạm Việt Đức | Tìm hiểu phương pháp, đối tượng nghiên cứu, ý nghĩa khoa học và thực tiễn (Chương 1) |  |
| 3. Vũ Quang Huy | Tìm hiểu về hàm băm SHA-1-2-3 (Chương 2)  Tổng hợp nội dung word. |  |
| 4. Nguyễn Quỳnh Giao | Kiến thức cơ sở |  |
| 2 | 1. Nguyễn Hải Biên | Nghiên cứu, tìm hiểu hệ mã hóa khóa công khai (Chương 2)  Tìm hiều về công cụ NetBean | Hoàn thành |  |
| 2. Phạm Việt Đức | Tìm hiểu phương pháp mã hóa bất đối xứng ứng dụng chữ ký điện tử (Chương 2)  Tìm hiều về công cụ Visual Studio |  |
| 3. Vũ Quang Huy | Nghiên cứu, tìm hiểu chữ ký số, ứng dụng thực tế (Chương 2)  Tìm hiều về công cụ Visual Studio |  |
| 4. Nguyễn Quỳnh Giao | Tìm hiểu phương pháp mã hóa RSA, thuật toán RSA (Chương 2) |  |
| 3 | 1. Nguyễn Hải Biên | Thiết kế giao diện chương trình bằng Java | Hoàn thành |  |
| 2. Phạm Việt Đức | Thiết kế kịch bản |  |
| 3. Vũ Quang Huy | Thiết kế giao diện chương trình bằng C# |  |
| 4. Nguyễn Quỳnh Giao | Giới thiệu ngôn ngữ lặp trình sử dụng cái đặt thuật toán |  |
| 4 | 1. Nguyễn Hải Biên | Tạo chữ ký bằng Java | Hoàn thành |  |
| 2. Phạm Việt Đức | Cài đặt thuật toán RSA và xác nhận chữ ký |  |
| 3. Vũ Quang Huy | Tạo chữ ký bằng C# |  |
| 4. Nguyễn Quỳnh Giao | Cài đặt thuật toán RSA và xác nhận chữ ký bằng Java |  |
| 5 | 1. Nguyễn Hải Biên | Kết luận kiến thức lĩnh hội  ( Chương 3)  Tổng hợp word, thực nghiệm bài báo cáo | Hoàn thành |  |
| 2. Phạm Việt Đức | Rút ra bài học kinh nghiệm |  |
| 3. Vũ Quang Huy | Hoàn thành báo cáo bản mềm, phiếu học tập, chương trình thực nghiệm. |  |
| 4. Nguyễn Quỳnh Giao | Đề xuất tính khả thi, khó khăn, thuận lợi của chủ đề nghiên cứu |  |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp