**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: *20241IT6001002*Khóa: K17

Tên nhóm: 07

Họ và tên sinh viên:

1. Nguyễn Tấn Dũng (2021607770)

2. Bùi Xuân An (2022600964)

3. Phạm Văn Hiếu (2021601595)

4. Nguyễn Ba Duy (2022600906)

Tên chủ đề: ***Tìm hiểu về sơ đồ chữ ký Schnorr và viết ứng dụng minh họa (Sử dụng ngôn ngữ Java, 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 | Cả nhóm | Tìm hiểu sơ lược về Sơ đồ chữ ký Schnorr | Xây dựng bố cục đề tài  Các thông tin chung về sơ đồ chữ ký Schnorr |  |
| Nguyễn Tấn Dũng  Phạm Văn Hiếu | Tìm hiểu cú pháp và các thư viện sử dụng ngôn ngữ C# | Học tập cú pháp của ngôn ngữ được phân công |
| Bùi Xuân An  Nguyễn Ba Duy | Tìm hiểu cú pháp và các thư viện sử dụng ngôn ngữ Java |
| 2 | Nguyễn Ba Duy | Tìm hiểu Tổng quan về an toàn bảo mật thông tin | Hoàn thiện nội dung chương I. Tổng quan |  |
| Phạm Văn Hiếu | Tìm hiểu chữ ký số và vai trò trong an toàn bảo mật thông tin |
| Bùi Xuân An | Thách thức và giải pháp an toàn bảo mật |
| Bùi Xuân An | Giới thiệu ngôn ngữ sử dụng |
| Nguyễn Tấn Dũng | Tìm hiểu kiến thức cơ sở về toán học |
| Nguyễn Tấn Dũng | Tìm hiểu kiến thức cơ sở về thuật toán xây dựng trong Sơ đồ chữ ký Schnorr |
| 3 | Nguyễn Tấn Dũng | Tìm hiểu nguyên lý hoạt động của sơ đồ chữ ký Schnorr | Hoàn thiện chương II. Kết quả |  |
| Bùi Xuân An | Thiết kế kịch bản chương trình |
| Bùi Xuân An | Phân tích ưu nhược điểm của sơ đồ chữ ký Schnorr |
| Phạm Văn Hiếu | Cài đặt giao diện chương trình C# |
| Nguyễn Ba Duy | Cài đặt giao diện chương trình Java |
| Nguyễn Tấn Dũng | Tìm hiểu về các thư viện, công cụ sử dụng cho chương trình C# |
| Bùi Xuân An | Tìm hiểu về các thư viện, công cụ sử dụng cho chương trình Java |
| 4 | Nguyễn Tấn Dũng | Thiết kế logic Tạo khóa và tạo chữ ký (C#) | Cài đặt chương trình thành công và cập nhật nội dung giải thuật |  |
| Phạm Văn Hiếu | Thiết kế logic xác minh chữ ký (C#) |
| Nguyễn Ba Duy | Thiết kế logic tạo khóa |
| Nguyễn Ba Duy | Thiết kế logic tạo chữ ký và xác minh chữ ký (C#) |
| 5 | Cả nhóm | Cài đặt các chức năng khuyến nghị từ GVHD | Hoàn thiện các sản phẩm và báo cáo |  |
| Nguyễn Tấn Dũng | Viết nội dung Chương 3 Tổng Kết |
| Bùi Xuân An | Kiểm định lại định dạng bài tập lớn |
| Nguyễn Ba Duy | Kiểm thử lại chương trình minh họa (Java) |
| Phạm Văn Hiếu | Kiểm thử lại chương trình minh họa (C#) |

Ngày 25 tháng 10 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**

Tên lớp: *20241IT6001002*Khóa: K17

Tên nhóm: 07

Họ và tên sinh viên:

1. Nguyễn Tấn Dũng (2021607770) 3. Phạm Văn Hiếu (2021601595)

2. Bùi Xuân An (2022600964) 4. Nguyễn Ba Duy (2022600906)

1. **Nội dung học tập**
2. Tên chủ đề: ***Tìm hiểu về sơ đồ chữ ký Schnorr và viết ứng dụng minh họa (Sử dụng ngôn ngữ Java, C#)***
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 sơ đồ chữ ký Schnorr
* Hoạt động/ Nội dung 2: Cài đặt thuật toán, xây dựng chương trình mô phỏng hoạt động của sơ đồ chữ ký Schnorr
* 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: *20241IT6001002*Khóa: K17

Tên nhóm: Nhóm 07

Tên chủ đề: ***Tìm hiểu về sơ đồ chữ ký Schnorr và viết ứng dụng minh họa (Sử dụng ngôn ngữ Java, C#)***

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| 1 | Cả nhóm | Tìm hiểu sơ lược về Sơ đồ chữ ký Schnorr | Nghiên cứu các nguồn thông tin |
| Nguyễn Tấn Dũng  Phạm Văn Hiếu | Tìm hiểu cú pháp và các thư viện sử dụng ngôn ngữ C# | Tham khảo tài liệu của ngôn ngữ và các diễn đàn |
| Bùi Xuân An  Nguyễn Ba Duy | Tìm hiểu cú pháp và các thư viện sử dụng ngôn ngữ Java |
| 2 | Nguyễn Ba Duy | Tìm hiểu Tổng quan về an toàn bảo mật thông tin | Tham khảo tài liệu |
| Phạm Văn Hiếu | Tìm hiểu chữ ký số và vai trò trong an toàn bảo mật thông tin |
| Bùi Xuân An | Thách thức và giải pháp an toàn bảo mật |
| Bùi Xuân An | Giới thiệu ngôn ngữ sử dụng |
| Nguyễn Tấn Dũng | Tìm hiểu kiến thức cơ sở về toán học |
| Nguyễn Tấn Dũng | Tìm hiểu kiến thức cơ sở về thuật toán xây dựng trong Sơ đồ chữ ký Schnorr |
| 3 | Nguyễn Tấn Dũng | Tìm hiểu nguyên lý hoạt động của sơ đồ chữ ký Schnorr | Nghiên cứu tài liệu, định nghĩa lại tên biến phù hợp, cải tiến thuật toán |
| Bùi Xuân An | Thiết kế kịch bản chương trình | Đánh giá, xây dựng kịch bản |
| Bùi Xuân An | Phân tích ưu nhược điểm của sơ đồ chữ ký Schnorr | So sánh, phân tích các mô hình |
| Phạm Văn Hiếu | Cài đặt giao diện chương trình C# | Cài đặt thực nghiệm |
| Nguyễn Ba Duy | Cài đặt giao diện chương trình Java |
| Nguyễn Tấn Dũng | Tìm hiểu về các thư viện, công cụ sử dụng cho chương trình C# | Nghiên cứu tài liệu |
| Bùi Xuân An | Tìm hiểu về các thư viện, công cụ sử dụng cho chương trình Java |
| 4 | Nguyễn Tấn Dũng | Thiết kế logic Tạo khóa và tạo chữ ký (C#) | Thiết kế giải thuật và cài đặt thực nghiệm |
| Phạm Văn Hiếu | Thiết kế logic xác minh chữ ký (C#) |
| Nguyễn Ba Duy | Thiết kế logic tạo khóa |
| Nguyễn Ba Duy | Thiết kế logic tạo chữ ký và xác minh chữ ký (C#) |
| 5 | Cả nhóm | Cài đặt các chức năng khuyến nghị từ GVHD | Tiếp thu cải tiến chương trình |
| Nguyễn Tấn Dũng | Viết nội dung Chương 3 Tổng Kết | Kiểm tra nội dung theo các tiêu chí đánh giá và quy định về định dạng |
| Bùi Xuân An | Kiểm định lại định dạng bài tập lớn |
| Nguyễn Ba Duy | Kiểm thử lại chương trình minh họa (Java) | Kiểm nghiệm, thẩm định lại chương trình dựa trên những tiêu chí đánh giá, xác định tính hoạt động của các ngoại lệ, các lỗi nhập xuất,… và thực hiện kiểm thử. |
| Phạm Văn Hiếu | Kiểm thử lại chương trình minh họa (C#) |

Ngày 25 tháng 10 năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp