CS 402 Cryptography

Problem Sheet 8

Let E be the elliptic curve over $\mathbb{Z}_{751}$ defined by $y^2 + y = x^3 - x$.

(a) Convert the stated equation defining E to one of the form $y^2 = f(x)$, where $f(x) = x^3 + ax + b$, by a suitable change of variable (hint: consider $\bar{y} = y + 376$).

(b) Let the plaintext message units be $\emptyset, 1, \ldots, 9, \mathrm{A}, \ldots, \mathrm{Z}$, numbered in that order. Embed the plaintext STOP$\emptyset\emptyset$7 as a sequence of points on E, by evaluating $x = 20m + j$, $0 \leq j \leq 19$, for each message unit m, and determining whether $f(x)$ is a square.

(c) Translate the sequence of points

$$(361, 383),\ (241, 605),\ (201, 380), (461, 467),\ (581, 395)$$

into a reply message.

(d) Use the elliptic curve analogue of ElGamal to send the message in (b) , with base point B chosen as $(0, 0)$. Suppose that your correspondent's public key is the point $(201, 380)$ and your sequence of random ks (one for each message unit) is $386, 209, 118, 589, 312, 483, 335$. What sequence of pairs of points do you send?