Question 1

State two reasons why elliptic curves are often used instead of plain modular arithmetic in cryptography.

Question 2

In this question, we will explore why it is important to verify points on elliptic curves. Suppose a website has encoded a private key n corresponding to the public key nP on a Hardware Security Module (HSM). The HSM lets them request nQ for any point Q of their choosing – you can think of it like an API endpoint. We (the adversary) have hacked the server, but can't access the inside of the HSM. We only have 5 minutes before we are detected and kicked off the network. Our goal is to recover the private key n in this short time.

We know that $2 \leq n < q$, where q is the order of a prime-order subgroup of the overall curve. $q-1$ is factored as such: $a_1, a_2, \ldots, a_k$ where all factors are small (**assume that solving the discrete logarithm problem over $\mod a_i$ takes constant time**).

Normally, points are chosen from this subgroup. **However, the HSM will not verify whether the point is from this subgroup.** Assume you as an adversary can pass in points Q_i of *arbitrary* order and receive nQ_i.

Devise an attack to recover n in $O(k)$ time.

HINT: If we set Q to be a point in a subgroup of order a_1, we receive $(n \mod a_1)P$. We can solve this discrete logarithm easily in this small set of values to get $n \mod a_1$.

HINT: Consider using the Chinese Remainder Theorem once you are able to recover the values $n \mod a_i$ for all $i \in [0,k]$.

Contributors:

- Ryan Cottone