7.9

I couldn't figure this problem out. It seemed simple, where I thought I would just have to plug the pairs into the *elgamald* function on the V200, using a pair as my *y*, then *p* and *a* as in the book. I tried plugging that into a WolframAlpha ElGamal Decryptor widget (https://www.wolframalpha.com/widgets/view.jsp?id=978d7097ff2a699194ad4282bd27b1dc), but when I tried to do the method myself, I got 28885 instead of 12354.

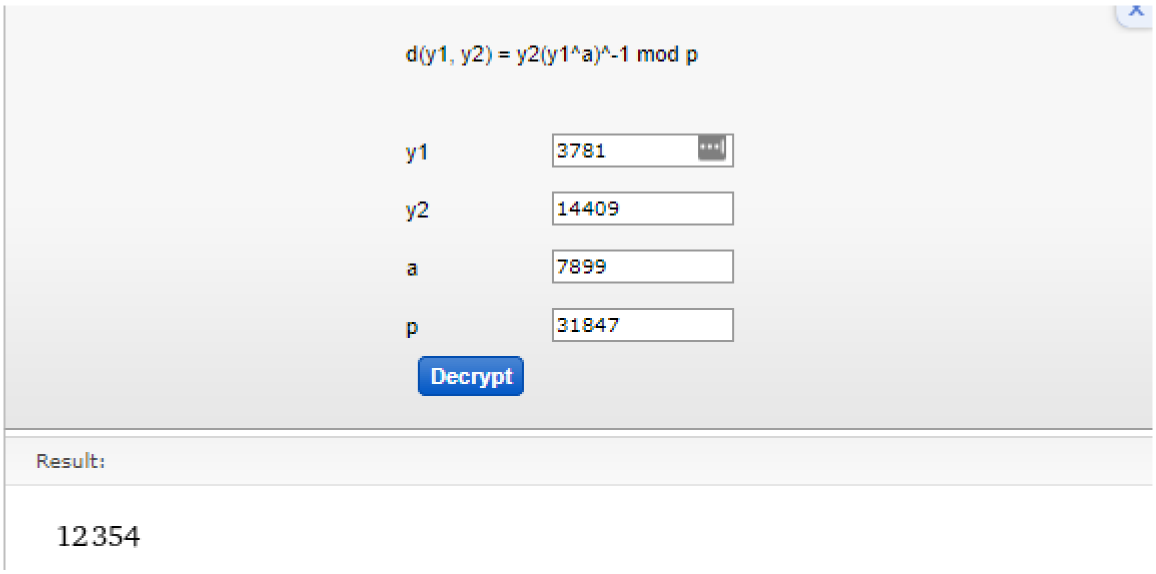

Figure 1

My process involved using the formula on the top of *Figure 1*. I first did my $y1^a$, which was 31847^{7899}. I took this mod *p* to make it manageable, which left me with

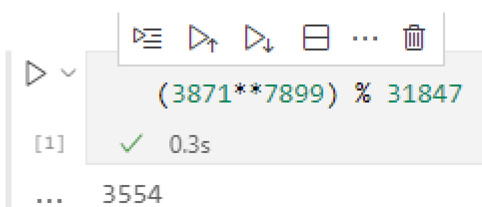

Figure 2

Then, I used my program that I've added to a previous assignment that finds *all* the invertible elements and their inverses, given a modulus. I searched this table for 3554, and found the inverse, which I then multiplied by *y2* mod *p*.

3550	4638
3551	4834
3552	11844
3553	735
3554	21766
3555	10544
3556	4057
3557	1343
3558	546
3559	12635

Figure 3

21766 x 14409 mod 31847 = 28885.

This is also the answer I got when I plugged in the following into the V200:

[[3871][14409]] -> y

31847 -> p

7899 -> a

elgamald(y, p, a)

output: 28885

However, this differs from the computed value from above, and I can’t figure out how to get to the correct answer.

7.10

I tried to follow this top answer's guide to find these polynomials:

> https://math.stackexchange.com/questions/32197/find-all-irreducible-monic-polynomials-in-mathbbz-2x-with-degree-equal

However, I had a hard time following, so I fully just checked the problems against his list.

$x^5 + x^4 + 1$ – Reducible

$x^5 + x^3 + 1$ – Irreducible

$x^5 + x^4 + x^2 + 1$ – Reducible

7.12

I tried setting up the problem as in **7.9**:

> (K, H) -> y
>
> K, H = 2x + 2, $x^2 + 2$
>
> y2 $(y1^a)^{-1}$ mod p
>
> $x^2 + 2 \, ((2x + 2)^{11})^{-1}$ mod p

However, this seemed impossible to solve without a proper value for *p*, and I had no idea where to go next.

I apologize for the poor workmanship on this and the past few assignments. I got married this past Saturday, and I've had no time for anything else.