Họ và tên: Nguyễn Đức Dương
Mã sinh viên: 18020386

Phương trình đường cong Elliptic:
E(2,11): $y^2 = x^3 + 9x + 14$ mod p
Với p = 127, đường cong có 113 điểm
Với p = 827, đường cong có 833 điểm

Mã nguồn tìm danh sách các điểm thuộc đường cong:
https://github.com/ducduongn/ElipticHW/blob/main/EllipticAlgorithm.js

Danh sách các điểm thuộc đường cong được export ra file csv:

- Với p = 127:
  https://github.com/ducduongn/ElipticHW/blob/main/pointList1.csv
- Với p = 827:
  https://github.com/ducduongn/ElipticHW/blob/main/pointList2.csv

A) Xét bài toán với p = 127,

Xét P (6, 41) là điểm sinh. Với p = 127, em tính được bảng kP như sau:
https://github.com/ducduongn/ElipticHW/blob/main/BangKP(127).csv

Xây dựng hệ mật EC - ElGamal trên đường cong đã lập, ta có P = (6,41).
Dựa vào bảng kP đã lập, với s = 94, B = sP = (92, 119).

B) Xét bài toán với p = 827

Ta xét P (12, 14) là điểm sinh. Với p = 827, em tính được bảng kP như sau:
https://github.com/ducduongn/ElipticHW/blob/main/BangKP(827).csv

Xây dựng hệ mật EC - ElGamal trên đường cong đã lập, ta có P = (12,14).
Dựa vào bảng kP đã lập, với s = 94, B = sP = (92, 119).