Week 11 Tutorial

1. The Trusted Party Store publishes toy credentials $(p, A, B, P, q) = (953, 13, 12, (375, 647), 113)$

   (a) Verify that P lies on the elliptic curve.

   (b) Use `http://www.christelbach.com/eccalculator.aspx` to verify that $\operatorname{ord}(P) = q$

   (c) You and Bob are implementing ECDHKE by sharing only x-components.

      i. If you pick $n_A = 102$, what is the value you send to Bob?
      ii. If you receive 362 from Bob, what is your shared key?

   (d) Sam publishes $V = (45, 266)$ for use with her ECDSA signatures.
   Which, if any, of the following are valid ECDSA signatures?

   The messages are entered in the Mathematica notebook for today so that you don't have to worry about formatting them, and you should use P from the Trusted Party Store as the point G.

      i. $(D, (s_1, s_2))$ = ("Whoever invented stew was a genius. I mean, it's got milk in it, but it still tastes good.", $(97, 52)$)
      ii. $(D, (s_1, s_2))$ = ("Someone hit the big score. They figured it out, that we're gonna do it anyway, even if doesn't pay.", $(23, 105)$)

   (e) You want to use ECDSA to sign the message
   "I come up here for perception and clarity. I like to imagine I'm playing SimCity"

      i. Use $s = 87$ to compute your value for V.
      ii. Use an ephemeral value of $e = 58$ to sign your message.

2. The purpose of this problem is to find a website that uses an elliptic curve crypto system.

   (a) Find a secure website (other than Wheaton's website) that uses ECDHKE. What's the url?

   (b) What is the cryptographic suite that is being used for the secure connection?
   Are there any acronyms that you don't understand now?

   (c) What elliptic curve is used?

   (d) Look up the parameters for this elliptic curve.