

# CÁC NHÓM PROJECTS

1. Số nguyên tố chuyên về thuật toán  
Miller – Rabin và AKS:

- Phạm Anh Tuấn: Nhóm trưởng
- Trần Tuấn Bình
- Trần Gia Khánh

***Báo cáo vào ngày 19/11/2025***

*Nhận xét nhóm*

2. Hệ mật RSA và sơ đồ chữ ký RSA:

- Nguyễn Thị Vân Anh: Nhóm trưởng
- Hoàng Thành Đạt
- Võ Minh Dũng
- ***Báo cáo vào ngày 19/11/2025***

Nhận xét nhóm 5

### 3. Hệ mật ElGamal và sơ đồ chữ ký ElGamal:

- Nguyễn Nam Khánh: Trưởng nhóm
- Nguyễn Văn Bản
- Phạm Mai Anh
- ***Báo cáo vào ngày 19/11/2025***

#### Nhận xét Nhóm 2

### 4. Xây dựng đường cong Elliptic với độ dài khóa 256 bit trở lên

- Vũ Thanh Tùng: Trưởng nhóm
- Nguyễn Quang Vinh
- Đặng Anh Quế
- ***Báo cáo vào ngày 19/11/2025***

#### Nhận xét Nhóm 3

## 5. Nhóm Bitcoin:

- Đào Thị Thu Hường: Trưởng nhóm
- Nguyễn Đức Huy
- Nguyễn Thu Hà (4/9/2004)
- ***Báo cáo vào ngày 19/11/2025***

## Nhận xét nhóm 4

## 6. Nhóm Xây dựng chữ ký tốc độ cao:

- Lê Đức Hoàng Anh: Trưởng nhóm
- Nguyễn Hải Nam: Phó nhóm
- Ngô Đăng Quyết: Nhóm viên

## 7. Hệ mật RSA và sơ đồ chữ ký RSA thứ 2:

- Nguyễn Thị Huyền: Trưởng nhóm

8. Tổng quan về Mật mã Hậu lượng tử  
và 1 Hệ mật Hậu lượng tử:

Nông Sơn Tùng và Ngô Đức Thịnh  
***Báo cáo vào ngày 26/11/2025***

Nhận xét nhóm 13

9. Mã hóa đồng cấu: Nguyễn An Minh

10. Hệ mật hậu lượng tử trên lưới:  
Hoàng Duy Anh, Nguyễn Mạnh  
Quỳnh

***Báo cáo vào ngày 26/11/2025***

Nhận xét nhóm 8

11. Hệ mật hậu lượng tử dựa trên hàm  
băm: Lê Anh Dũng, Lê Thị Hoàng  
Linh

***Báo cáo vào ngày 26/11/2025***

Nhận xét nhóm 10

12. Hệ mật Hậu lượng tử dựa trên code:  
Nguyễn Thị Thanh Tuyền, Đỗ Khôi  
Nguyễn

***Báo cáo vào ngày 26/11/2025***

Nhận xét nhóm 11

13. Đường cong Elliptic Edward:  
Nguyễn Nhất Huy, Nguyễn Đức  
Thành, Trịnh Hải Tiến

***Báo cáo vào ngày 26/11/2025***

Nhận xét nhóm 12

14. Chủ đề bài báo đã giao và Lập trình:  
Nguyễn Ngọc Duy, Nguyễn Đình  
Bình
15. Chủ đề dịch bài báo và Lập trình:  
Trương Thi Xuân Sang, Tạ Việt  
Hùng
16. Chủ đề dịch báo và Lập trình: Phạm  
Hữu Mạnh, Nguyễn Thu Hà,  
Nguyễn Xuân Trường Khải