Problem Set #5

Due Friday, March 28, 2025 @ 2:00 pm

1. A Trusted Party recommends using the elliptic curve $E : y^2 = x^3 + 931x + 28\,570\,498$ over $\mathbb{F}_p$ where $p = 244\,860\,899$ and the point $P = (1743, 732\,413)$ for ECDHKE.

   (a) Is P a valid point to use?

   (b) Do you trust this Trusted Party? Why or why not?

   (c) No matter what you answered to (b), you and Bob decide to use these parameters for ECDHKE where you are exchanging only x-coordinates.

      i. If you choose a secret multiplier $n_A = 150\,314$, what value do you send to Bob?

      ii. If you receive $73\,091\,251$ from Bob, what is your shared secret key?

2. Curve25519 is often used in ECDHKE.

   Look up the parameters for this curve at `https://www.rfc-editor.org/rfc/rfc7748`

   (a) What is the equation for the curve? What is the modulus p? What is the basepoint? What is the order of the basepoint q?

   (b) Explain why these seem like good parameters to use for ECDHKE.

   (c) Convert the curve to the form $Y^2 = X^3 + AX + B$. What are A and B?
   Use this form of the curve for the remainder of the problem.

   (d) What is the basepoint point P for this form of the curve?
   Verify that P has order q.

   (e) If your private key is $n_A = 2^{132} + 131$, what value do you send to Bob?

   (f) If you receive the value
   $x(Q_B) = 24289809243218792578850560939197117261645082089782354596335198476798734690 7$
   from Bob, what is the shared key? Use the n_A from part (d).

3. Decrypt the following message:

```
WI SC EL YA EH AY MG TN BI IO EH PF AC IM DS PA WX CR EY SC EM XW SD QY
YA OW AR AK PN IR EC MR CL FS IP NZ AK EG QW DS MS FS CS RY MS YA YO PN
EY HY GM EL YA QY YS MP AF QK IW OC BT ER WZ MC OL MX MC AK DT FS PE SW
TW WX DT HA UI RE YN QK CM WE CE IY AM EC ER HR AH PF
```

   Hint: Guess what? I got a fever! And the only prescription is …

   You should turn in a one to two page writeup that explains your analysis that allowed you to find the plaintext or the different approaches you attempted if you were unable to break the cipher. In the latter case, your score for this problem will be based on the quality of your failure.