Fall 2025 CIS 3362 Homework #7: Elliptic Curve Challenge
Check WebCourses for the due date

Note: This assignment is to be done in pairs. Sign up on Webcourses. Come to class for specific instructions.

1) (50 pts) In this question, you will decode a ciphertext that will reveal Alice's Private Key which will be necessary to solve question 2. Alice's Private Key is a large integer.

The following ciphertext below was created via the ADFGVX cipher using the keyword "ELLIPTICURVE" and the following 6 x 6 grid:

```
K L T E V O
R A 1 4 U C
S Y F J 7 P
X H I 5 D W
Q 0 6 9 G 3
B Z N 8 2 M
```

```
VXGVVDVDGVGVVGFDGFFGXGDXVGVVVGDFVXVGGVFFGDGVFVGGVXXVVGXDGGVG
DXGGDFVXVGVGDFVFVXXFDXVXGGVDFGXVVFVFGGDVXGVGGGXDDGFVXFFGVGFF
GFGXVVXXGXGFGVXFVVGVVDGDFVVDGDVXGVVDGX
```

Please feel free to do this by hand, or more likely, write a program. You may build off of sample programs from the course website. Also, it's best to copy paste the 6 x 6 grid above so the number 0 and the letter O don't get confused.

2) (75 pts) The message to break for this question resides in the file

`h7_q2_ciphertext.txt`

The file first lists the Alice's Public Elements for her cryptosystem:

1. The Curve for the system with the prime number (labeled x in the file) as well as the constants a and b (as described in class).

2. The "Generator" point for the system is listed as two separate values gx and gy, for the x and y coordinates, respectively, for the curve.

3. Finally Alice's Public Key is listed, though you won't actually have to use this.

Following this there is the ciphertext. Each pair of points C1 and C2, are listed on consecutive lines, followed by a blank like. Each pair of points encrypts 256 bits or 32 bytes of text. There are a total of 17 blocks of text, so that means the plaintext will be 32 x 17 = 544 total Ascii characters.

You must first solve question 1 to get Alice's Private key, and then use that to decrypt.

There is no prize for question #1, but there is a prize for the first team that solves question #2.

Good luck!!!