**BÁO CÁO HỌC TẬP CÁ NHÂN/ NHÓM**

Tên lớp: An toàn và bảo mật thông tin - 20241IT6001002 Khóa: K16

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

1. Mầu Lê Hiệp - 2021600082
2. Trần Đức Hoàng - 2021605654
3. Nguyễn Quang Hà Phương - 2022602592
4. Nguyễn Nhật Quang - 2021601647
5. Hoàng Quốc Quý - 2021602668

Tên nhóm: Nhóm 10

Tên chủ đề: Xây dựng chương trình mã hóa và giải mã RSA (Sử dụng ngôn ngữ C++, C#)

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| 1 | Mầu Lê Hiệp | - Tìm hiểu về đề tài và thuật toán Elgamal cần thực hiện.  - Lên kế hoạch làm việc nhóm, xác định các công việc cho tuần đầu tiên. | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Thông qua các cuộc họp, tham khảo ý kiến thành viên để phân công công việc |
| Trần Đức Hoàng | - Tìm hiểu về cơ sở toán học  - Nghiên cứu các khái niệm: số nguyên tố, nguyên tố cùng nhau, modulo, Hàm EULER, … | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Nguyễn Quang Hà Phương | - Tìm hiểu về hệ mật mã và an toàn bảo mật thông tin | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Nguyễn Nhật Quang | - Nghiên cứu các thành phần của hệ mật mã, phân loại hệ mật mã | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Hoàng Quốc Quý | - Tìm hiểu chung về chữ ký điện tử Elgamal | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| 2 | Mầu Lê Hiệp | - Tìm hiểu về đề tài và thuật toán Elgamal cần thực hiện.  - Lên kế hoạch làm việc nhóm, xác định các công việc cho tuần đầu tiên. | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Thông qua các cuộc họp, tham khảo ý kiến thành viên để phân công công việc |
| Trần Đức Hoàng | - Tìm hiểu về cơ sở toán học  - Nghiên cứu các khái niệm: số nguyên tố, nguyên tố cùng nhau, modulo, Hàm EULER, … | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Nguyễn Quang Hà Phương | - Tìm hiểu về hệ mật mã và an toàn bảo mật thông tin | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Nguyễn Nhật Quang | - Nghiên cứu các thành phần của hệ mật mã, phân loại hệ mật mã | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Hoàng Quốc Quý | - Tìm hiểu chung về chữ ký điện tử Elgamal | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| 3 | Mầu Lê Hiệp | - Nghiên cứu và tìm hiểu: [Thuật toán Euclid tìm ước chung lớn nhất](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.gmqlan27d3vu), [Thuật toán Euclid mở rộng tìm phần tử nghịch đảo](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.6hnxqlstv1pn)  - Nghiên cứu p[hương pháp tấn công](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.s1a11qvb3baz) | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Thông qua các cuộc họp, tham khảo ý kiến thành viên để phân công công việc |
| Trần Đức Hoàng | - Nghiên cứu [Định lí Ferma](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.4t6p08dp2ccw)  - [Đánh giá độ phức tạp của thuật toán](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.4rmk5m53jmkq) | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Nguyễn Quang Hà Phương | - Nghiên cứu [Định lí Eule](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.e1t9tqb3n7zf)  - Tìm hiểu về [Hướng phát triển](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.jdqcicc7jm4c) | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Nguyễn Nhật Quang | - Nghiên cứu [Thuật toán Miller - Rabin](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.g2s2otr1461k)  -Tìm hiểu ư[u điểm và nhược điểm của hệ mã RSA](https://docs.google.com/document/d/1ChI5j7Ehks6nrDyFY-8tdLSPuWIG84LAzXarTiK-030/edit?tab=t.0#heading=h.2qzm22si82kr) | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| Hoàng Quốc Quý |  | - Nghiên cứu giáo trình An toàn và bảo mật thông tin  - Tìm hiểu các thông tin kiến thức trên Internet. |
| 4 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |
| 5 | A  B  C  D  E | Công việc 1  Công việc 2  Công việc 3  Công việc 4  Công việc 5 |  |

Ngày …. tháng …. năm 2024

XÁC NHẬN CỦA GIẢNG VIÊN

(Ký, ghi rõ họ tên)

Phạm Văn Hiệp