Exam 3 – Take home

Printed Name: Paul Beggs

Instructions: This is an individual, open-book, open-notes exam. You may not give help, receive help, or discuss this exam with anyone apart from me.

You may use a calculator or the computer to help with computations, just be sure to cite when you do so.

You may consult your textbook, your personal class notes, and your previous homework assignments while working on this exam. You may also consult anything posted on our Teams page. Only these resources are allowed.

You may NOT consult any other sources. No internet sources. No other textbooks. No notes or any other material from other students. No consulting with another student. No consulting with another professor.

As always, show work to get full credit (the correct answer may NOT be enough).
Write clearly! Double check your answers!

Honor Pledge: I have neither received nor given aid on this work, nor have I witnessed any such violation of the Honor Code.

Honor Pledge Signature:

Question	Points	Score
1	12	
2	14	
Total:	26	

1. Decrypt the following message that was encrypted using a Vignère cipher.

   Note: Spaces are provided to help you type but should be removed before doing any cryptanalysis.

   UOEJG NYBRR UGNWF NMVSC GXQND NUJJB JNEDI SQITN WNQCQ JUF

   UOEJGNYBRRUGNWFNMVSCGXQNDNUJJBJNEDISQITNWNQCQJUF

   (a) Check all key lengths between 3 and 5 letters long to determine which is the most likely. Feel free to use Excel or other tools, but discuss here the appropriate calculations and answers you got to determine the key length. [6]

   > *Solution.* For key length 3, the average index of coincidence is 0.061. Then, for length 4, I got 0.064. Finally, for length 5, I got 0.046. I decided to go with key length 4 because it was the closest to 0.065, which is the expected index of coincidence for English text.

   (b) Find the key word and then decipher the message. Feel free to use Excel or other tools, but discuss here the appropriate calculations and answers you got to determine the key word and plaintext. [6]

   > *Solution.* However, with index 4, I did not get χ^2 values that were reasonable. Still, I tried different shifts, and the deciphered text was not readable. I then tried key length 3 (the next IndCo value closest to 0.065) and got lower χ^2 values, but still high ($\approx .70$). Nevertheless, I tried the different shifts (5, 20, and 13, respectively), and I got a readable text:
   >
   > PUREMATHEMATICSISINITSWAYTHEPOETRYOFLOGICALIDEAS
   >
   > For the keyword, I just subtracted the index of the ciphertext letter by the index of the plaintext letter mod 26. I found the key word to be "FUN."

2. Consider the elliptic curve $E\colon y^2 \equiv x^3 + x + 3 \pmod{53}$ and $P = (10, 18)$.

   (a) Bob chooses $n = 3$ as his private key. Compute his public key using the elliptic curve addition algorithm. Show all work. *Note: you may use Wolfram, etc., to compute modulo arithmetic but* ***DO NOT*** *use the elliptic curve calculator.* [6]

   > *Solution.* We have $E\colon Y^2 = X^3 + x + 3 \pmod{53}$ and $P = (10, 18)$. We can compute Bob's public key (Q_B) by finding $3(10, 18)$. Thus, by the double-and-add algorithm, we have:
   >
   > (i) $n = 3 = 2^1 + 2^0$.
   >
   > (ii) For our table, we need to find $2P$. Thus, we need to calculate λ, X_3, and Y_3:
   >
   > $$\lambda = \frac{3(10)^2 + 1}{2(18)} = \frac{301}{36} = 301 \cdot 36^{-1} \equiv 301 \cdot 28 \pmod{53} \equiv 1,$$
   >
   > $$X_3 = 1^2 - 10 - 10 \equiv -19 \equiv 34 \pmod{53},$$
   >
   > $$\text{and} \quad Y_3 = 1(10 - 34) - 18 \equiv -42 \equiv 11 \pmod{53}.$$

Thus, we have $2P = (34, 11)$.

$$1P = (10, 18)$$
$$2P = (34, 11)$$

(iii) $3P = (10, 18) + (34, 11)$. We need to calculate λ, X_3, and Y_3:

$$\lambda = \frac{11 - 18}{34 - 10} = \frac{-7}{24} = -7 \cdot 24^{-1} \equiv -7 \cdot 42 \pmod{53} \equiv 24,$$

$$X_3 = 24^2 - 10 - 34 \equiv 532 \equiv 2 \pmod{53},$$

$$\text{and} \quad Y_3 = 24(10 - 2) - 18 \equiv 15 \pmod{53}.$$

Thus, we have $Q_B = 3P = (2, 15)$.

(b) Alice uses that to send the initials of the person she likes "Tarin Quentantino" to Bob using $A = 0$, $Z = 25$ $(19, 16)$. Show that this does produce a point on E. [2]

Solution. For the equation $E\colon Y^2 = X^3 + X + 3$, we have:

$$16^2 \stackrel{?}{\equiv} 19^3 + 19 + 3 \pmod{53}$$
$$256 \stackrel{?}{\equiv} 6859 + 19 + 3 \pmod{53}$$
$$44 \stackrel{?}{\equiv} 6881 \pmod{53}$$
$$44 \equiv 44 \pmod{53}.$$

Therefore, the point $(19, 16)$ is on the curve E.

(c) Find the ciphertext (C_1, C_2) that she sends to Bob if the random key used is $k = 21$. Use the double-and-add algorithm when multiplying by $k = 21$. Show all work. [6]
Note: you may use Wolfram and the elliptic curve calculator to do intermediate computations, but you must show the work of using the double-and-add algorithm.

Solution. For the curve $E\colon Y^2 \equiv X^3 + X + 3$ with $P = (10, 18)$, we need to compute C_1. Hence, we need to find $kP \pmod{p}$. Thus,

(i) $k = 21 = 16 + 4 + 1$.

(ii) We need to find $2P$, $4P$, and $16P$. For $2P$:

$$\lambda = \frac{3(10)^2 + 1}{2(18)} = \frac{301}{36} = 301 \cdot 36^{-1} \equiv 301 \cdot 28 \pmod{53} \equiv 1,$$

$$X_3 = 1^2 - 10 - 10 \equiv -19 \equiv 34 \pmod{53},$$

$$\text{and} \quad Y_3 = 1(10 - 34) - 18 \equiv -42 \equiv 11 \pmod{53}.$$

Thus, we have $(34, 11)$ for $2P$.

For $4P$ $(34, 11) + (34, 11)$:

$$\lambda = \frac{3(34)^2 + 1}{2(11)} = \frac{3469}{22} = 3469 \cdot 22^{-1} \equiv 3469 \cdot 41 \pmod{53} \equiv 30$$

$$X_3 = 30^2 - 34 - 34 \equiv 900 - 34 - 34 \equiv 832 \equiv 37 \pmod{53},$$

$$\text{and} \quad Y_3 = 30(34 - 37) - 11 \equiv 30 \cdot (-3) - 11 \equiv -101 \equiv 5 \pmod{53}.$$

Thus, we have $(37, 5)$ for $4P$.
For $8P$ $(37, 5) + (37, 5)$:

$$\lambda = \frac{3(37)^2 + 1}{2(5)} = \frac{4108}{10} = 4108 \cdot 10^{-1} \equiv 4108 \cdot 16 \pmod{53} \equiv 8,$$

$$X_3 = 8^2 - 37 - 37 \equiv 64 - 37 - 37 \equiv 43 \pmod{53},$$

$$\text{and} \quad Y_3 = 8(37 - 43) - 5 \equiv 8 \cdot (-6) - 5 \equiv -53 \equiv 0 \pmod{53}.$$

Thus, we have $(43, 0)$ for $8P$.
Since we have $(X, 0)$, $16P = \mathcal{O}$. Hence, $16P = \infty$.

(iii) $21P = 16P + 4P + P = \infty + (37, 5) + (10, 18) = (46, 17)$. Thus, $C_1 = (46, 17)$.

Now, we need to find $C_2 = M + kQ_B = (19, 16) + 21(2, 15)$. Thus,

(i) $21 = 16 + 4 + 1$.

(ii) Then, for $2Q_B$, we have:

$$\lambda = \frac{3(2)^2 + 1}{2(15)} = \frac{13}{30} = 13 \cdot 30^{-1} \equiv 13 \cdot 23 \pmod{53} \equiv 34,$$

$$X_3 = 34^2 - 2 - 2 \equiv 1156 - 2 - 2 \equiv 1152 \equiv 39 \pmod{53},$$

$$\text{and} \quad Y_3 = 34(2 - 39) - 15 \equiv -1273 \equiv 52 \pmod{53}.$$

Thus, we have $2Q_B = (39, 52)$.
For $4Q_B$, we have:

$$\lambda = \frac{3(39)^2 + 1}{2(52)} = 4564 \cdot 51^{-1} \equiv 6 \cdot 26 \pmod{53} \equiv 50,$$

$$X_3 = 50^2 - 39 - 39 \equiv 2422 \equiv 37 \pmod{53},$$

$$\text{and} \quad Y_3 = 50(39 - 37) - 52 \equiv 50 \cdot 2 - 52 \equiv 48 \pmod{53}.$$

Thus, we have $4Q_B = (37, 48)$.
For $8Q_B$, we have:

$$\lambda = \frac{3(37)^2 + 1}{2(48)} = 4108 \cdot 96^{-1} \equiv 27 \cdot 37 \equiv 45 \pmod{53},$$

$$X_3 = 45^2 - 37 - 37 \equiv 2025 - 37 - 37 \equiv 1951 \equiv 43 \pmod{53},$$

$$\text{and} \quad Y_3 = 45(37 - 43) - 48 \equiv -318 \equiv 0 \pmod{53}.$$

Thus, we have $8Q_B = (43, 0)$.
Similarly to before, since we have $(X, 0)$, $16Q_B = \infty$.
Now, we need to add everything together:

$$M+21Q_B = M+16Q_B+4Q_B+Q_B = (19, 16)+\infty+(37, 48)+(2, 15) = (35, 6).$$

Finally, this gives us the ciphertext $(C_1, C_2) = ((46, 17), (35, 6))$.