**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: 20222IT6001009 Khóa: 15

Tên nhóm:13

Họ tên các thành viên: Trương Công Mạnh, Nguyễn Văn Nguyên, Trần Hồng Nhung, Nguyễn Nam Phi, Nguyễn Thị Thu Phương

Tên chủ đề: Xây dựng chương trình mã hóa và giải mã RSA bằng C#, Java

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Kết quả đạt được** | **Kiến nghị với giảng viên hướng dẫn** |
| 1 | Trần Hồng Nhung Nguyễn Thị Thu Phương | Sự cần thiết của An toàn và bảo mật thông tin | Nêu được nhu cầu về an toàn bảo mật thông tin |  |
| An toàn và bảo mật thông tin | Nắm được các loại hình tấn công và cách bảo vệ |  |
| Trương Công Mạnh | Lý do chọn đề tài | Xây dựng chương trình mã hóa và giải mã RSA bằng Java, C# |  |
| Nội dung nghiên cứu | Nêu các hoạt động chính của trong quá trình thực hiện bài thực nghiệm |  |
| Các kiến thức cơ sở | Sử dụng được các thuật toán |  |
| Nguyễn Văn Nguyên Nguyễn Nam Phi | Các phương pháp mã hóa cổ điển | Nắm được các phương pháp |  |
| 2 | Trần Hồng Nhung Nguyễn Văn Nguyên Nguyễn Nam Phi | Nghiên cứu, tìm hiểu hệ mã hóa công khai | Hiểu về hệ mã hóa công khai |  |
| Trương Công Mạnh Nguyễn Thị Thu Phương | Nghiên cứu tìm hiểu về hệ mật mã RSA | Hiểu về hệ mật mã RSA |  |
| 3 | Nguyễn Văn Nguyên | Kiểm tra số nguyên tố | Nắm được các bước xây dựng thuật toán |  |
| Thuật toán Miller-Rabin | Nắm được các bước xây dựng thuật toán |  |
| Nguyễn Thị Thu Phương | Thuật toán Euclid | Nắm được các bước xây dựng thuật toán |  |
| Thuật toán Euclid mở rộng | Nắm được các bước xây dựng thuật toán |  |
| Nguyễn Nam Phi | Định lý Fermat | Nắm được các bước xây dựng thuật toán |  |
| Định lý Euler | Nắm được các bước xây dựng thuật toán |  |
| Trần Hồng Nhung | Thuật toán Bình phương và nhân | Nắm được các bước xây dựng thuật toán |  |
| Trương Công Mạnh | Thuật toán RSA | Nắm được các bước xây dựng thuật toán |  |
| 4 | Trần Hồng Nhung | Giới thiệu ngôn ngữ C# | Nêu được lý do chọn ngôn ngữ |  |
| Thiết kế kịch bản, giao diện chương trình | Xây dựng được các bước thực hiện và giao diện chương trình |  |
| Nguyễn Nam Phi | Mã hóa, giải mã, đọc ghi file | Thêm thành công vào chương trình |  |
| Nguyễn Thị Thu Phương | Tạo khóa, xử lí chức năng các nút | Thêm thành công vào chương trình |  |
| Nguyễn Văn Nguyên | Thiết kế kịch bản chương trình | Xây dựng được các bước thực hiện chương trình |  |
| Đọc ghi file, giải mã, xử lý chức năng các nút | Thêm thành công vào chương trình |  |
| Trương Công Mạnh | Giới thiệu ngôn ngữ Java | Nêu được lý do chọn ngôn ngữ |  |
| Thiết kế giao diện, tạo khóa, mã hóa, xử lý chức năng các nút | Thêm thành công vào chương trình |  |
| 5 | Cả nhóm | Kiến thức lĩnh hội |  |  |
| Cả nhóm | Bài học kinh nghiệm | Rút ra được các bài học |  |
| Cả nhóm | Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn | Nêu được những thuận lợi và khó khăn trong quá trình thực nghiệm |  |

Ngày …. tháng …. năm 2023

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp

**PHIẾU HỌC TẬP CÁ NHÂN/NHÓM**

1. **Thông tin chung**

Tên lớp: 20222IT6001009 Khóa: 15

Tên nhóm:13

Họ tên các thành viên: Trương Công Mạnh, Nguyễn Văn Nguyên, Trần Hồng Nhung, Nguyễn Nam Phi, Nguyễn Thị Thu Phương

1. **Nội dung học tập**
2. Tên chủ đề: Xây dựng chương trình mã hóa và giải mã RSA bằng C#, Java
3. Hoạt động của sinh viên

* Hoạt động/ Nội dung 1: Tìm tài liệu, nghiên cứu lý thuyết về an toàn bảo mật thông tin , Tìm hiểu về các thuật toán như: thuật toán Euclid, định lí Fermat, hàm số Euler, thuật toán Miller-Rabin, thuật toán RSA, thuật toán Bình phương và nhân, kiểm tra số nguyên tố
* Hoạt động/ Nội dung 2: Cài đặt thuật toán, xây dựng chương trình mô phỏng hoạt động xây dựng chương trình mã hóa và giải mã RSA bằng Java, C#
* Hoạt động/ Nội dung 3: Demo chương trình, làm slide toám tắt và viết báo cáo tổng kết

1. Sản phẩm nghiên cứu

* Báo cáo thực nghiệm
* Chương trình mô phỏng
* Slide tóm tắt báo cáo

1. **Nhiệm vụ học tập**
2. Hoàn thành Bài tập lớn theo đúng thời gian quy định (từ ngày 15/5/2023 đến ngày 17/6/2023)
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].TS. Phạm Văn Hiệp – Bài giảng, tài liệu môn An toàn bảo mật thông tin – Đại học Công nghiệp Hà Nội.

[2]. Tài liệu điện tử trên Internet.

[3]. 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: 20222IT6001009 Khóa: 15

Họ và tên sinh viên: Trương Công Mạnh, Nguyễn Văn Nguyên, Trần Hồng Nhung, Nguyễn Nam Phi, Nguyễn Thị Thu Phương

Tên nhóm:13

Tên chủ đề: Xây dựng chương trình mã hóa và giải mã RSA bằng C#, Java

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| 1 | Trần Hồng Nhung Nguyễn Thị Thu Phương | Sự cần thiết của An toàn và bảo mật thông tin | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| An toàn và bảo mật thông tin | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Trương Công Mạnh | Lý do chọn đề tài | Word |
| Nội dung nghiên cứu | Word |
| Các kiến thức cơ sở | Word |
| Nguyễn Văn Nguyên Nguyễn Nam Phi | Các phương pháp mã hóa cổ điển | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| 2 | Trần Hồng Nhung Nguyễn Văn Nguyên Nguyễn Nam Phi | Nghiên cứu, tìm hiểu hệ mã hóa công khai | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Trương Công Mạnh Nguyễn Thị Thu Phương | Nghiên cứu tìm hiểu về hệ mật mã RSA | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| 3 | Nguyễn Văn Nguyên | Kiểm tra số nguyên tố | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Thuật toán Miller-Rabin | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Nguyễn Thị Thu Phương | Thuật toán Euclid | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Thuật toán Euclid mở rộng | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Nguyễn Nam Phi | Định lý Fermat | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Định lý Euler | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Trần Hồng Nhung | Thuật toán Bình phương và nhân | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| Trương Công Mạnh | Thuật toán RSA | Tra cứu Internet, tài liệu tham khảo giảng viên cung cấp |
| 4 | Trần Hồng Nhung | Giới thiệu ngôn ngữ C# | Tra cứu Internet |
| Thiết kế kịch bản, giao diện chương trình | Vistudio 2019 |
| Nguyễn Nam Phi | Mã hóa, giải mã, đọc ghi file | Vistudio 2019 |
| Nguyễn Thị Thu Phương | Tạo khóa, xử lí chức năng các nút | Vistudio 2019 |
| Nguyễn Văn Nguyên | Thiết kế kịch bản chương trình | Word |
| Đọc ghi file, giải mã, xử lý chức năng các nút | Esclip, Netbean |
| Trương Công Mạnh | Giới thiệu ngôn ngữ Java | Tra cứu Internet |
| Thiết kế giao diện, tạo khóa, mã hóa, xử lý chức năng các nút | Esclip, Netbean |
| 5 | Cả nhóm | Kiến thức lĩnh hội | Word |
| Cả nhóm | Bài học kinh nghiệm | Word |
| Cả nhóm | Đề xuất về tính khả thi của chủ đề nghiên cứu, những thuận lợi, khó khăn | Word |

Ngày …. tháng …. năm 2023

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp