BÁO CÁO BÀI TẬP

**Môn học: CRYPTOGRAPHY – Mật mã học**

**Tên chủ đề: TRAO ĐỔI KHOÁ ECDH**

*GVHD: Nguyễn Ngọc Tự*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: **NT219.N21.ANTT.1**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Lê Đoàn Trà My | 21521149 | 21521149@gm.uit.edu.vn |
| 2 | Nguyễn Thị Thanh Mai | 21521112 | 21521112@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Trao đổi ECDH | 100% | 2 - 4 |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

***\* Chuẩn bị, thiết lập hệ thống trong quá trình thực hiện Trao đổi khoá ECDH:***

- Đối tượng tham gia trao đổi: Trà My, Thanh Mai.

- Curve sử dụng: Curve384.

- Thiết lập hệ thống: Sử dụng 1 phần thành phẩm của Lab03 Lập trình Mạng căn bản để xây dựng Server lắng nghe, sử dụng Telnet client để kết nối với Server và trao đổi thông tin với bạn.

***\* Các bước thực hiện:***

*Bước 1:*Khởi tạo điểm G dựa trên curve384 với các thông số p, a, b, G(x, y), n, h nhập thủ công (các thông số ở dạng hexadecimal – thập lục phân).

***A screenshot of a computer

Description automatically generated with low confidence***

*Hình 1. Các thông số p, a, b, G(x, y), n, h được nhập thủ công trong code thực hiện*

*Bước 2****:*** Chọn/Tạo một số bí mật r1 (PrivateKey) và tiến hành tính toán toạ độ điểm (toạ độ PublicKey), với: PublicKey = PrivateKey \* G

***A screenshot of a computer code

Description automatically generated with low confidence***

*Hình 2. Đoạn code nhập PrivateKey r1 và tính toán, in ra màn hình toạ độ của PublicKey*

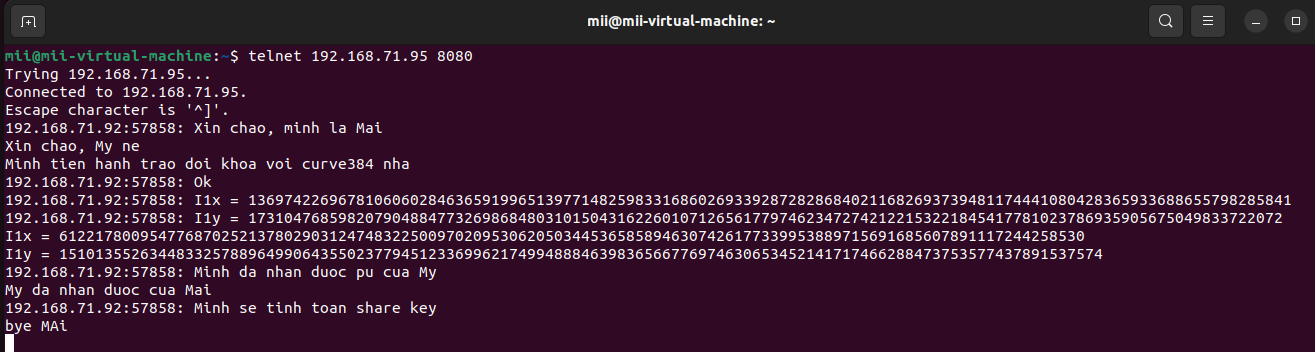
**A picture containing text, screenshot, font

Description automatically generated**

*Hình 3. Kết quả thực hiện đoạn code, in ra các thông số và kết quả tính toán PublicKey*

*Bước 3****:*** Trao đổi PublicKey với bạn (Thanh Mai) qua Telnet với Server được xây dựng từ 1 phần bài làm Lab03 Lập trình Mạng căn bản.

(*Link code Server:* [*https://drive.google.com/drive/folders/1FVC\_GmxLTNRuVMBnOjsndDausT1iGD5c*](https://drive.google.com/drive/folders/1FVC_GmxLTNRuVMBnOjsndDausT1iGD5c) )

****

*Hình 4. Kết nối tới Server 192.168.71.95 - port:8080 và trao đổi PublicKey với partner qua telnet*

A screenshot of a computer

Description automatically generated

*Hình 5. Thông tin hiển thị trên Server khi tiến hành kết nối và giao tiếp giữa 2 client*

*(Trà My vừa xây dựng Server vừa là Client kết nối tới Server để giao tiếp với Client khác (Thanh Mai), chúng em giao tiếp trong môi trường mạng LAN)*

- PublicKey nhận được từ Thanh Mai:



*Bước 4****:*** Tiến hành tính toán Khoá phiên ShareKey dựa trên PublicKey nhận từ Thanh Mai và PrivateKey bản thân (ShareKey = PublicKey(TMai) \* PrivateKey (TMy))

A screenshot of a computer

Description automatically generated with low confidence

*Hình 6. Đoạn code nhập thủ công PublicKey của Mai, tính toán ShareKey và in ra màn hình*

**A screenshot of a computer

Description automatically generated**

*Hình 7. Kết quả đoạn code, in ra các thông số, PrivateKey của bản thân, PublicKey của 2 bên và ShareKey*

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)