UNIVERSITY OF PUERTO RICO

RESEARCH PROJECT

Abstract Algebra

Elliptic Curves Cryptosystem

Author:

Ray Rosario, Alec

Zabel-Mena

Supervisor:

Prof. Janwa

December 7, 2018

Contents

Abstract

Elliptic Curves Cryptosystem

by Ray Rosario, Alec Zabel-Mena

The development of new types of cryptosystems helps maintain confidentiality and stronger ways of securing information. This work analyzes the use of elliptic curves as a tool in cryptography and provides some proofs and details of how they are composed focusing on elliptic curves defined over finite fields. The definition and general equation of an elliptic curve is presented as well as its group laws on addition of points, which are explained. An example of an elliptic curve over a finite field is used in order to present properties of the points such as order. Also, it is shown how they form an abelian group. Finally, an analog to the Massey-Omura cryptosystem is discussed in which the use of points of an elliptic curve is highlighted. Here, the steps in the communication protocol are detailed and it is explained step by step how the message is encrypted and decrypted.

keywords: Elliptic Curve, Cryptography, Massey-Omura cryptosystem

Acknowledgements

We want to thank Dr. Heeralal Janwa, our Abstract Algebra professor for providing us with the space and necessary skills to tackle important questions and problems in cryptography. Also, for his help and eagerness to achieve more with us by making us have the opportunity to develop this work, which is not usually a part of the course.

Additionally, we would like to thank our fellow students for their feedback, cooperation and of course, their help when working with difficult assignments in class...

Chapter 1

Project Summary

1.1 Introduction

This project begins by giving an overall background of elliptic curve cryptosystems. It starts by drawing out the concept of a cryptosystem. It is done by giving an informal definition first, followed by a more formal mathematical one. The motivation for the use of cryptosystems are presented as well as why this topic is relevant today. Definitions are shown for concepts that arise from the use of cryptosystems. Concepts such as plaintext, ciphertext, encryption and decryption are all explained accordingly. After that, the basic process of sending an encrypted message is shown by simple steps, in order to provide an overview of how communication works in cryptosystems.

Then, elliptic curves are introduced, by giving a formal definition using the standard equation

$$y^2 = x^3 + ax + b \tag{1.1}$$

The motivations for the use of elliptic curves are highlighted as well as the benefits from its use when compared to other systems like RSA.

In the proofs section, definitions and examples are presented in order to show some properties and calculate results about elliptic curves. First, the group laws on addition of points are be described, as well as basic properties of elliptic curves. An example of an elliptic curve,

$$y^2 = x^3 - x \tag{1.2}$$

is used in order to perform some of the calculations and proofs. Beginning with listing all of the points of the elliptic curve, which is done in the field $\mathbb{F}_7 = \mathbb{Z}_7$. Then it is shown that it is possible to obtain an abelian group of order 8 with a point at infinity. After that, the orders of each point are calculated. Then it is shown that this group is isomorphic with $\mathbb{Z}_8$. Finally, the public key cryptosystem of the Analog of Massey-Omura is explained, with a detailed step-by-step messaging protocol demonstration.

1.2 Problem Statement

To provide an adequate treatment of the material in this paper, we would like to pose the following problems to be solved.

1. Explain the group laws of addition of points on elliptic curves
2. List all the points on the elliptic curve

$$y^2 = x^3 - x$$

with coefficients in the field $\mathbb{F}_7$.

3. Together with the point at infinity, show that this elliptic curve forms a group under addition
4. Find the orders of each of the points in this group
5. Show whether or not this group is isomorphic to the group $\mathbb{Z}_8$

Chapter 2

Background

2.1 Cryptosystem

With the progress of modern informatics taking over and advances of technology the topic of security is more relevant than never. Communications, transactions and exchanges in information are getting more advanced each day, which is why the use of cryptography is crucial to help ensure security in the processes. Companies are more willing to invest in security in terms of means of transmitting classified data. This could be anything from personal data like credit card information to codes and strategies that a corporation wants to keep hidden. To achieve this, In other words, it is the science of keeping information hidden and secure from unintended audiences. A more formal definition of a cryptosystem is presented.

A cryptosystem (or cipher) can be defined as a quintuple (P, C, K, E, D) where:

- P is the set of plaintexts
- C is the set of ciphertexts
- K is the set of keys

- E: $K \times P \rightarrow C$ is the encryption function
- D: $K \times C \rightarrow P$ is the decryption function

Here, the original message that is meant to be sent is called the plaintext. This will be encoded as a ciphertext and at most times will be written in the same alphabet as the plaintext. The plaintext and the ciphertext will contain also contain the same number of characters.

2.2 Message sending process

The process of converting a plaintext to ciphertext is called encryption, and the inverse process is called decryption. The basic process of sending a message is described below involving three people, Alice, Bob, and Eve:

- Alice wants to send a message called plaintext to Bob
- For Eve to not find out about the message, Alice will encrypt the plaintext into a ciphertext. This is done using an encryption key.
- Bob receives the ciphertext and decrypts it using a decryption key and can read the plaintext.
- Eve is not able to decrypt the messege without a decryption key,so the messege between Alice and Bob stays secure

2.3 Introduction to Elliptic Curves

Modern cryptography uses algorithms and secret keys in order to encrypt and decrypt data and focuses mostly on the secrecy of the keys than the secrecy

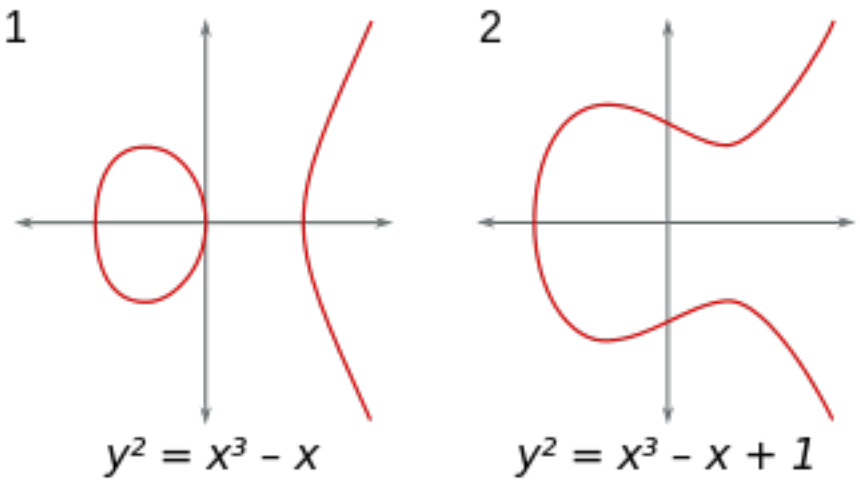

FIGURE 2.1

of the encryption method. Many cryptosystems have been proposed in order to provide the most optimal secrecy and integrity to data, as well as anonymity to the users. One of these methods is the use of elliptic curves. A definition for elliptic curves is presented below.

Definition. Let K be a field of characteristic $\neq 2, 3$, and let $x^2 + ax + b$ (where $a, b \in K$) be a cubic polynomial with no multiple roots. An *elliptic curve* over K is the set of all points $(x, y) \in K^2$ with $x, y \in K$ which satisfy the equation

$$y^2 = x^3 + ax + b \tag{2.1}$$

together with a single element denoted $\mathcal{O}$ and called the *Point at Infinity*.[1]

We will denote the elliptic curve over K, as the set $E(K)$ such that

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b, a, b \in K\} \cup \{\mathcal{O}\} \tag{2.2}$$

The use of elliptic curves has risen because it provides equivalent security

[1] Koblitz, N. (1994)

compared to other systems like RSA (Rivest-Shamir-Adleman), but with the use of fewer bits. A typical Elliptic Curve Cryptosystem key size of 256 bits has the same security as an RSA key of 3072 bits. So, on the long run, RSA keys have to get exponentially large to provide equivalent security compared to the fewer bits that the Elliptic Curves Cryptosystem can provide. Another reason for their use is that it becomes an alternative in case that a major weakness is RSA is found.

Other reasons for why this cryptosystem has been beneficial is because it is faster than systems like RSA. This is because of the use of smaller keys, which means that less data will be transmitted from server to client. Also, it will take less processing power (CPU) which will again, bring faster responses. [2]

[2]Thayer, W. (2015, April 04)

Chapter 3

Proofs and Demonstrations

redGive citations at appropriate places to the material you have used.

3.1 Addition over Elliptic Curve and The Group Law

To construct a suitable notion of addition of points of elliptic curves, let us consider the curve:

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b; a, b \in \mathbb{R}\} \cup \{\mathcal{O}\} \tag{3.1}$$

Definition. Let $E(\mathbb{R})$ be an elliptic curve over the reals and let $P, Q \in E(R)$ We define $+$ as follows:

- If $P = \mathcal{O}$, then $-P = \mathcal{O}$ and $P + Q = \mathcal{O}$. That is, $\mathcal{O} = -\mathcal{O}$ and $\mathcal{O} + Q = Q$
- Let $P = (x, y) \in E(\mathbb{R})$ then $-P = (x, -y) \in E(\mathbb{R})$
- If $P \neq Q$, then take $l = \overline{PQ}$ to be the line that cuts $E(\mathbb{R})$ at P, Q, and another point R.Then $P + Q = -R$

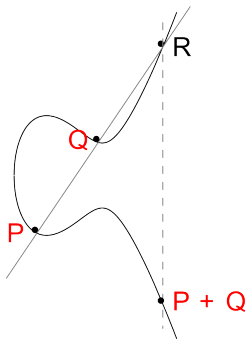

FIGURE 3.1: Addition of points on an elliptic curve

If we let the line $l = \overline{PQ}$ be the plane line $y = \alpha x + \beta$ and $P = (x_1, y_1), and Q = (x_2, y_2)$ be points on $E(\mathbb{R})$, then we can find the coordinates of $P + Q$ adhering to two cases, the first looks at when P and Q are distinct points, in this case we draw the line that cuts $E(\mathbb{R})$ at P and Q then we note that $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$. The latter, concerns itself when P and Q are the same, then it results that the line $y = \alpha x + \beta$ is tangent to the curve, and we consider the derivative of the curve $2y\frac{dy}{dx} = 3x^2 + a$, and here, $\alpha = \frac{dy}{dx}$, In both cases, $\beta = y_1 - \alpha x_1$.

Case 1 If $P \neq Q$ then $P + Q = (x_3, y_3)$ such that

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_1, y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_1) - y_1 \tag{3.2}$$

Case 2 If $P = Q$ then $P + Q = P + P = (x', y')$ such that

$$x' = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1, y' = (\frac{3x_1^2 + a}{2y_1})(x_1 - x') - y_1 \tag{3.3}$$

Now that we have found equations for coordinates the point $P + Q$ in $E(\mathbb{R})$, we can take them to be the coordinates for points on a general elliptic curve $E(K)$.

It can be shown that the elliptic curve $E(K)$ forms an abelian group over $+$, that is for $P, Q, R \in E(K)$

- $P + Q \in E(K)$ (*Closure*)
- $(P + Q) + R = P + (Q + R)$ (*Associative*)
- $\exists I \in E(K)$ such that $P + I = I + P = P$ (*Identity Law*)
- $\exists P^{-1} \in E(K), \forall P \in E(K)$ such that $P + P^{-1} = P^{-1} + P = I$ (*Inverse Law*)
- $P + Q = Q + P$ (*Commutative*)

In fact, it follows by our definition of $+$ over $E(K)$ that closure, and the identity and inverse laws are satisfied, where $I = \mathcal{O}$ and $P^{-1} = -P$, it is also rather easy to show closure. Thus, the only law left to prove, is associative, but the proof for it is beyond the scope of this paper, so we simply accept it as true. In fact, we will go on to prove associative in a much simpler case in the next section, rather than a general proof. Now that we have gone over addition over elliptic curves and it's properties, we can state the following as a theorem

Theorem 3.1.1. *Let K be a field of characteristic $\neq 2, 3$ and for $a, b \in K$ let $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\}$ be an elliptic curve, and let $+$ be the addition of points over $E(K)$. Then $(E(K), +)$ forms a group*

3.2 Points of Elliptic Curves Over Finite Fields

We would like to find elliptitc curves defined over a finite number of points. A natural start, would be to consider the field $\mathbb{F}_q$[1] where $q = p^r$ for some $r \in \mathbb{Z}$ and where p is prime. For our purposes, it is useful just to consider for now the set $\mathbb{F}_p$ where p is prime.

Consider the elliptic curve:

[1] here $\mathbb{F}_q = \mathbb{Z}_q$

Points of $y^2 = x^3 - x$				
x	x^3	$x^3 - x$	y	*points*
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$(\bar{0}, \bar{0})$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$(\bar{1}, \bar{0})$
$\bar{2}$	$\bar{8}$	$\bar{6}$	-	-
$\bar{3}$	$\bar{2}$	$\bar{3}$	-	-
$\bar{4}$	$\bar{2}$	$\bar{4}$	$\bar{2}$,$\bar{5}$	$(\bar{4},\bar{2})$,$\bar{4},\bar{5})$
$\bar{5}$	$\bar{4}$	$\bar{1}$	$\bar{1}$,$\bar{6}$	$(\bar{5},\bar{1})$,$(\bar{5},\bar{6})$
$\bar{6}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$(\bar{6}, \bar{0})$

FIGURE 3.2

$$E(\mathbb{F}_7) = \{(x, y) \in \mathbb{F}_7^2 : y^2 = x^3 - x\} \cup \{\mathcal{O}\}$$

where $\mathbb{F}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. We would like to find the points on the curve $E(\mathbb{F}_7)$. This is achieved simply by finding the points in $\mathbb{F}_7^2$ that satisfy the equation $y^2 = x^3 - x$:

Using 3.2 we find that:

$$E(\mathbb{F}_7) = \{\mathcal{O}, (\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{4}, \bar{2}), (\bar{4}, \bar{5}), (\bar{5}, \bar{1}), (\bar{5}, \bar{6}), (\bar{6}, \bar{0})\}$$

where $|E(\mathbb{F}_7)| = 8$. Now that we have found points that satisfy $E(\mathbb{F}_7)$, we would like to establish that this set forms a group over addition[2]. Since it is beyond our scope to prove associativity, we undertake the endeavor of proving it using a cayley table. With this table, we will be able to prove the appropriate group laws.

Theorem 3.2.1. *Let $+$ be the addition of points on an arbitrary elliptic curve $E(K)$. Then $(E(\mathbb{F}_7), +)$ forms a group.*

[2]We would be proving a special case of $E(K)$

TABLE 3.1: The Cayley tabel for $(E(\mathbb{F}_7), +)$

$+$	$\mathcal{O}$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{4},\bar{2})$	$(\bar{4},\bar{5})$	$(\bar{5},\bar{1})$	$(\bar{5},\bar{6})$	$(\bar{6},\bar{0})$
$\mathcal{O}$	$\mathcal{O}$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{4},\bar{2})$	$(\bar{4},\bar{5})$	$(\bar{5},\bar{1})$	$(\bar{5},\bar{6})$	$(\bar{6},\bar{0})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$\mathcal{O}$	$(\bar{6},\bar{0})$	$(\bar{5},\bar{1})$	$(\bar{5},\bar{6})$	$(\bar{4},\bar{2})$	$(\bar{4},\bar{5})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{6},\bar{0})$	$\mathcal{O}$	$(\bar{4},\bar{5})$	$(\bar{4},\bar{2})$	$(\bar{5},\bar{6})$	$(\bar{5},\bar{1})$	$(\bar{0},\bar{0})$
$(\bar{4},\bar{2})$	$(\bar{4},\bar{2})$	$(\bar{5},\bar{1})$	$(\bar{4},\bar{5})$	$(\bar{4},\bar{5})$	$\mathcal{O}$	$(\bar{6},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{5},\bar{1})$
$(\bar{4},\bar{5})$	$(\bar{4},\bar{5})$	$(\bar{5},\bar{6})$	$(\bar{4},\bar{2})$	$\mathcal{O}$	$(\bar{4},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{6},\bar{0})$	$(\bar{5},\bar{1})$
$(\bar{5},\bar{1})$	$(\bar{5},\bar{1})$	$(\bar{4},\bar{2})$	$(\bar{5},\bar{6})$	$(\bar{6},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$\mathcal{O}$	$(\bar{5},\bar{6})$
$(\bar{5},\bar{6})$	$(\bar{5},\bar{6})$	$(\bar{4},\bar{5})$	$(\bar{5},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{6},\bar{0})$	$\mathcal{O}$	$(\bar{1},\bar{0})$	$(\bar{5},\bar{1})$
$(\bar{6},\bar{0})$	$(\bar{6},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{5},\bar{1})$	$(\bar{5},\bar{1})$	$(\bar{5},\bar{6})$	$(\bar{1},\bar{0})$	$\mathcal{O}$

Proof. Since $E(K)$ is closed and commutative under $+$ for any field, $(E(\mathbb{F}_7), +)$ inherits closure and commutative. Then refering to the cayley table 3.1

We see from 3.1 that the Inverse and Identity laws are satisfied, furthermore, associativity is satisfied. For example we see that:

$$((\bar{4},\bar{5}) + (\bar{5},\bar{1})) + (\bar{4},\bar{2}) = (\bar{0},\bar{0}) + (\bar{4},\bar{2}) = (\bar{5},\bar{1})$$

and

$$(\bar{4},\bar{5}) + ((\bar{5},\bar{1}) + (\bar{4},\bar{2})) = (\bar{4},\bar{5}) + (\bar{6},\bar{0}) = (\bar{5},\bar{1})$$

so

$$((\bar{4},\bar{5}) + (\bar{5},\bar{1})) + (\bar{4},\bar{2}) = (\bar{4},\bar{5}) + ((\bar{5},\bar{1}) + (\bar{4},\bar{2}))$$

Therefore we see that $E(\mathbb{F}_7)$ satisfies the group laws, along with commutative and hence is an abelian group. ■

Remark. In essence $E(\mathbb{F}_7)$ didn't need to inherit closure or commutativity from $E(K)$, as the cayley table 3.1 establishes both properties. We could have show closure and commutativity independently; but we would like $E(\mathbb{F}_7)$ to have some dependence on $E(K)$ as to illustrate the group structure of $E(K)$

TABLE 3.2

Inverses	Order
$\mathcal{O} = -\mathcal{O}$	$o(\mathcal{O}) = 1$
$(\bar{0}, \bar{0}) = -(\bar{0}, \bar{0})$	$o((\bar{0}, \bar{0})) = 2$
$(\bar{1}, \bar{0}) = -(\bar{1}, \bar{0})$	$0((\bar{1}, \bar{0})) = 2$
$(\bar{4}, \bar{2}) = -(\bar{4}, \bar{5})$	$o((\bar{4}, \bar{2})) = 3$
$(\bar{4}, \bar{5}) = -(\bar{4}, \bar{2})$	$o((\bar{4}, \bar{5})) = 3$
$(\bar{5}, \bar{1}) = -(\bar{5}, \bar{6})$	$o((\bar{5}, \bar{1})) = 4$
$(\bar{5}, \bar{6}) = -(\bar{5}, \bar{1})$	$o((\bar{5}, \bar{1})) = 4$
$(\bar{6}, \bar{0}) = -(\bar{6}, \bar{0})$	$o((\bar{6}, \bar{0})) = 2$

We find of all the elements in $E(\mathbb{F}_7)$ that $\mathcal{O}$ is its own inverse[3], the elements $(\bar{0}, \bar{0})$, $(\bar{1}, \bar{0})$ and $(\bar{6}, \bar{0})$ also share this property, they also have the same order. The elements $(\bar{4}, \bar{2})$ and $(\bar{4}, \bar{5})$ are each others inverse and share the same order, and the same is said for $(\bar{5}, \bar{1})$ and $(\bar{5}, \bar{6})$.

It is natural to wonder, since the group $E(\mathbb{F}_7)$ has order 8 whether or not it is isomorphic to some other group like $\mathbb{Z}_8$ which also has order 8. We know that $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$[4]. Let $\phi : E(\mathbb{F}_7) \to \mathbb{Z}_8$ be a isomorphism between $E(\mathbb{F}_7)$ and $\mathbb{Z}_8$. Then for every element $P \in E(\mathbb{F}_7)$, $\phi(P) \in \mathbb{Z}_8$ and the properties of every P carry over to $\phi(P)$. Hence, ϕ takes the group structure and properties of $E(\mathbb{F}_7)$ into $\mathbb{Z}_8$. Now Z_8 is cyclic with respect to $[1]$ (that is $\langle [1] \rangle = \mathbb{Z}_8$), then $[1]$ has order 8. Since ϕ is and isomorphism, there must exist some $P \in E(\mathbb{F}_7)$ such that $\phi(P) = [1]$, hence P must have order 8. However[5], $E(\mathbb{F}_7)$ has no such element whose order 8. Therefore such a ϕ cannot exist, and we see that $E(\mathbb{F}_7)$ is not isomorphic to $\mathbb{Z}_8$.

Remark. It is also sufficient to show that since $E(\mathbb{F}_7)$ has no element of order 8, that it cannot be cyclic with respect to any element, so isomorphism with $\mathbb{Z}_8$ again fails to hold.

[3] rote, since $\mathcal{O}$ is the identity element

[4] To distinguish between the elements of equivalence classes in $\mathbb{F}_7$ and Z_8 we take $\bar{a}$ to be an element of $\mathbb{F}_8$ and $[a]$ an element of Z_8

[5] referring to 3.2

3.3 Analog of Massey-Omura

The Analog of Massey–Omura Cryptosystem was proposed by James Massey and Jim K. Omura in 1982. It is a public key cryptosystem which transmits a message m as points on an elliptic curve E over the field $\mathbb{F}_q$, where $q = p^r$ for some $r \in \mathbb{Z}$ and p, prime. Here, the elliptic curve, as well as its points are public and fixed. The number N of points of E is also known. The protocol for message sending is as follows:

- The message will be embedded as points on the elliptic curve and will be denoted P_m. A prime modulus p will be chosen between both users.
- Each user (sender A and receiver B) will choose a random integer e such that $1 < e < N$ and (e,N). Because these e's will be different for each, we will denote them e_a and e_b. This element e will be called encryption key.
- The users will then calculate their respective decryption keys, which will be in the form d= $\{d \mid e \times d = 1(modN)\}$. This is done using the Euclidean Algorithm and will be denoted d_a and d_b respectively.
- The sender enciphers P_m by computing $e_a P_m$ mod p. This point will be sent to the receiver.
- The receiver would not be able to retrieve P_m from $e_a P_m$, since he does not know what neither P_m or e_a are. Instead, he will compute $e_b e_a P_m$ and will send it to the original sender.
- The sender will partially decipher the message by computing his decryption key $d_a e_b e_a P_m$ and since $d_a \times e_a = 1(modN)$, this will be $e_b P_m(modN)$ and will be sent to the receiver yet again.

- The receiver will finish decryption of the message by computing his decryption key $d_b e_b P_m (mod N)$ which will give P_m which is the original message.[6]

Note that someone who might want to intercept the message will only be able to know $e_a P_m, e_b P_M$ and $e_b e_a P_m$ and it is not easy to get P_m from those.

[6] Koblitz, N. (1994)

Chapter 4

Open Problems and Future Directions

This work provided some basic definitions and showed some properties of elliptic curves as a whole. In a future project, types of elliptic curves could be studied as well as explore elliptic curves with characteristic 2 or 3. Additionally, elliptic curves could be studied over the complex and the rationals.

More examples of elliptic curves could be presented as well as all of the calculations done for the one in this work but for each of them. This would show how the formulas work for different forms of elliptic curves. Also, in a future work, an isomorphism could be found with the example elliptic curve provided in this work as well as for others that could be added.

The elliptic curve discrete logarithm problem (ECDLP) is where the elliptic curve crypstosystem draws its strength. This could be further explained in a future work. Other types of cryptosystems that use elliptic curves such as the analog of Massey Omura could be described in a future project, these may include analog of Diffie–Hellman (ECDH) and analog of ElGamal.

Chapter 5

References

[1] Castryck, W. (2013, September 11). Introduction to Elliptic Curve Cryptography. Retrieved from https://www.cosic.esat.kuleuven.be/ecc2013/files/wouter.pdf

[2] Brown, E. (2010, December). Elliptic Curve Cryptography. Retrieved from https://www.math.hmc.edu/ ursula/teaching/math189/finalpapers/elaine.pdf

[3] Koblitz, N. (1994). A course in number theory and cryptography. Seattle, WA: Springer.

[4] Thayer, W. (2015, April 04). Benefits of Elliptic Curve Cryptography. Retrieved from https://casecurity.org/2014/06/10/benefits-of-elliptic-curve-cryptography/

[5] Winston, R. (n.d.). Enhancing the Massey-Omura Cryptosystem. Journal of Mathematical Sciences Mathematics Education, 21-29. Retrieved from http://www.msme.us/2007-1-3.pdf

[6] Koblitz, N. (1987, January). Elliptic Curve Cryptosystems. American Mathematical Society, 203-209. Retrieved from https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf