ĐỒ ÁN 2 - DIFFIE HELLMAN

1 Diffie Hellman trên trường số nguyên tố (5 điểm)

Nhắc lại, phần tử g trong nhóm $\mathbb{Z}_p^*$ với p là số nguyên tố lớn được gọi là phần tử sinh nếu nó thoả tính chất sau:

$$\forall x \in [1, p-2],\ g^x \neq 1 \pmod{p}.$$

Cho một số nguyên tố p lớn và một số nguyên dương g là phần tử sinh trong nhóm $\mathbb{Z}_p^*$. Alice và Bob thực hiện giao thức trao đổi khóa Diffie Hellman lần lượt theo các bước như sau:

1. Alice chọn ngẫu nhiên một số nguyên dương bí mật là $a \in \mathbb{Z}_p^*$ và gửi cho Bob giá trị công khai $A = g^a \pmod{p}$.
2. Bob chọn ngẫu nhiên một số nguyên dương bí mật là $b \in \mathbb{Z}_p^*$ và gửi cho Alice giá trị công khai $B = g^b \pmod{p}$.
3. Với giá trị bí mật a của Alice và giá trị công khai $B = g^b \pmod{p}$ của Bob, Alice thu được khóa bí mật chung là $K = B^a = g^{ab} \pmod{p}$.
4. Tương tự, Bob cũng thu được khóa bí mật chung là $K = A^b = g^{ab} \pmod{p}$.

1.1 Yêu cầu bài toán

Trong phần này, sinh viên được yêu cầu thiết kế một chương trình dùng để tính khoá bí mật chung của Alice và Bob sau khi thực hiện giao thức Diffie Hellman. Chương trình phải đảm bảo các yêu cầu sau:

- Sử dụng ngôn ngữ lập trình C++. Mọi ngôn ngữ lập trình khác nếu sinh viên sử dụng đều không được chấp nhận và sẽ nhận điểm 0 trong bài tập này.
- Chỉ được sử dụng các thư viện tiêu chuẩn có sẵn từ phiên bản C++17 trở xuống. Mọi thư viện khác nếu sinh viên cố ý sử dụng trong bài làm đều sẽ nhận điểm 0 trong bài tập này.
- Toàn bộ mã nguồn cho chương trình phải nằm trong một file duy nhất, đặt tên là `bai1.cpp`.
- Sau khi biên dịch mã nguồn thành file `a.exe`, chương trình phải được chạy thông qua lệnh sau:

  ```
  $ .\a.exe test.inp test.out
  ```

  Với `test.inp` là file chứa dữ liệu đầu vào, và `test.out` là file chứa kết quả đầu ra của chương trình.
- Thời gian chạy tối đa cho mỗi test case là **60 giây**. Sau thời gian này, bài làm của bạn sẽ bị dừng và test case đó không được tính điểm.

1.2 Các file chương trình

- File `test.inp` bao gồm 3 dòng. Dòng thứ nhất chứa 2 số nguyên dương lần lượt là số nguyên tố p và phần tử sinh g trong nhóm $\mathbb{Z}_p^*$. Dòng thứ hai chứa một số nguyên dương là giá trị bí mật $a \in \mathbb{Z}_p^*$ của Alice. Dòng thứ ba chứa một số nguyên dương là giá trị bí mật $b \in \mathbb{Z}_p^*$ của Bob. Tất cả các giá trị trên đều được lưu bằng các chữ số thập lục phân in hoa dưới dạng big endian.
- Kết quả sau khi chạy chương trình sẽ được lưu trong file `test.out`. File này chứa 1 số nguyên dương duy nhất là khoá bí mật chung $K = g^{ab} \pmod p$ của Alice và Bob, được lưu bằng các chữ số thập lục phân in hoa dưới dạng big endian.

1.3 Ví dụ

test.inp	test.out
65 1D 12 21	55

Giải thích: Có `0x65 = 101, 0x1D = 29, 0x12 = 18, 0x21 = 33`. Khi đó, với $p = 101$ ta tính được khoá bí mật chung $K = g^{ab} = 29^{18\times 33} = 85 =$ `0x55` (mod 101).

test.inp	test.out
67 2B 1A 41	13

Giải thích: Có `0x67 = 103, 0x2B = 43, 0x1A = 26, 0x41 = 65`. Khi đó, với $p = 103$ ta tính được khoá bí mật chung $K = g^{ab} = 43^{26\times 65} = 19 =$ `0x13` (mod 103).

1.4 Ràng buộc

- $g, a, b \in \mathbb{Z}_p^*$.
- 40% số test ứng với 40% số điểm thoả mãn độ dài của p tính theo bit nhỏ hơn hoặc bằng 64 bit, kí hiệu $|p| \leq 64$.
- 40% số test ứng với 40% số điểm thoả mãn $64 < |p| \leq 128$.
- 10% số test ứng với 10% số điểm thoả mãn $128 < |p| \leq 256$.
- 10% số test ứng với 10% số điểm thoả mãn $256 < |p| \leq 512$.

2 Diffie Hellman trên đường cong Elliptic (5 điểm)

Cho số nguyên tố p lớn, ta định nghĩa đường cong elliptic ở dạng $(EC) : y^2 = x^3 + ax + b$ $(a, b \in \mathbb{F}_p)$ với a, b là hằng số được cho trước thoả $4a^3 + 27b^2 \neq 0$. Đặt $E(a, b, p) = \{(x, y) \in (EC) : y^2 = x^3 + ax + b \in \mathbb{F}_p\}$ là tập hợp các điểm nằm trên đường cong elliptic với hệ số a, b cho trước. Từ đó, ta định nghĩa phép cộng $+$ trên tập $E(a, b, p)$ như sau:

- $+ : E(a, b, p) \times E(a, b, p) \to E(a, b, p)$ biểu diễn ánh xạ của 1 phép đóng, nghĩa là khi ta thực hiện phép $+$ trên 2 điểm $P, Q \in E(a, b, p)$, kết quả của phép tính là điểm $R \in E(a, b, p)$.
- Ta thêm điểm "vô cực" $\mathcal{O}$ vào tập $E(a, b, p)$ thoả $\forall P \in E(a, b, p)$ thì $P + \mathcal{O} = \mathcal{O} + P = P$.

  $\to \mathcal{O}$ là một phần tử đơn vị trong tập $E(a, b, p)$.
- Phần tử nghịch đảo của P, kí hiệu là $-P$, là điểm đối xứng với P qua trục hoành.

Gọi $P, Q \in E(a, b, p)$ thì phép cộng $R = P + Q$ được thực hiện theo các bước như sau:

1. Tìm $(d) : y = cx + d$ là đường thẳng đi qua 2 điểm P, Q.
2. Tìm điểm Y là giao điểm giữa đường cong (EC) và đường thẳng (d).
3. Vậy, $R = P + Q = -Y$ là kết quả sau khi thực hiện phép cộng trên đường cong elliptic, hay tập $E(a, b, p)$.

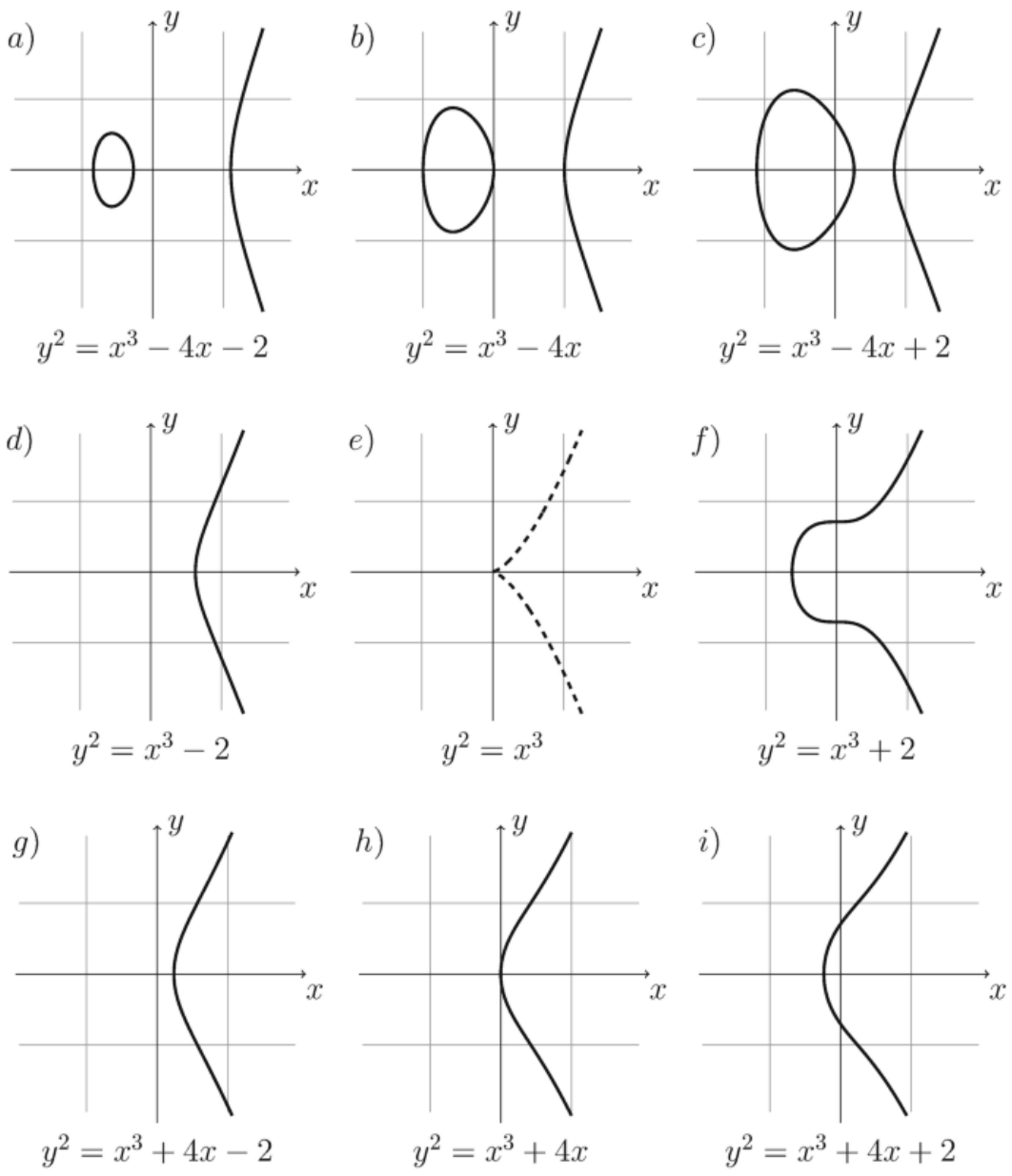
Với việc đặt hệ số a, b thoả $4a^3 + 27b^2 \neq 0$ thì đường thẳng (d) đi qua 2 điểm P, Q khả năng rất cao sẽ cắt đường cong elliptic tại điểm thứ ba Y khác với điểm P và điểm Q. Trường hợp đường thẳng (d) song song với trục tung, nghĩa là P và Q đối xứng với nhau qua trục hoành, thì đường thẳng (d) sẽ cắt đường cong tại điểm "vô cực" $\mathcal{O}$. Do vậy, $R = -\mathcal{O}$ là kết quả của phép tính $P + Q$ khi P và Q đối xứng với nhau qua trục hoành.

- Dễ thấy việc định nghĩa $\mathcal{O}$ như phần tử đơn vị là hợp lý, vì $P + \mathcal{O} = P \Leftrightarrow P + (-P) = -\mathcal{O} \Leftrightarrow P + Q = -\mathcal{O}$.
- Trong trường hợp ta cần tính $2P = P + P$ thì đường thẳng (d) mà ta cần tìm sẽ là tiếp tuyến của đường cong (EC) tại điểm P, sau đó ta thực hiện các bước tiếp theo như bình thường.

Sau khi hoàn thành định nghĩa về đường cong elliptic (EC) và phép tính $+$ trên đường cong, ta thấy $(E(a, b, p), +)$ tạo thành một nhóm abel. Do vậy, khi đề cập đến bài toán log rời rạc trên nhóm $\mathbb{Z}_p^*$, ta có thể chuyển thành định nghĩa của bài toán log rời rạc trên đường cong elliptic như sau:

Định nghĩa 2.1 *Cho đường cong elliptic (EC) trên trường hữu hạn $\mathbb{F}_p$, điểm $Q \in (EC)$ và phần tử sinh $G \in (EC)$. Bài toán log rời rạc trên đường cong elliptic yêu cầu tìm một số nguyên dương $x \in \mathbb{Z}_p^*$ thoả $Q = xG = G + G + ... + G$ (x lần), giả sử luôn tồn tại ít nhất 1 nghiệm cho phương trình trên.*

- Bài toán này được xem là khó (không thể giải được bằng thuật toán chạy với thời gian đa thức) nếu p là số nguyên tố lớn (ví dụ, $p \geq 2^{256}$).



Hình 1: Một số biểu diễn đồ thị cho đường cong elliptic, trong đó đường cong $y^2 = x^3$ không phải là đường cong elliptic

2.1 Yêu cầu bài toán

Trong phần này, sinh viên được yêu cầu thiết kế một chương trình dùng để tính $R = P + Q$ với hai điểm $P, Q \in (EC)$ cho trước. Chương trình phải đảm bảo các yêu cầu sau:

- Sử dụng ngôn ngữ lập trình C++. Mọi ngôn ngữ lập trình khác nếu sinh viên sử dụng đều không được chấp nhận và sẽ nhận điểm 0 trong bài tập này.
- Chỉ được sử dụng các thư viện tiêu chuẩn có sẵn từ phiên bản C++17 trở xuống. Mọi thư viện khác nếu sinh viên cố ý sử dụng trong bài làm đều sẽ nhận điểm 0 trong bài tập này.
- Toàn bộ mã nguồn cho chương trình phải nằm trong một file duy nhất, đặt tên là `bai2.cpp`.
- Sau khi biên dịch mã nguồn thành file `a.exe`, chương trình phải được chạy thông qua lệnh sau:

  ```
  $ .\a.exe test.inp test.out
  ```

  Với `test.inp` là file chứa dữ liệu đầu vào, và `test.out` là file chứa kết quả đầu ra của chương trình.
- Thời gian chạy tối đa cho mỗi test case là **60 giây**. Sau thời gian này, bài làm của bạn sẽ bị dừng và test case đó không được tính điểm.

2.2 Các file chương trình

- File `test.inp` bao gồm 3 dòng. Dòng thứ nhất chứa ba số nguyên dương lần lượt là số nguyên tố p và hệ số a, b để định nghĩa đường cong elliptic. Dòng thứ hai chứa hai số nguyên dương biểu diễn điểm $P \in (EC)$, bao gồm lần lượt là hoành độ x_P và tung độ y_P. Dòng thứ ba chứa hai số nguyên dương biểu diễn điểm $Q \in (EC)$, bao gồm lần lượt là hoành độ x_Q và tung độ y_Q. Tất cả giá trị trên được lưu bằng các chữ số thập lục phân in hoa dưới dạng big endian.
- Kết quả sau khi chạy chương trình sẽ được lưu trong file `test.out`. File này chứa hai số nguyên dương biểu diễn điểm $R = P + Q$ bao gồm lần lượt là hoành độ x_R và tung độ y_R, được lưu bằng các chữ số thập lục phân in hoa dưới dạng big endian.

2.3 Ví dụ

test.inp	test.out
7CF 724 68B 212 1CF 6EB 31	440 D0

Giải thích: Có $p = \texttt{0x7CF} = 1999$, $(EC) : y^2 = x^3 + ax + b \pmod p = x^3 + 1828x + 1675 \pmod{1999}$ với $a = \texttt{0x724} = 1828$ và $b = \texttt{0x68B} = 1675$, $P = (x_P, y_P) = (\texttt{0x212}, \texttt{0x1CF}) = (530, 463)$, $Q = (x_Q, y_Q) = (\texttt{0x6EB}, \texttt{0x31}) = (1771, 49)$. Vậy, ta tính được $R = P + Q = (1088, 208) = (\texttt{0x440}, \texttt{0xD0})$.

test.inp	test.out
C95 605 537 B52 1B7 B52 1B7	B94 BA1

Giải thích: Có $p = \texttt{0xC95} = 3221$, $(EC) : y^2 = x^3 + ax + b \pmod p = x^3 + 1541x + 1335 \pmod{3221}$ với $a = \texttt{0x605} = 1541$ và $b = \texttt{0x537} = 1335$, $P = Q = (x_P, y_P) = (\texttt{0xB52}, \texttt{0x1B7}) = (2898, 439)$. Vậy, ta tính được $R = P + Q = (2964, 2977) = (\texttt{0xB94}, \texttt{0xBA1})$.

2.4 Ràng buộc

- $a, b \in \mathbb{Z}_p^*$.
- **Tất cả các test sẽ đảm bảo đầu vào và đầu ra không bao gồm điểm "vô cực" $\mathcal{O}$.**
- 50% số test ứng với 50% số điểm thoả mãn độ dài của p tính theo bit nhỏ hơn hoặc bằng 64 bit, kí hiệu $|p| \leq 64$.
- 30% số test ứng với 30% số điểm thoả mãn $64 < |p| \leq 128$.
- 20% số test ứng với 20% số điểm thoả mãn $128 < |p| \leq 256$.

3 Các quy định khác về đồ án

- Đồ án này được thực hiện cá nhân. Nếu phát hiện bất kì hành vi sao chép bài nào của các bạn cùng môn học, toàn bộ phần điểm thực hành của những sinh viên có liên quan sẽ được đưa về 0.
- Thời gian thực hiện là 2 tuần tính từ lúc đồ án được chính thức đăng lên trên hệ thống quản lý môn học Moodle.
- Cấu trúc file để nộp đồ án như sau:

```
MSSV.zip
└── MSSV-Project2
    ├── bai1.cpp
    └── bai2.cpp
```

  Trong đó:

  - Thay cụm `MSSV` thành mã số sinh viên của người nộp. Ví dụ, file dùng để nộp bài có tên `22127001.zip`, hay thư mục được đặt tên là `22127001-Project2`.
  - `MSSV-Project2` là thư mục chứa các file mã nguồn trong đồ án này.
  - `.zip` là định dạng nén cho bài làm.
  - Các file `*.cpp` là các file chứa toàn bộ mã nguồn ứng với từng yêu cầu bài tập nêu trên.

- Nộp file `MSSV.zip`. Nếu sinh viên nộp sai quy định thì toàn bộ phần đồ án này sẽ bị điểm 0.
- Nếu chương trình không biên dịch được thì sẽ bị điểm 0 ở bài tập đó.
- Nếu chương trình biên dịch được nhưng không trả ra được kết quả (do gặp lỗi khi chạy hoặc quá thời gian quy định) ở test nào thì test đó không được tính điểm.
- Thư viện chuẩn của `C++` (`C++` Standard Library) là các thư viện được liệt kê ở `https://en.cppreference.com/w/cpp/standard_library`. Sinh viên cần lưu ý về phiên bản C++ để lựa chọn thư viện thích hợp.
- Mọi thắc mắc về đồ án này, vui lòng gửi qua email: `nvqhuy@fit.hcmus.edu.vn`.