http://waikato.researchgateway.ac.nz/

Research Commons at the University of Waikato

Copyright Statement:

The digital copy of this thesis is protected by the Copyright Act 1994 (New Zealand).

The thesis may be consulted by you, provided you comply with the provisions of the Act and the following conditions of use:

- Any use you make of these documents or images must be for research or private study purposes only, and you may not make them available to any other person.
- Authors control the copyright of their thesis. You will recognise the author's right to be identified as the author of the thesis, and due acknowledgement will be made to the author where appropriate.
- You will obtain the author's permission before publishing any material from the thesis.

Comparison between the RSA cryptosystem and elliptic curve cryptography

A thesis

submitted in partial fulfilment

of the requirements for the Degree

of

Master of Science

at the

University of Waikato

by

Kamilah Abdullah

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

University of Waikato

2010

Abstract

In the globalization era, cryptography becomes more popular and powerful; in fact it is very important in many areas (i.e. mathematics, computer science, networks, etc). This thesis provides an overview and comparison between the RSA cryptosystem and elliptic curve cryptography, which both focus on sending and receiving messages. The basic theories of the RSA cryptosystem and elliptic curve cryptography are explored. The RSA cryptosystem and elliptic curve cryptography theories are quite similar but elliptic curve cryptography is more complicated. The idea of the RSA cryptosystem is based on three popular theorems which are Euler's Theorem, Fermat's Little Theorem and the Chinese Remainder Theorem. This discussion shows that the reliability and strong security of the RSA cryptosystem depends on the degree of difficulty of integer factorization. Therefore, methods for integer factorization are discussed. In addition I show how the security of elliptic curve cryptography depends on the apparent difficulty of solving the elliptic curve discrete logarithm problem (ECDLP).

Acknowledgements

I would like to express my deepest gratitude to Associate Professor Kevin Broughan, who willingly agreed to supervise and guide me patiently in this endeavour. Indeed, to him I owe this thesis, without his assistance and constructive comments, this study would never have been possible. Sincere gratitude and appreciation also goes to senior students for the inspiration, ideas and support they imparted to me. Most of all, I owe the warmest gratitude to my parents, Abdullah Ismail and Wan Fatimah Wan Yusoff for their support, emotional assistance and encouragement. Also, for my special husband, Adlan Rahmat, thank you for your understanding, patience and support. Finally, this thesis would not have been possible without the help and support of my dear colleagues and friends; Mrs. Junaidah Januin, Mrs. Ruhaya Hussin, Mrs. Masleeyati Yusop and Miss. Fauziah Sulaiman for being there with me through my ups and downs. Thank you for the endless support you have given me.

Contents

Chapter 1

Introduction

Cryptography is the area of mathematics that disguises the information or data of communications. The purpose of cryptography is to secure the message between two persons so another person or adversary cannot understand the enciphered message. Only the recipient can decipher the message. For instance, military, government and diplomatic communications are suitable applications for cryptography.

The objective of this thesis is to compare the encryption and decryption between the RSA cryptosystem and elliptic curve cryptography. I also describe some examples of their applications.

The RSA cryptosystem is the best known and most commonly used cryptosystem. It is often called the public key cryptosystem. Elliptic curve cryptography is the other cryptosystem which is included in this thesis. It involves solving the discrete logarithm problem for elliptic curves over a finite field.

Chapter 1 outlines the literature review, history of cryptography and some basic theorems and algorithms. Then a description of the Diffie-Hellman key exchange method and the El-Gamal public key cryptosystem are provided.

In Chapter 2 I discuss the RSA cryptosystem. The chapter begins with the Euler's formula and integer factorization that are significant for RSA. The

RSA algorithm and primality testing are introduced. Further, the theory of discrete logarithm in a finite field ($\mathbb{F}_p$) and some applications of RSA are also provided.

Chapter 3 is about elliptic curves and the associated elliptic curve cryptography method. Further, a description of the elliptic curve discrete logarithm problem is provided. I also present some applications of elliptic curve cryptography in the real life.

Chapter 4 includes a comparison between the RSA cryptosystem and elliptic curve cryptography, using Mathematica software. This also includes some examples to show how the encryption and decryption works in each case.

In Chapter 5 some conclusions will be made.

1.1 Literature review

The following are the literature I consulted:

1. Books

   (a) Title: An Introduction to Mathematical Cryptography.
   Authors: Jeffrey H., Jill P., Joseph H.S.
   Publication: Springer, 2008.
   Chapters used: 1, 2, 3 and 5.

   (b) Title: Elliptic curves (Number theory and Cryptography).
   Author: Lawrence C.Washington.
   Publication: Chapman & Hall / CRC, 2003.
   Chapters used: 2, 4, 5 and 6.

   (c) Title: A classical introduction to cryptography exercise book.
   Authors: Thomas Baignères, Pascal Junad, Yi Lu and Serge Vaudenay.

Publication: Springer Science + Business Media Incorporation, 2006.

Chapters used: 1 and 9.

(d) Title: Cryptoclub: Using mathematics to make and break secret codes, workbook.

Authors: Beissinger, Janet, Pless and Vera.

Publication: AK Peters Limited, 2006.

Units used: 1, 2, 3, 6 and 7.

(e) Title: Basics of contemporary cryptography for IT practitioners.

Authors: Ryabko, Boris, Fionov and Andrey.

Publication: World Scientific Publishing Company Incorporated, 2005.

Chapters used: 2, 3 and 6.

(f) Title: Elliptic curves, A computational approach.

Authors: Susan Schmit and Horst G. Zimmer.

Publication: Berlin, Germany, 2003.

Chapters used: 1 and 3.

(g) Title: Rational points on elliptic curves.

Author: Joseph H. Silverman.

Publication: Springer-Verlag, New York Incorporation, 1992.

Chapters used: 1, 2 and 4.

(h) Title: An introduction to cryptography.

Author: Richard A. Mollin.

Publication: Chapman & Hall, 2001.

Pages used: 1 - 251.

2. Lecture notes

(a) Title: INFO412 - Mathematical and Cryptography.

Authors: Associate Professor Peter Nickolas & Professor Martin Bunder.

Publication: School of Mathematics & Applied Statistics, University of Wollongong,Australia.

Sections used: 4, 6, 7, 8, 9, 10 and 11.

(b) Title: RSA crptosystem.

Author: Xin Guo.

Publication: Department of Industrial Engineering and Operations Research.

Section used: Introduction.

(c) Title: Lecture 22: Cryptology.

Author: R. Sedgewick.

Publication: Department of Computer Science, Princeton University.

Pages used: 1 - 7.

(d) Title: Lecture 14 - Elliptic curve cryptography.

Author: Avinash Kak.

Publication: Computer and Network Security, Purdue University.

Pages used: 1 - 48.

(e) Title: Online number theory lecture notes and teaching materials.

Author: Keith Matthews.

Publication: Brisbane, Australia. Topics used: 22, 23 and 43.

(f) Title: Chapter 6 - RSA cryptosystem.

Author: Jozef Gruska.

Publication: Faculty of Informatics, Masaryk University.

Pages used: 1 - 15.

(g) Title: Lecture 12 - Non-secret key cryptosystems (How Euclid, Fer-

mat and Euler created E-Commerce).

Author: David Evans.

Publication: Department of Computer Science, University of Virginia.

Address: http://www.cs.virginia.edu/cs588/lectures/lecture12.ppt

Pages used: 1 - 34.

(h) Title: Security.

Authors: Kevin Wayne and Robert.

Publication: Department of Computer Science, Princeton University.

Address: http://www.cs.duke.edu/courses/spring04/cps001/notes/Security-4up.pdf

(i) Title: The RSA public key cryptosystem.

Author: Kevin Jeffay.

Publication: Department of Computer Science, University of North Carolina.

Pages used: 1 - 11.

(j) Title: Number theory lecture notes.

Author: Broughan, K.A.

Publication: Department of Mathematics, University of Waikato.

Chapters used: 1, 2, 5, 6, 9, 10, 11, 12 and 14.

3. Web sources

(a) Title: Overview of Elliptic Curve Cryptosystems.

Address: www.rsa.com/rsalabs/node.asp?id=2013.

Publication: RSA Laboratories.

(b) Title: Elliptic curve cryptography, An introduction.

Author: Dr. F. Vercauteren.

Publication: Katholieke Universiteit Leuven.

Address: www.cosic.esat.kuleuven.be/publications/talk-95.pdf

Content used: Introduction.

(c) Title: Elliptic curve cryptography.

Publication: Wikipedia.

Address: http://en.wikipedia.org/wiki/Elliptic curve cryptography

(d) Title: Securing the web with elliptic curve cryptography.

Publication: Sun Microsystems Incorporation.

Address: http://research.sun.com/projects/crypto/

Section used: Introduction.

(e) Title: Elliptic curve cryptography.

Author: Steven Galbraith.

Publication: Department of Mathematics, University of Auckland, New Zealand.

Address: www.isg.rhul.ac.uk/∼sdg/ecc.html

Section used: Summary.

(f) Title: An introduction to the RSA cryptosystem.

Author: Marcus Griep.

Address: www.devhood.com/Tutorials/*tutorial_details.aspx?tutorial_id* = 544

4. Journals, papers and book chapter

(a) Title: Elliptic curve cryptography and smart card.

Author: Ahmed Khaled M. Al-Kayali.

Publication: SANS Institute InfoSec Reading Room.

Pages used: 1 - 15.

(b) Title: The advantages of elliptic curve cryptography.

Author: Kristin Lauter.

Publication: Microsoft Corporation.

Pages used: 62 - 67.

(c) Title: Elliptic curve cryptosystem and its application.

Authors: G.V.S Raju and Rehan Akbani.

Publication: Proceedings of the IEEE International Conference on Systems, Man & Cybernetics (IEEE-SMC), 2003.

Pages used: 1 - 4.

(d) Title: Efficient implementation of elliptic curve cryptography and personal digital assistance (PDAs).

Authors: Amol Dabholkal and Kin Choong Yow.

Publication: Nanyang Technological University, Singapore.

Sections used: Abstract, introduction and elliptic curve cryptography.

(e) Title: Overview of elliptic curve cryptography.

Authors: Kiyomichi Araki, Takakazu Satoh and Shinji Miura.

Publication: Springer-Verlag Berlin Heidelberg.

Sections used: Introduction, discrete logarithm problem and the ElGamal system.

(f) Title: RSA cryptosystem.

Author: Weihu Hong.

Publication: Department of Mathematics, Clayton College & State University.

Pages used: 1 - 6.

(g) Title: RSA cryptosystem.

Author: Silvia Robles.

Publication: Massachusetts Institute of Technology.

Pages used: 1 - 10.

(h) Title: Securing telecommunication based on speaker voice as the public key.

Authors: Monther Rateb Enayah and Azman Samsudin.

Publication: IJCSNS International Journal of Computer Science and Network Security, VOL. 7 No. 3.

Pages used: 1 - 9.

(i) Title: Introduction to elliptic curve cryptography.

Author: Elisabeth Oswald.

Publication: Institute of Applied Information Processing and Communication, Austria.

Contents used: Abstract and section 1.

(j) Title: Introduction to cryptography.

Author: Johannes Buchman.

Publication: Springer 2004.

Chapter used: 7.

5. History

(a) Title: Public key cryptography (PKC) History.

Address: www.livinginternet.com/i/*is_crypt_pkc_inv.htm*

(b) Title: Cryptography.

Publication: Cryptography portal.

Address: en.wikipedia.org/wiki/Cryptography

(c) Title: History of cryptography.

Author: David Terr.

Address: www.davidterr.com/science-articles/cryptography.html

(d) Title: RSA.

Publication: Wikipedia.

Address: en.wikipedia.org/wiki/RSA

(e) Title: A brief history - The origins of public key cryptography and ECC.

Address: www.certicom.com/index.php/a-brief-history

(f) Title: A brief history of cryptography.

Authors: Charles Edge, Wlliam Barker and Zack Smith.

Publication: Foundation of Mac OS X Security.

1.2 A brief history of cryptography

1.2.1 Introduction and terminology of cryptography

Both cryptography and cryptology are mathematics and computer science areas that focus on security of information, particularly encryption and verification. Nowadays, cryptography makes frequent use of mathematics, especially discrete mathematics (i.e. number theory, information theory, computational complexity, statistics and combinatorics). Recently, cryptography has become an important part of computer and network security. This is to protect the communication between computers (i.e. to protect data in the computer and to protect data when it is being transferred), [58, 63].

Cryptography is from the Greek language where 'kryptos' means "*hidden*" and 'graphein' means "*to write*". So, generally cryptography means "*secret writing*". Cryptology means "the study of secret writing" and cryptanalysis means "*code breaking*". Basically, cryptography is concerned with encryption which is the process of converting plaintext (i.e. the original message) into ciphertext (i.e. the disguised message). The reverse process of encryption is called decryption (i.e.

transforming the ciphertext into plaintext), [63, 58].

1.2.2 Types of cryptosystems

1. **Caesar's cipher**

   Caesar's cipher was invented by Julius Caesar around 100 B.C. - 44 B.C., and used during his military campaigns. This cipher is one of the earliest and simplest substitutions. The message (or plaintext) is encrypted by changing each letter into a fixed number and then replacing each number with a new letter which is also in the alphabet. The problem with this method is that Caesar's ciphers are very easy to break. Caesar's cipher is an instance of a substitution cipher, where each letter is substituted with a different letter from the alphabet. By using the frequency of occurrence of letters in the languages (i.e. English or others), these substitution ciphers are very easy to break, [59, 58].

2. **Vignere cipher**

   The Vignere cipher was created by Giovan Batista Belaso in 1553. This cipher uses a secret keyword to encrypt the plaintext (i.e. the original message). First, each letter in the plaintext is converted into a number. Then this numerical value for each letter of the plaintext is added to the numerical value of each letter of a secret keyword to get the ciphertext. The Vignere cipher is harder to break than a substitution cipher, [59].

3. **One-Time Pad**

   The one-time pad was invented in 1917. It is a very secure cryptosystem. This cryptosystem works like the Vignere cipher, but this cipher uses a secret keyword which is as long as the original text. Unfortunately, this one-time pad might only be used once as the name implies, [59].

4. **Enigma**

   The Enigma machine was used during World War II by the German Army to encrypt messages. The Enigma machine was like a typewriter and applied a 4-letter secret code that was set by a user. The encrypted message was considered to be impossible to break. The Allies tried to break and analyze the code and did so near the end of the war, [59, 58].

5. **Symmetric-key cryptography**

   Symmetric-key cryptography is where both senders and receivers share the same keys. So those keys are used for both encryption and decryption. They are used mainly with block ciphers and stream ciphers. The block cipher is an alphabetic form of cipher in which a block of plaintext data and a key is taken, then ciphertext of the same size is output. In contrast, stream ciphers works by creating randomly a long stream of key material, which is combined with plaintext. It works like a one-time pad encryption technique. Unfortunately, the key for decryption is easily calculated from the key used for encryption. The reason for this is the key is hard to hide during transport (or passing). Besides, the key and the method of decryption must be sent to the correct receiver. The following cryptosystem solves this problem, [59, 58, 63].

6. **Public-key cryptography**

   Public-key cryptography is also known as asymmetric key cryptography because it uses two different keys. The following are the types of public-key cryptography:

(a) Diffie-Hellman cryptosystem

This is the first public-key cryptosystem that was invented by Whitfield Diffie and Martin Hellman, working in collaboration with Ralph Merkle in 1976. This cryptosystem uses two different keys, but they are related: a public key and a private key. Both keys are secretly generated. Basically, the public key is used for encryption while the private key is used for decryption. The Diffie-Hellman algorithm is based on the difficulty of the discrete logarithm problem. Even though Diffie achieved the concept of an asymmetric cipher, he did not really get the precise function that met his requirements. This only solved the key distribution. However, he inspired other mathematicians and scientists to discover another cipher, the RSA cryptosystem which is discussed next, [58, 63, 59, 47, 62, 61].

(b) RSA cryptosystem

RSA cryptosystem was developed by Ronald Rivest, Adi Shamir and Leonard Adleman in 1978. It has become a standard public-key cryptography used to encrypt private data, and it was the first published public key system. The high level of security of RSA depends on the difficulty of factoring large numbers which are products of large primes. Around the 1980s, scientists noticed that even though this difficulty occurred, it still did not achieve sufficient security. Therefore, they developed a strong method for security which created a hypothesis about the weaknesses of an adversary. This method is used with specific computational algorithms to meet the requirements of security. In 1984 the ElGamal public-key encryption appeared. It was based on the discrete logarithm problem and competed with the RSA cryptosystem. A year later, elliptic curve cryptography appeared which was also based on the discrete

logarithm problem, [47, 58, 62, 63, 61, 60].

(c) Elliptic curve cryptography

Elliptic curve cryptography was invented by Neal Koblitz and Victor S. Miller in 1985. This is an efficient algorithm because it is based on the discrete logarithm problem, which is apparently harder to solve than other algorithms, particularly algorithms for factoring, [62, 63, 39].

1.3 Basic theorems

The following results are standard propositions in elementary number theory.

Theorem 1.1 *(Euler's Theorem).*
Let $\phi(n)$ be Euler's phi function (i.e. $\phi(n) = \sharp\{j : 1 \leq j \leq n, gcd(j,n) = 1\}$). If $gcd(a,n) = 1$ then $a^{\phi(n)} \equiv 1 \ (mod\ n)$.

Proof. Let $k_1, k_2, \ldots, k_{\phi(n)}$ be a complete set of residues prime to n. Since $gcd(a,n) = 1$, then $ak_1, ak_2, \ldots, ak_{\phi(n)}$ is also a complete set of residues prime to n. Then,

$$\begin{aligned} k_1 k_2 \ldots k_{\phi(n)} &\equiv ak_1 ak_2 \ldots ak_{\phi(n)} \pmod{n} \\ &\equiv a^{\phi(n)} k_1 k_2 \ldots k_{\phi(n)} \pmod{n} \end{aligned}$$

Since $gcd(k_i, n) = 1$, we can cancel k_i from each side which gives

$$1 \equiv a^{\phi(n)} \pmod{n}.$$

□

Theorem 1.2 *(Fermat's Little Theorem).*
If p is prime then $a^p \equiv a \ (mod\ p)$ and if $p \nmid a$ then $a^{p-1} \equiv 1 \ (mod\ p)$.

Proof. $p \nmid a$ implies that $gcd(a, p) = 1$. Also, $\phi(p) = p - 1$ and so $a^{p-1} \equiv 1 \pmod{p}$. Multiplying by a proves the first result in the case $p \nmid a$. If $p|a$ then $a \equiv 0 \pmod{p}$ and so both sides are $0 \pmod{p}$. □

Theorem 1.3 *(Chinese Remainder Theorem).*
Let $m_1, m_2, \ldots, m_k$ be a collection of pairwise relatively prime integers. This means that

$$gcd(m_i, m_j) = 1 \text{ for all } i \neq j.$$

Let $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then the system of simultaneous congruences

$$x \equiv a_1 \ (mod\ m_1), x \equiv a_2 \ (mod\ m_2), \ldots, x \equiv a_k \ (mod\ m_k) \tag{1.1}$$

has a solution $x = c$. Further, if $x = c$ and $x = c'$ are both solutions, then

$$c \equiv c' \ (mod\ m_1 m_2 \ldots m_k). \tag{1.2}$$

Proof. (See [1, Theorem 2.25, p83]) □

1.4 Basic algorithms

Theorem 1.4 *(Division Algorithm), [52].*
Given any strictly positive integer d and any integer a, then there exist unique integers q and r such that

$$a = qd + r \text{ and } 0 \leq r < d.$$

Proof. To prove this algorithm, we need to look at the existence and uniqueness which are to be proved separately.

Lemma: If $a - qd \geq d$ for a certain value of q, then we can replace q by $q' = q + 1$ and still satisfy the condition $a - q'd \geq 0$.

Proof: If $a - qd \geq d$ and $q' = q + 1$, then $a - q'd = a - (q+1)d = a - qd - d \geq d - d = 0$. QED (Lemma).

Proof for existence:

Consider the set of all numbers of the form $a - qd$, such that q is an integer and $a - qd \geq 0$. There do exist numbers in the set: for instance, if a is positive, then a is in the set (i.e. choose $q = 0$), and if a is negative then $a - ad = -a(d-1) = |a|(d-1)$ is in the set (i.e. choose $q = a$) since by assumption d is strictly positive and so $d - 1 \geq 0$.

Since we have seen that the set of integers of the form $a - qd$ such that $a - qd \geq 0$ is not empty, this set has a smallest number $a - qd$. Then by assumption $a - qd \geq 0$. We claim that for this particular q, $a - qd < d$. In fact, if $a - qd \geq d$, then by the lemma above we can replace q by $q' = q + 1$ and still have $a - q'd \geq 0$. But if $q' = q + 1$ then $a - q'd$ is smaller than $q - qd$ (because $q' < q$ and $d > 0$, so $a - q'd < q - qd$), so if $a - q'd \geq 0$ this would contradict the fact that we have already chosen the smallest possible non-negative number of the form $a - qd$. This proves the claim that $a - qd < d$, and that proves the existence part of the Division algorithm theorem.

Proof for uniqueness:

Note first that since r is uniquely determined by q (i.e. since it is required that $r = a - qd$), what we need to show is that there exist a unique value of q such that $0 \leq a - qd < d$. Now suppose that q and q' are satisfy this condition, i.e. $0 \leq a - qd < d$ and $0 \leq a - q'd < d$ as well. Then by subtraction we see that since $a - q'd \geq 0$,

$$(q' - q)d = (a - qd) - (a - q'd) \leq a - qd < d,$$

and likewise

$$(q' - q)d = (a - qd) - (a - q'd) \geq 0 - (a - q'd) = -(a - q'd) > -d$$

since $a - q'd < d$. Together, these two inequalities says that $(q' - q)d$ is an integer strictly between $-d$ and d. Since $d > 0$, one can divide through by d to get

$$-1 < q' - q < 1.$$

Since $q' - q$ is an integer, this implies that $q' - q = 0$, (i.e. $q' = q$). This finishes the proof that q is unique and as previously noted it follows automatically that r must also be unique. □

Theorem 1.5 *(The Euclidean Algorithm).*
Let a and b be positive integers with $a \geq b$. The following algorithm computes the $gcd(a, b)$ in a finite number of steps.

1. *Let $r_0 = a$ and $r_1 = b$.*

2. *Set $i = 1$.*

3. *Divide r_{i-1} by r_i to get a quotient q_i and reminder r_{i+1},*

$$r_{i-1} = r_i \cdot q_i + r_{i+1} \text{ with } 0 \geq r_{i+1} < r_i.$$

4. *If the remainder $r_{i+1} = 0$, then $r_i = gcd(a, b)$ and the algorithm terminates.*

5. *Otherwise, $r_{i+1} > 0$, so set $i = i + 1$ and go to Step 3. The division step (Step 3) is executed at most*

$$2\log_2(b) + 1 \text{ times.}$$

Proof. (See [1, Theorem 1.7, p13]). □

It is easy to understand the algorithm of Theorem 1.5 if we use an example.

Example 1.1 *Finding the gcd of 97 and 56 by the Euclidean Algorithm:*

$$97 = 1(56) + 41$$

$$56 = 1(41) + 15$$

$$41 = 2(15) + 11$$

$$15 = 1(11) + 4$$

$$11 = 2(4) + 3$$

$$4 = 1(3) + 1$$

$$3 = 1(3) + 0$$

Thus, $gcd(81, 57) = 1$.

Theorem 1.6 *(Extended Euclidean Algorithm).*
Let a *and* b *be positive integers. Then the equation*

$$au + bv = gcd(a, b)$$

always has a solution in integers u *and* v.

Instead of a complete proof we give an example of a special case which illustrates the main idea of a complete proof.

Proof. Given $gcd(a, b) = au + bv = z$. Let $c_1 = a, c_2 = b, u_1 = 1, u_2 = 0, v_1 = 0, v_2 = 1$. Then,

$$c_1 = c_2q_2 + c_3$$

$$c_2 = c_3q_3 + c_4$$

$$c_3 = c_4q_4 + c_5$$

$$c_4 = c_5q_5 + c_6$$

$$c_5 = c_6q_6 + 0.$$

So, $gcd(a,b) = c_6 = z = au_6 + bv_6$. The backward recurrence is

$$\begin{aligned}
c_6 &= c_4 - c_5q_5 \\
&= c_4 - q_5(c_3 - c_4q_4) = c_4 - c_3q_5 + c_4q_4q_5 \\
&= c_4(1 + q_4q_5) - c_3q_5 \\
&= (c_2 - c_3q_3)(1 + q_4q_5) - c_3q_5 \\
&= c_2 + c_2q_4q_5 - c_3q_3 - c_3q_3q_4q_5 - c_3q_5 \\
&= c_2(1 + q_4q_5) + c_3(-q_3 - q_3q_4q_5 - q_5) \\
&= c_2(1 + q_4q_5) + (c_1 - c_2q_2)(-q_3 - q_3q_4q_5 - q_5) \\
&= c_2(1 + q_4q_5) - c_1q_3 - c_1q_3q_4q_5 - c_1q_5 + c_2q_2q_3 + c_2q_2q_3q_4q_5 + c_2q_5 \\
&= c_1(-q_3 - q_3q_4q_5 - q_5) + c_2(1 + q_4q_5 + q_2q_3 + q_2q_3q_4q_5 + q_5) \\
&= c_1u_5 + c_2v_5.
\end{aligned}$$

Thus, $u_5 = -q_3 - q_3q_4q_5 - q_5$ and $v_5 = 1 + q_4q_5 + q_2q_3 + q_2q_3q_4q_5 + q_5$. □

For the Extended Euclidean algorithm, it is easy to understand if we give an example to show how it works.

Example 1.2 *Take $a = 987, b = 543$. Apply the Euclidean Algorithm:*

- *Step 1:* $a_1 = 987, b_1 = 543$.

$$987 = 543 \cdot 1 + 444$$

- *Step 2:* $a_2 = 543, b_2 = 444$.

$$543 = 444 \cdot 1 + 99$$

- *Step 3:* $a_3 = 444, b_3 = 99$.

$$444 = 99 \cdot 4 + 48$$

- *Step 4:* $a_4 = 99, b_4 = 48$.

$$99 = 48 \cdot 2 + 3$$

- *Step 5:* $a_5 = 48, b_5 = 3$.

$$48 = 3 \cdot 16 + 0$$

So,

$$gcd(987, 543) = 3.$$

Reversing the steps enables us to write the greatest common divisor as a multiple of 987 *added to a multiple of* 543*:*

$$\begin{aligned} 3 &= 99 - 48 \cdot 2 \\ &= 99 - ((444 - 99 \cdot 4) \cdot 2) \\ &= 99 - (2 \cdot 444 - 99 \cdot 8) \\ &= 99 \cdot 9 - 2 \cdot 444 \\ &= 9 \cdot (543 - 444) - (2 \cdot 444) \\ &= 9 \cdot 543 - 7 \cdot 444 \\ &= 9 \cdot 543 - 7(987 - 543) \\ &= 2 \cdot 543 - 7 \cdot 987. \end{aligned}$$

So,

$$gcd(987, 543) = 3 = (-7) \cdot 987 + 2 \cdot 543$$

and we can take $u = -7$ *and* $v = 3$.

1.5 The Diffie-Hellman key exchange method.

Here I give the steps in the well-known Diffie-Hellman key exchange method.

1. Alice and Bob are agree to use the large prime p with nonzero integer g modulo p. Then they make the values of p and g available as public knowledge. If possible, g is chosen such that its order (i.e., the order g of is the smallest natural number n such that $g^n \equiv 1 \pmod{\text{p}}$) in $\mathbb{F}_p^*$ (the multiplicative group of the finite field of prime order p) is a large prime.

2. Alice has to pick a secret integer known to her only, say a, (i.e. she does not tell anyone the value of a). At the same time, Bob also picks an integer b that he keeps secret. Then Alice and Bob use their secret integers to compute $A \equiv g^a \pmod{p}$ and $B \equiv g^b \pmod{p}$ respectively.

3. Then Alice sends A to Bob and Bob sends B to Alice. Notice that a third person, might be able to observe the values of A and B.

4. Lastly, Alice and Bob use their secret integers to calculate as follows:

$$\text{Alice computes : } A' \equiv B^a \pmod{p} \text{ and}$$
$$\text{Bob computes : } B' \equiv A^b \pmod{p}.$$

Note that $A' \equiv B^a \equiv (g^b)^a \equiv (g^a)^b \equiv A^b \equiv B' \pmod{p}$, so $A' \equiv B' \pmod{p}$. This common value A' and B' is their exchange key.

Example 1.3 *1. Alice and Bob agree to use the prime* $p = 937$ *and the primitive root* $g = 610$.

2. Alice chooses the secret key $a = 345$ *and computes*

$$A \equiv g^a \ (mod\ p) \equiv 610^{345} \ (mod\ 937) \equiv 872 \ (mod\ 937).$$

Similarly, Bob chooses the secret key $b = 789$ *and computes*

$$B \equiv g^b \ (mod\ p) \equiv 610^{789} \ (mod\ 937) \equiv 223 \ (mod\ 937).$$

3. *Alice sends Bob the number* 872 *and Bob sends Alice the number* 223. *These transmission are done over an insecure channel, so both* $A = 872$ *and* $B = 223$ *is considered as a public knowledge. But the private keys* $a = 345$ *and* $b = 789$ *are remain secret.*

4. *Suppose that an eavesdropper, say Eve, sees this entire exchange. So she can reconstitute Alice's and Bob's shared secret if she can solve either of the congruences:*

$$A' \equiv B^a \ (mod\ p) \equiv 223^a \ (mod\ 937) \equiv 520 \ (mod\ 937) \ or$$
$$B' \equiv A^b \ (mod\ p) \equiv 872^b \ (mod\ 937) \equiv 520 \ (mod\ 937),$$

for a and b, since then she will know one of their secret exponents.

As far as is known, this is the only way for Eve to find the secret shared value without Alice's or Bob's assistance.

1.6 The El-Gamal public key cryptosystem

The El-Gamal public key cryptosystem was invented by Taher ElGamal in 1985, [64]. This cryptosystem is based on the discrete logarithm problem which is also connected to the Diffie-Hellman key exchange. Even though Diffie-Hellman gives a method of transporting a secret key, it does not attain all the objectives of public key cryptosystems. The Diffie-Hellman method only provides a solution for the key distribution problem while the El-Gamal public key cryptosystem solves the entire problem. A summary of El-Gamal public key cryptosystem is given below.

Public Parameter Creation	
A trusted party chooses and publishes a large prime p and an element g(mod p)of large (prime) order.	
Alice	Bob
Key creation	
Choose a private key $1 \leq a \leq p-1$, compute $A \equiv g^a (\text{mod } p)$, publish the public key A.	
Encryption	
	Choose a plaintext number m, encode as a number $\hat{m}$, choose a random ephemeral key k, use Alice's public key A to compute $c_1 \equiv gk (\text{mod } p)$ and $c_2 \equiv \hat{m}A^k (\text{mod } p)$, Send the ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} * c_2 (\text{mod } p)$, This quantity is equal to $\hat{m}$.	

Table 1.1: El-Gamal key creation, encryption and decryption, [1, Table 2.3, p70].

The following is an example using the El-Gamal public key cryptosystem.

Example 1.4 *Bob chooses a prime* $p = 107$ *and primitive element* $g = 2$. *Alice chooses* $a = 99$ *to be her private key. Then she computes and publishes her public key A:*

$$A \equiv g^a \ (mod\ p) \equiv 2^{99} \ (mod\ 107) \equiv 51 \ (mod\ 107).$$

Bob decides to send Alice the message encoded by $m = 55$. *He chooses an ephemeral key* $k = 197$ *and computes two quantities*

$$c_1 \equiv 2^{197} \equiv 70 \ (mod\ 107) \ and$$
$$c_2 \equiv 55 \cdot 51^{197} \equiv 81 \ (mod\ 107).$$

The pair $(c_1, c_2) = (70, 81)$ *is the ciphertext that Bob sends to Alice. Alice, using her private key* $a = 99$, *first computes*

$$(c_1)^a \equiv 70^{99} \equiv 54 \ (mod\ 107) \ and\ then$$
$$((c_1)^a)^{-1} \equiv 2 \ (mod\ 107).$$

Finally, Alice computes

$$((c_1)^a)^{-1} \cdot c_2 \ (mod\ p) \equiv 2 \cdot 81 \equiv 55 \ (mod\ 107),$$

and recovers the plaintext message $m = 55$.

Chapter 2

The RSA cryptosystem

Introduction: The RSA algorithm was developed by three reseachers, Rivest, Shamir and Adleman in 1978, [60]. It is one of the most world famous public-key cryptosystems. Its purpose is to secure communication via networks by using public keys to encrypt and decrypt messages, where a private key is kept secret.

In this chapter I describe the theories that are related to the RSA cryptosystem. These are integer factorization, the RSA algorithm, primality testing and solving the discrete logarithm problem in finite field. Also, I give some applications of the RSA cryptosystem in the real world. Basically the RSA cryptosystem is based on modular exponentiation. The modulus N is the product of two large primes $N = pq$. I start with Euler's formula which is the fundamental formula for RSA cryptosystems.

2.1 Euler's formula and roots modulo pq

Theorem 2.1 *(Euler's Formula for pq). [1, Theorem 3.1, p114]*
Let p and q be distinct odd primes and let $g = gcd(p-1, q-1)$. Then, $a^{(p-1)(q-1)/g} \equiv 1 (mod\ pq)$, for all a satisfying $gcd(a, pq) = 1$.

Proof. By assumption, we know that p does not divide a and that g divides $q-1$, so we can compute

$$\begin{aligned} a^{(p-1)(q-1)/g} &= (a^{(p-1)})^{(q-1)/g}, \quad ((q-1)/g, \text{ is an integer}) \\ &\equiv 1^{(q-1)/g} \pmod{p}, \quad (a^{p-1} \equiv 1 \pmod{p}, \text{ from Fermat Little Theorem}) \\ &\equiv 1 (\text{mod } p). \end{aligned}$$

The exact same computation, reversing the roles p and q, shows that $a^{(p-1)(q-1)/g} \equiv 1 \pmod{q}$. This proves that $a^{(p-1)(q-1)/g} - 1$ is divisible by both p and q. Hence, it is divisible by pq. □

The difficulty of finding e^{th} roots modulo N (i.e. solving equations of the form $x^e \equiv c \pmod{N}$) makes the RSA cryptosystem very secure. The next proposition is to take e^{th} roots modulo N, where the modulus N is prime.

Proposition 2.2 *[1, Proposition 3.2, p115]*
Let p be a prime and let $e \geq 1$ be an integer satisfying $gcd(e, p-1) = 1$. Then e has an inverse d modulo $p-1$, $de \equiv 1 \pmod{p-1}$, and the congruence $x^e \equiv c \pmod{p}$ has the unique modulo p solution $x \equiv c^d \pmod{p}$.

Proof. Let $c \equiv 0 \pmod{p}$. Then we set $x = 0$ and we are done. Let $c \not\equiv 0 \pmod{p}$. Then, there exist an integer d such that $de \equiv 1 \pmod{p-1}$ i.e. $de = 1 + k(p-1)$ where k is a positive integer.

We need to check that $x^e \equiv c \pmod{p}$:

$$\begin{aligned} x^e &\equiv (c^d)^e \\ &\equiv c^{de} \pmod{p} \\ &\equiv c^{1+k(p-1)} \pmod{p}, \quad (\text{since } de = 1 + k(p-1)) \\ &\equiv c^1 \cdot c^{k(p-1)} \pmod{p} \\ &\equiv c \cdot (c^{p-1})^k \pmod{p} \\ &\equiv c \cdot 1^k \pmod{p}, \quad (\text{by Fermat's Little Theorem}) \\ &\equiv c \pmod{p}. \end{aligned}$$

This shows that c^d is the solution for $x^e \equiv c \pmod{p}$, (i.e. $x = c^d$).
We need to show the solution is unique. Let x_1 and x_2 are the solutions to $x^e \equiv c \pmod{p}$. Then

$$x_1 \equiv x_1^{de} \equiv (x_1^e)^d \equiv c^d \equiv (x_2^e)^d \equiv x_2^{de} \equiv x_2 \pmod{p}.$$

Thus, $x_1 \equiv x_2 \pmod{p}$ and $x^e \equiv c \pmod{p}$ has an unique solution modulo p.
□

Example 2.1 *Let* $p = 127, q = 131, n = 127 * 131 = 16637$ *and* $d = 157$. *Then,* $\varphi(16637) = 126 * 130 = 16380$. *The Extended Euclidean algorithm (Theorem 1.6) is a procedure to find* α, β, *and* c *where* $\alpha * a + \beta * b = c$, *for integers* a, b, *and* c *such that* $gcd(a, b) = c$. *If we compute* e *using the Extended Euclidean algorithm we can set* $a = \varphi(n), b = d$ *and we know that, since* $\varphi(n)$ *and* d *are relatively prime, at the end of the algorithm we will obtain* $c = 1$. *However, we will also obtain* α *and* β *where* $\alpha * \varphi(n) + \beta * d = 1$, *and* β *will be the multiplicative inverse of* $d \pmod{\varphi(n)}$. *Using this procedure we arrive at* $e = 157^{-1} \pmod{126} = 61$. *Suppose we have a message*

$$m = MY\ BEST\ FRIEND.$$

Then, we can set each letter in the alphabet equal to a two-digit number. This will ensure that there is no ambiguity when encoding and decoding. If $A = 1, B = 2, \ldots,$ *then 12 could mean AB or L. Therefore we set* $blank = 00, A = 01, B = 02, \ldots, Z = 26$. *The encoded message becomes*

$$m = 1325\ 0002\ 0519\ 2000\ 0618\ 0905\ 1404.$$

Note that the message has is broken into 7 blocks of two letters each. If we put it in blocks of three letters, they would not necessarily each be less than $n - 1 = 16636$. *Let* m_1 *be the first block of the message. Then to encipher* m_1 *we calculate*

$$E(m_1) \equiv (m_1)^e \equiv (1325)^{61} \equiv 3164 \ (mod\ 16637).$$

$$E(m_2) \equiv (m_2)^e \equiv (2)^{61} \equiv 6509 \ (mod\ 16637).$$

$$E(m_3) \equiv (m_3)^e \equiv (519)^{61} \equiv 6371 \ (mod\ 16637).$$

$$E(m_4) \equiv (m_4)^e \equiv (2000)^{61} \equiv 1762 \ (mod\ 16637).$$

$$E(m_5) \equiv (m_5)^e \equiv (618)^{61} \equiv 9046 \ (mod\ 16637).$$

$$E(m_6) \equiv (m_6)^e \equiv (905)^{61} \equiv 5271 \ (mod\ 16637).$$

$$E(m_7) \equiv (m_7)^e \equiv (1404)^{61} \equiv 9963 \ (mod\ 16637).$$

Let c denote the ciphertext for the entire message, then

$$c = 3164\ 6509\ 6371\ 1762\ 9046\ 5271\ 9963.$$

It is easy to check that the deciphering method works. For example for m_1, $3164^{157} \equiv 1325 \ (mod\ 16637)$.

The next proposition is quite similar to Proposition 2.2, but this proposition describes what to do if $N = pq$, where p and q are primes.

Proposition 2.3 *(Modulo pq) [1, Proposition 3.4, p116] Let p and q be distinct primes and let* $e \geq 1$ *satisfy* $gcd(e, (p-1)(q-1)) = 1$, *so e has an*

inverse modulo $(p-1)(q-1)$*, say* $de \equiv 1 \ (mod (p-1)(q-1))$*. Then, the congruence,* $x^e \equiv c \ (mod \ pq)$ *has the unique solution* $x \equiv c^d \ (mod \ pq)$*.*

Proof. We assume that $gcd(c, pq) = 1$. The congruence $de \equiv 1 \pmod{(p-1)(q-1)}$ means that there is an integer k such that $de \equiv 1 + k(p-1)(q-1)$. Now, we check that c^d is a solution to $x^e \equiv c \pmod{pq}$:

$$\begin{aligned}
(c^d)^e &\equiv c^{de} \pmod{pq} \\
&\equiv c^{1+k(p-1)(q-1)} \pmod{pq} \\
&\equiv c(c^{(p-1)(q-1)})^k \pmod{pq} \\
&\equiv c \cdot 1^k \pmod{pq} \\
&\equiv c \pmod{pq}.
\end{aligned}$$

This completes the proof that $x \equiv c^d$ is a solution to the congruence $x^e \equiv c \pmod{pq}$. I need to show that the solution is unique. Suppose that $x = u$ is a solution to the congruence, then

$$\begin{aligned}
u &\equiv u^{de-k(p-1)(q-1)} \pmod{pq}, \quad \text{since } de = 1 + k(p-1)(q-1) \\
&\equiv (u^e)^d \cdot (u^{(p-1)(q-1)})^{-k} \pmod{pq} \\
&\equiv (u^e)^d \cdot 1^{-k} \pmod{pq} \\
&\equiv c^d \pmod{pq}.
\end{aligned}$$

Thus, every solution to the congruence is equal to $c^d \pmod{pq}$, so this is the unique solution. □

Example 2.2 *We solve the congruence,*

$$x^{18761} \equiv 32198 \ (mod \ 27221)$$

where the modulus $N = 27221 = 163 \cdot 167$ *is the product of the two primes* $p = 163$ *and* $q = 167$*. The first step is to solve the congruence*

$$18761 \cdot d \equiv 1 \ (mod\ 26892)$$

where $26892 = (p-1)(q-1) = 162 \cdot 166$. *The solution for* d *is* $d \equiv 10901 \ (mod\ 26892)$. *Then,* $x \equiv 32198^{10901} \equiv 13619 \ (mod\ 27221)$ *is the solution to* $x^{18761} \equiv 32198 \ (mod\ 27221)$ *or we have*

$$g = gcd(p-1, q-1) = gcd(162, 166) = 2,$$

so $(p-1)(q-1)/g = (162)(166)/2 = 13446$, *means we can find a value of* d. *Solving the congruence,* $18761 \cdot d \equiv 1 \ (mod\ 13446)$. *The solution is*

$$d \equiv 10901 \ (mod\ 13446),$$

then $x \equiv 32198^{10901} \equiv 13619 \ (mod\ 27221)$ *is the solution to*

$$x^{18761} \equiv 32198 \ (mod\ 27221).$$

2.2 Integer Factorization

Introduction: The security of the RSA cryptosystem and elliptic curve cryptography depends on large prime numbers (i.e. the factors of the modulus N). To break a system, we simply need to factor $N = pq$ to discover p and q. This section describes four methods for factorization. If N is very large, this problem is difficult, especially if p and q are themselves also large. Here four of the early methods used to factor integers are given. There is no attempt here to be comprehensive. We describe the difference of two squares factorization, the trial division method, the Pollard's $p-1$ factorization method and conclude with Lenstra's elliptic curve factorization method.

2.2.1 Difference of two squares factorization.

This factorization is sometimes known as a quadratic sieve. We start with the simple factorization,

$$X^2 - Y^2 = (X + Y)(X - Y).$$

Suppose we need to factor a number N, where $N + b^2$, for some integer b, is a perfect square, say a^2. Then, $N + b^2 = a^2$, so

$$N = a^2 - b^2 = (a + b)(a - b),$$

and we have a factorization of N.

Example 2.3 *We factor* $N = 34571$ *by looking for an integer* b *making* $N + b^2$ *a perfect square:*

$$\begin{aligned}
&34571 + 1^2 = 34572, && \textit{Not a square},\\
&34571 + 2^2 = 34575, && \textit{Not a square},\\
&34571 + 3^2 = 34580, && \textit{Not a square},\\
&34571 + 4^2 = 34587, && \textit{Not a square},\\
&34571 + 5^2 = 34596 = 186^2, && \textit{A square}.
\end{aligned}$$

Then we compute

$$34571 = 186^2 - 5^2 = (186 + 5)(186 - 5) = 191 \cdot 181.$$

The numbers 191 *and* 181 *are primes, so the factorization of* N *is* $34571 = 191 \cdot 181$.

2.2.2 Trial Division.

The trial division method seeks to find a factor of N by checking all possible prime factors of N. Trial division algorithm checks for all prime numbers p that are less than or equal to $\sqrt{N}$, whether they divide N. If the algorithm fails (i.e. none of the prime numbers p divides N), then it shows that N is prime. Trial division is an inefficient algorithm for large numbers N with large prime factors. In factorization, trial division is usually applied to find

any small prime factors. This leads us to the following definition and theorem.

Definition 2.1 *Given a composite integer N (i.e. N can be factored), then trial division consists of trial-dividing N by every prime number less than or equal to $\sqrt{N}$.*

Theorem 2.4 *[57, Theorem 7.1.1, p152] If N is a composite positive integer, then N has a prime divisor p which is less than or equal to $\sqrt{N}$.*

Proof. Since N is composite, we can write $N = ab$ with $a > 1$ and $b > 1$. Now we have $a \leq \sqrt{N}$ or $b \leq \sqrt{N}$, since otherwise

$$N = ab > \sqrt{N}\sqrt{N} = N.$$

Suppose that $a \leq \sqrt{N}$. Then, a has a prime divisor p which also divides N. Thus, $p \leq a \leq \sqrt{N}$. □

Example 2.4 *We use trial division to factor* 584. *The first prime divisor that we find is* 2 *and* $\frac{584}{2} = 292$. *The next prime factor is again* 2 *and* $\frac{292}{2} = 146$. *Similarly, the next factor is also* 2 *and* $\frac{146}{2} = 73$. *The number* 73 *is prime. Hence, the prime factorization of* 584 *is*

$$584 = 2^3 \cdot 73.$$

Trial division also can be used to decide whether a number N is prime. This leads us to the following example.

Example 2.5 *Let* $N = 120643$ *is prime. We have*

$$\lfloor \sqrt{N} \rfloor = \lfloor \sqrt{120643} \rfloor = 347.$$

Hence, we must test whether one of the prime numbers $p \leq 347$ *divides* N. *The primes* $p \leq 347$ *are*

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,$
$101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181,$
$191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271,$
$277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347.$

The primes which divide N are 223 and 541. Therefore, N is a not prime.

Example 2.6 *We use trial division to factor $N = 1549$. So we have*

$$\lfloor \sqrt{N} \rfloor = \lfloor \sqrt{1549} \rfloor = 39.$$

So, we must test whether one of the prime numbers $p \leq 39$ divides N. The primes $p \leq 39$ are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.
By observation, none of the 12 primes divides N evenly. Thus, N is a prime number.

2.2.3 Pollard's $p-1$ factorization algorithm.

Pollard's $p-1$ algorithm was invented by John Pollard in 1974, [65]. This algorithm finds, a factor of $N \in \mathbb{N}$. Following are the steps of the algorithm.

1. Given a number $N = pq$ and we need to find the prime factors p and q. Suppose that we search for an integer L such that

   $$p-1 | L \text{ and } q-1 \nmid L.$$

   This means that there are integers i, j and k with $k \neq 0$ satisfying

   $$L = i(p-1) \text{ and } L = j(q-1) + k.$$

2. Choose an integer a (i.e. by assuming $p \nmid a$ and $q \nmid a$) and compute a^L. Fermat's Little Theorem (Theorem 1.2) tells that

   $$a^L = a^{i(p-1)} = a^{(p-1)i} \equiv 1^i \equiv 1 \pmod{p},$$
   $$a^L = a^{j(q-1)+k} = a^k \cdot a^{(q-1)j} \equiv a^k \cdot 1^j \equiv a^k \pmod{q}.$$

3. The exponent $k \neq 0$, so $a^k \not\equiv 1 \pmod{q}$.

4. So for the given value of a, we find that

$$p|a^L - 1 \text{ and } q \not| a^L - 1.$$

   This implies that $p = gcd(a^L - 1, N)$.

5. If $p - 1$ is a product of small primes, then $p - 1|n!$ for some n (i.e. Let $n = 2, 3, \ldots$, then compute $p = gcd(a^{n!} - 1, N)$).

6. If $gcd(a^{n!} - 1, N) = 1$, then go on to the next value of n. Otherwise, we have a nontrivial factor of N. But if $p = N$, then this algorithm is fails.

Example 2.7 *We use Pollard's $p - 1$ algorithm to factor $N = 220459$.*

$$gcd(2^{2!} - 1, 220459) = 1$$

$$gcd(2^{3!} - 1, 220459) = 1$$

$$gcd(2^{4!} - 1, 220459) = 1$$

$$gcd(2^{5!} - 1, 220459) = 1$$

$$gcd(2^{6!} - 1, 220459) = 1$$

$$gcd(2^{7!} - 1, 220459) = 1$$

$$gcd(2^{8!} - 1, 220459) = 449$$

The final line gives us a nontrivial factor $p = 449$ of N. This factor is prime, and the other factor $q = \frac{N}{p} = \frac{220459}{449} = 491$ is also prime. The reason that an exponent of $8!$ worked in this instance is that $p - 1$ factors into a product of small primes,

$$p - 1 = 448 = 2^6 \cdot 7|8! = 90.$$

The other factor satisfies

$$q - 1 = 490 = 2 \cdot 5 \cdot 7^2 \not| 8! = \tfrac{576}{7},$$

which also a product of a small primes.

2.2.4 Lenstra's factorization algorithm using elliptic curves.

Lenstra's elliptic curve method was invented by Hendrik Lenstra to solve the problems of factoring integers into a product of two primes, [75].
Pollard's method presented in the previous section is based on the non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ form a multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p-1$.
However, Lenstra's method replaces the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$ by the group of points on an elliptic curve $E(\mathbb{F}_p)$, and an integer a by a point $P \in E(\mathbb{F}_p)$. By choosing an integer k as a product of small primes, so the number of elements of $E(\mathbb{F}_p)|k$, which implies $kP = \mathcal{O} \in E(\mathbb{F}_p)$. Using this idea we can get a non-trivial factor of N.
Pollard's method fails if $N = pq$ then both $p-1$ and $q-1$ have large prime factors. However Lenstra's method is flexible. If it fails using a particular elliptic curve, we can choose a new curve and start over again.
Note that these are unclear explanations but consider it as an algorithm.
Note that

$$\#E(\mathbb{F}_p) = p - 1 - \varepsilon_p \text{ with } |\varepsilon_p| \leq 2\sqrt{p}, \text{ [72, p133].}$$

As the curve E varies over all such curves, the numbers ε_p are reasonably uniformly distributed over an interval of length $4\sqrt{p}$. Thus, we can find a curve E with the number of elements of $E(\mathbb{F}_p)$ equal to a product of small primes.
There is some basic information about elliptic curve and the group structure in Chapter 3.
Lenstra's elliptic curve factorization algorithm: [72, 56]
Choose a composite integer $N \geq 2$.

1. Check $gcd(N, 6) = 1$ so that $N \neq m^r$ for any $r \geq 2$.

2. Choose any integers A, x_1 and y_1 such that $1 < A, x_1, y_1 < N$.

3. Let E be an elliptic curve, $E : y^2 = x^3 + Ax + B$.

   Let $B = y_1^2 - x_1^2 - Ax_1$ and point $P = (x_1, y_1) \in E$.

4. Check that $a = gcd(4A^3 + 27B^2, N) = 1$.

   If $a = N$, then return to step 2 and choose a new integer A.

   If $1 < a < N$, then a is a non-trivial factor of N and we are done.

5. Choose an integer k such that

$$k = LCM\{1, 2, 3, \ldots, K\} \text{ for some } K \in \mathbb{N}.$$

6. Compute

$$\begin{aligned} kP &= (\frac{a_k}{d_k^2}, \frac{b_k}{d_k^3}) \\ &= 1P + 2P + 2^2P + 2^3P + \ldots + 2^rP, \quad \text{for some } r \in \mathbb{N} \\ &= P_0 + P_1 + P_2 + P_3 + \ldots + P_r, \quad \text{for some } r \in \mathbb{N} \\ &= \sum_{k_i=1}^{r} P_i. \end{aligned}$$

7. Calculate $D = gcd(d_k, N)$.

   If $1 < D < N$, then D is a non-trial factor of N and we are done.

   If $D = 1$, then return to step 2 and choose a new integer A.

   If $D = N$, then return to step 5 and decrease the value of k.

Example 2.8 *Let* $N = 1999843247$*, a point* $P = (2, 1)$ *and elliptic curve* $E : y^2 = x^3 + Ax + B$*. Note that* $gcd(N, 6) = 1$*. Let* $A = 6$ *implies* $B = y^2 - x^3 - Ax = -19$*. So,* $E : y^2 = x^3 + 6x - 19$ *and a point* $P = (2, 1) \in E$*.*

Now, choose

$$\begin{aligned} k &= LCM\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\} \\ &= 232792560 \\ &= 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^{13} + 2^{21} + 2^{22} + 2^{23} + 2^{24} + 2^{26} + 2^{27}. \end{aligned}$$

So,

r	$2^r P \ (mod\ 1999843247)$
0	$(2, 1)$
1	$(77, 1999842571)$
2	$(1010023132, 416202416)$
3	$(1821315272, 1927904597)$
4	$(672263808, 912268394)$
5	$(1937039248, 1450774960)$
6	$(995387252, 445795708)$
7	$(1963543744, 228429936)$
8	$(213910635, 1203300646)$

r	$2^r P \ (mod\ 1999843247)$
9	$(1925178367, 1096237088)$
10	$(1031420139, 455919973)$
11	$(1369870593, 830431437)$
12	$(1061855853, 264657833)$
13	$(758379778, 916045511)$
14	$(568842154, 1701729891)$
15	$(1343153277, 600645524)$
16	$(1053104612, 438503062)$
17	$(1060705278, 1183122481)$
18	$(434698066, 1218407806)$
19	$(614705915, 351047729)$
20	$(418567986, 241447683)$
21	$(1745194563, 793504621)$
22	$(777079984, 1688813810)$
23	$(1766760042, 1954188834)$
24	$(266756875, 696952738)$
25	$(1771573042, 1664186057)$
26	$(1658585264, 842158092)$
27	$(998323914, 274099838)$

I then compute $kP = 232792560P$,

$$2^4P = 16P = (1053104612, 438503062)$$

$$(2^4 + 2^5)P = 48P = (689737312, 766476874)$$

$$(2^4 + 2^5 + 2^6)P = 112P = (326736690, 931029681)$$

$$(\textit{previous partial sum}) + 2^7P = 240P = (392582429, 1939553715)$$

$$(\textit{previous partial sum}) + 2^8P = 496P = (582646364, 295105563)$$

$$(\textit{previous partial sum}) + 2^{13}P = 8688P = (1055413349, 1526098803)$$

$$(\textit{previous partial sum}) + 2^{21}P = 2105840P = (1985478926, 1966774618)$$

$$(\textit{previous partial sum}) + 2^{22}P = 6300144P = (1852388958, 510710323)$$

$$(\textit{previous partial sum}) + 2^{23}P = 14688752P = (896131026, 1237386275)$$

$$(\textit{previous partial sum}) + 2^{24}P = 31465968P = (1774327685, 1451569673)$$

$$(\textit{previous partial sum}) + 2^{26}P = 98574832P = (1634636045, 1074342536)$$

$$(\textit{previous partial sum}) + 2^{27}P = 232792560P = \quad \textit{The addition law breaks here.}$$

The addition law breaks when we want to find the inverse modulo N *of the difference of x-coordinates between* $98574832P$ *and* $2^{27}P$. *We obtain the* $gcd(1634636045 - 998323914, N) = 569 \neq 1$ *which gives us the factor of* $N = 569 \cdot 6514663$.

2.2.5 State of the art of integer factorization

Several factorization algorithms have been discovered which factor an integer N which is a product of two primes faster than the 4 methods given above. On 9 May 2005, the factorization of RSA-200 (i.e. a 663 bit number of 200 decimal numbers) was announced by the German Federal Agency's team. This algorithm was designed using general number field sieve (i.e. for factoring numbers which have between 100 and 200 digits) with efficiency which is

$$O(exp((\tfrac{64}{9}n)^{\frac{1}{3}}(logn)^{\frac{2}{3}})).$$

On 4 November 2005, the same team announced the factorization of RSA-640 which is 640 bits long (i.e. 193 decimal digits). These factorizations need a few months using ordinary computer time, [68]. In August 1999, the largest semiprime (i.e numbers with two prime factors) factored was RSA-155 (155 bits) using general number field sieve algorithms on 300 workstations and personal computers. This factorization required 7.4 months, [70].
For a quantum computer, Shor's algorithm solves the problem in polynomial time. It was discovered by Peter Shor in 1994. Shor's algorithm requires only $O(n^3)$ time and $O(n)$ space on n-bit number inputs. The first 7-qubit quantum computer ran Shor's algorithm in 2001 and factored the number 15, [69].

2.3 The RSA Algorithm

Suppose Alice wants to send a message to Bob over an insecure communication line, but has a problem sending sensitive information.
The RSA algorithm is based on the following idea: [1, Section 3.2, p119]

1. Setup
    - Let p and q be large primes, let $N = pq$ and let e and c be integers.
2. Problem
    - Solve the congruence $x^e \equiv c \pmod{N}$ for the unknown x.
3. Easy
    - Bob, who knows the values of p and q can easily solve for x.
4. Hard

- Eve, who does not know the values of p and q, cannot easily find x.

5. Dichotomy

   - Solving $x^e \equiv c \pmod{N}$ is easy for a person who possesses certain extra information, but it is apparently hard for all other people.

Example 2.9 *We illustrate the RSA public key cryptosystem with a small numerical example:*

1. RSA Key Creation

- *Bob chooses two secret primes* $p = 1597$ *and* $q = 1481$.
  Bob computes his public modulus, $N = pq = 1597 \cdot 1481 = 2365157$.

- *Bob chooses a public encryption exponent* $e = 25637$ *with the property that* $gcd(e, (p-1)(q-1)) = gcd(25637, 2362080) = 1$.

2. RSA Encryption

- *Alice converts her plaintext into an integer* $m = 1987654$ *satisfying* $1 \leq m < N$.

- *Alice uses Bob's public key* $(N, e) = (2365157, 25637)$ *to compute* $c \equiv m^e \ (mod\ N)$, $c \equiv 1987654^{25637} \equiv 1563057 \ (mod\ 2365157)$

- *Alice sends the ciphertext* $c = 1563057$ *to Bob.*

3. RSA Decryption

- *Bob knows* $(p-1)(q-1) = 1596 \cdot 1480 = 2362080$. *So he can solve,* $ed \equiv 1 \ (mod\ (p-1)(q-1))$ *implies* $25637 \cdot d = 1 \ (mod\ 2362080)$ *for* d *and find that* $d = 984653$.

- *Bob takes the ciphertext* $c = 1563057$ *and computes* $c^d \pmod N$, $1563057^{984653} \equiv 1987654 \pmod{2365157}$. *The value that he computes is Alice's message* $m = 1987654$.

We summarized the RSA cryptosystem in the table:

Bob	Alice
Key creation	
Choose secret primes p and q, choose encryption exponent e with $gcd(e,(p-1)(q-1)) = 1$. Publish $N = pq$ and e.	
Encryption	
	Chooses plaintext m.
	Use Bob's public key (N,e) to compute $c \equiv m^e \pmod N$. Sends ciphertext c to Bob.
Decryption	
Compute d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. Compute $m' \equiv c^d \pmod N$. Then, m' equals the plaintext m.	

Table 2.1: RSA key creation, encryption and decryption, [1, Table 3.1, p119]

2.4 Primality testing

The purpose of this section is to describe the primality tests, i.e. algorithms which determine whether a number is prime or not with probability 1.
The situation is as follows: Bob uses his RSA public/private key pair to communicate with Alice. So, Bob needs to choose primes p and q that are very large to form a RSA key pair. If p and q are small primes, then the eavesdropper, say Eve, can find the factors p and q and break Bob's system. Assume Bob knows how to distinguish prime and composite numbers. Then he can choose large random numbers until he finds one that is prime.
Fermat's Little theorem says if p is prime then $a^{p-1} \equiv 1 \pmod{p}$. We state a suitable version of Fermat's Little theorem that puts no restriction on a.

Theorem 2.5 *(Fermat's Little Theorem, Version 2)*
Let p be a prime number. Then

$$a^p \equiv a \ (mod\ p),$$

for every integer a.

Proof. If $p \not| a$, then the first version of Fermat's Little Theorem (Theorem 1.2) implies that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplying both sides by a proves that $a^p \equiv a \pmod{p}$ is true. On the other hand, if $p|a$, then both sides of $a^p \equiv a \pmod{p}$ are 0 modulo p. □

The compositeness test given below shows that a number is composite with a probability 1 or prime with probability 1. We need to check whether n is composite. This leads us to make the following definition.

Definition 2.2 *Fix an integer n. We say that an integer a is a witness for (the compositeness of) n if $a^n \not\equiv a \ (mod\ n)$.*

The next proposition is used to formulate the so-called Miller-Rabin test which is used to test whether a number is (probably) prime.

Proposition 2.6 *[1, Proposition 3.16, p126]*
Let p be an odd prime and write

$$p - 1 = 2^k q, \text{ with } q \text{ an odd integer.}$$

Let a be any number not divisible by p. Then one of the following two conditions is true:
(i) a^q is congruent to 1 modulo p.
(ii) One of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to -1 modulo p.

Proof. Fermat's Little Theorem (Theorem 1.2) tells us that $a^{p-1} \equiv 1 \pmod{p}$. This means that when we look at the list of numbers

$$a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}, a^{2^k q},$$

we know that the last number in the list, which equals a^{p-1}, is congruent to 1 modulo p. Further, each number in the list is the square of the previous number. Therefore one of the following two possibilities must occur:
(i) The first number in the list is congruent to 1 modulo p.
(ii) Some number in the list is not congruent to 1 modulo p, but when it squared, it becomes congruent to 1 modulo p. But the only number satisfying both

$$b \not\equiv 1 \pmod{p} \text{ and } b^2 \equiv 1 \pmod{p}$$

is -1, so one of the numbers in the list is congruent to -1 modulo p. □

If the number n is definitely composite number then it can be said that a is a Miller-Rabin witness for n. This is given more precisely by the following definition.

Definition 2.3 *Let n be an odd number and write $n-1 = 2^k q$ with q an odd integer. An integer a satisfying $gcd(a, n) = 1$ is called a Miller-Rabin witness for (the compositeness of) n if both of the following conditions are true:*
(a) $a^q \not\equiv 1 \ (mod\ n)$.
(b) $a^{2^i q} \not\equiv -1 \ (mod\ n)$ for all $i = 0, 1, 2, \ldots, k-1$.

Note: A Carmichael number is a composite positive integer n which satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all integers b which are relatively prime to n.

Example 2.10 *We illustrate the Miller-Rabin test with $a = 4$ and the number $n = 561$, which you may recall, is Carmichael number. We factor*

$$n - 1 = 560 = 2^4 \cdot 35$$

and compute

$$4^{35} \equiv 166 \ (mod\ 561),$$
$$4^{2 \cdot 35} \equiv 166^2 \equiv 67 \ (mod\ 561),$$
$$4^{4 \cdot 35} \equiv 67^2 \equiv 1 \ (mod\ 561).$$

The first number $4^{35} \ (mod\ 561)$ is neither 1 nor -1, and the other numbers in the list are not congruent to -1, so 4 is the Miller-Rabin witness to the fact that 561 is composite.

2.5 The discrete logarithm problem (DLP) in a finite field ($\mathbb{F}_p$)

Introduction: The discrete logarithm problem can be solved using ideas from the "index calculus". We use an example to understand easily how the DLP works.

Example 2.11 *Let p be the prime $p = 18757$ and use the index calculus to solve the discrete logarithm problem*

$$2^x \equiv 211 \ (mod\ 18757).$$

We note that $g = 2$ is a primitive root modulo $p = 18757$. We take $B = 5$, so our so-called factor base is the set of primes $\{2, 3, 5\}$. We start by taking random powers of $g = 2$ modulo 18757 and pick out the values that are B-smooth, (i.e. $g^n = 2^{e_1}3^{e_2}5^{e_3} \ (mod\ p), e_i \geq 0$). After several hundred attempts we obtain four equations/congruences:

$$g^{6819} \equiv 2^2 \cdot 3^2 \cdot 5 \ (mod\ 18757), \quad g^{8612} \equiv 2^3 \cdot 3^3 \cdot 5 \ (mod\ 18757),$$
$$g^{10053} \equiv 2^3 \cdot 3^2 \cdot 5^2 \ (mod\ 18757), \quad g^{12934} \equiv 2^2 \cdot 5^4 \ (mod\ 18757).$$

These in turn give linear relations for the discrete logarithms of $2, 3$ and 5 to base g. For example, the first one says that

$$6819 \equiv 2 \cdot log_g(2) + 2 \cdot log_g(3) + log_g(5) \ (mod\ p - 1),$$

where $log_g(a)$is the discrete logarithm value.To ease notation, we let

$$x_2 = log_g(2), \quad x_3 = log_g(3), \quad x_5 = log_g(5).$$

Then, the four congruences become the following four linear relations:

$$6819 = 2x_2 + 2x_3 + x_5 \ (mod\ 18756)$$
$$8612 = 3x_2 + 3x_3 + x_5 \ (mod\ 18756)$$
$$10053 = 3x_2 + 2x_3 + 2x_5 \ (mod\ 18756)$$
$$12934 = 2x_2 \qquad + 4x_5 \ (mod\ 18756)$$

Note that the formulas above are congruences modulo

$$p - 1 = 18756 = 36 \cdot 521,$$

since discrete logarithms are defined only modulo $p - 1$. The number 521 is prime, so we need to solve the system of linear equations modulo 36 and

modulo 521. *This is easily accomplished by Gaussian elimination, (i.e. by adding multiples of one equation to another to eliminate variables). The solutions are*

$$(x_2, x_3, x_5) \equiv (1, 28, 29) \ (mod\ 36),$$
$$(x_2, x_3, x_5) \equiv (1, 229, 107) \ (mod\ 521).$$

Combining these solutions yields

$$(x_2, x_3, x_5) \equiv (1, 1792, 3233) \ (mod\ 18756).$$

We check the solutions by computing

$$2^1 \equiv 2 \ (mod\ 18757), \quad 2^{1792} \equiv 3 \ (mod\ 18757), \quad 2^{3233} \equiv 5 \ (mod\ 18757).$$

Recall that our ultimate goal is to solve the discrete logarithm problem

$$2^x \equiv 223 \ (mod\ 18757).$$

We compute the value of $223 \cdot 2^{-k} \ (mod\ 18757)$ *for random values of* k *until we find that is B-smooth. After a few attempts we find that*

$$223 \cdot 2^{-12380} \equiv 2^4 \cdot 3^3 \cdot 5^2 \ (mod\ 18757).$$

Using the values of the discrete logs of 2,3 and 5 from above, this yields

$$\begin{aligned} log_g(223) &= 12380 + 4log_g(2) + 3log_g(3) + 2log_g(5) \\ &= 12380 + 4 \cdot 1 + 3 \cdot 1792 + 2 \cdot 3233 \\ &\equiv 5470 \ (mod\ 18756). \end{aligned}$$

Finally, we check our answer $log_g(223) = 5470$ *by computing*

$$2^{5470} \equiv 223 \ (mod\ 18757).$$

2.6 Applications of the RSA cryptosystems

1. **Smart card**

   - The use of RSA keys on smart cards is a significant development because smart cards are time constrained and algorithms can generate the keys quickly.
   - The cost of generating the keys is low. Since the private keys are kept secret by the end user, the cards are more secure and have more memory, [74].

2. **Mobile phone conversation**

   - Mobile devices are very important in the modern world. So the RSA cryptosystem, Diffie-Hellman (DH) key exchange and RC4 ("Rivest Cipher 4" designed by Ron Rivest, 1987) have been used to generate a public cryptographic key from a user's voice so that a speaker's voice can be identified. This generated key is used to encrypt and decrypt the information sent via an open communication channel.
   - The encryption/decryption prevents eavesdroppers listening or interrupting voice calls. Furthermore, it eliminates the need for a trusted third party in a communication (e.g. a telephone company).
   - Generated keys are divided into public keys and private keys. The public key is generated from the speaker's voice and the corresponding private key will be considered as the DH private key. A shared secret will be calculated to generate the input key for the RC4. The RC4 algorithm will generate a key-stream to complete the encryption and decryption process, [32].

3. **Automatic Teller Machines (ATM)**

- An ATM card is one kind of smart card. Conventionally, when a customer attempts to withdraw money from a bank, the bank officer will ask for account holder identification (e.g. a driving license) in order to verify an individual's identity. The ATM machines, however, use cryptography for identification, [76, 50].
- Every ATM card is holds a "secret" Personal Identification Number (PIN), which gives the card holders more secure access to their account. As soon as an ATM card is inserted into the ATM machine, the cardholder is immediately asked for the PIN. If the correct PIN is entered, the machine identifies that person as the rightful owner and grants access, [76].

Chapter 3

Elliptic curve cryptography

Introduction: This chapter will describe the basic theory of elliptic curves, the way elliptic curves work in cryptography (i.e. for encryption and decryption) and the applications of elliptic curves to cryptography in the real world, [1, Chapter 5, p279].

3.1 Elliptic curves

Introduction: The equation of an elliptic curve can be written in the form

$$Y^2 = X^3 + AX + B$$

where A and B are integers with discriminant $\Delta = 16(4A^3 - 27B^2) \neq 0$. This condition ensures the curve does not have a cusp or double point on the real axis. This is also called a Weierstrass equation. It is a special type of elliptic curve but is all that we need here. Two examples of elliptic curves are

$$Y^2 = X^3 - 3X + 3,$$
$$Y^2 = X^3 - 6X + 5.$$

In the figures 3.1 and 3.2, I give plots of the points in $(x, y) \in \mathbb{R}^2$ which satisfy these equations. Note that for the first equation the cubic $X^3 - 3X + 3$ has 1 real root and the second has 3 real roots.

```
In[191]:= E1 = ContourPlot[y^2 - x^3 + 3 * x - 3, {x, -10, 10},
             {y, -10, 10}, ContourShading → False, Contours → {0}, PlotPoints → 200]
```

Out[191]=

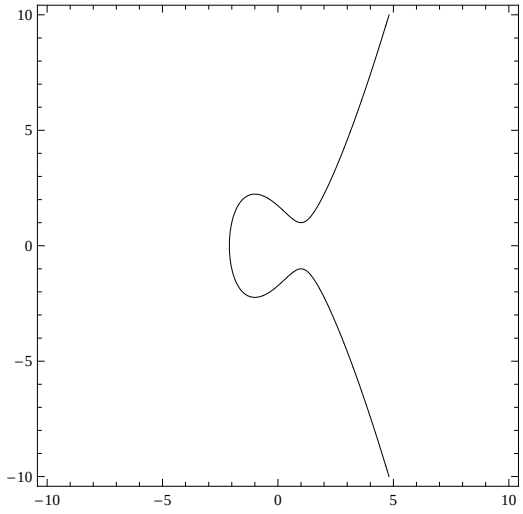

Figure 3.1: $E : Y^2 = X^3 + 3X - 3$ and $\Delta = 16(4(3^3) - 27(-3^2)) > 0$.

```
In[192]:= E2 = ContourPlot[y^2 - x^3 + 6 * x - 5, {x, -10, 10},
             {y, -10, 10}, ContourShading → False, Contours → {0}, PlotPoints → 200]
```

Out[192]=

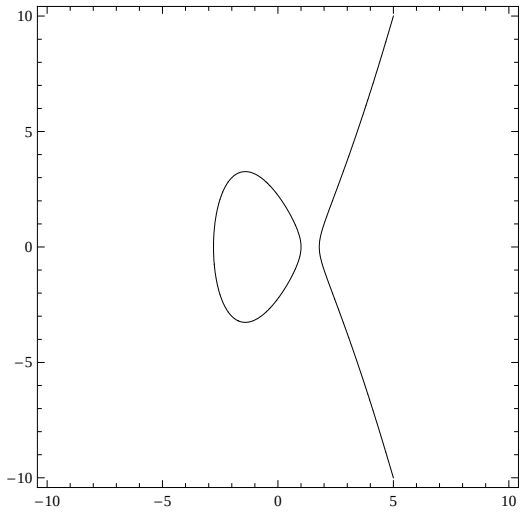

Figure 3.2: $E : Y^2 = X^3 - 6X + 5$ and $\Delta = 16(4(-6^3) - 27(5^2)) < 0$.

The very important property of elliptic curves is that we are able to define an operation + of addition for points which are on the curve, to produce a third point which is also on the curve. This operation makes the curve, and various subsets of points on the curve, into a finitely generated abelian group.

Example 3.1 *Here the operation + is illustrated.*
Let E be the elliptic curve, $Y^2 = X^3 - 7X + 10$. The points $P = (-3, -2)$ and $Q = (1, 2)$ are on the curve E. The line L connecting them is $L : Y = X + 1$. To find the points where E and L intersect: $Y = X + 1$ and $Y^2 = X^3 - 7X + 10$. Then,

$$\begin{aligned} Y^2 = (X+1)^2 &= X^3 - 7X + 10 \\ &= X^2 + 2X + 1 = X^3 - 7X + 10 \\ &= X^3 - X^2 - 7X - 2X + 10 - 1 = 0 \\ &= X^3 - X^2 - 9X + 9 = 0 \end{aligned}$$

So, $X_1 = -3, X_2 = 3, X_3 = 1$. P and Q are in the intersection $E \cap L$, so

$$X^3 - X^2 - 9X + 9 = (X+3)(X-3)(X-1)$$

So, the third point (R) of intersection of L and E is $X = 3$. Thus,

$$Y = X + 1 = 1(3) + 1 = 4.$$

So, $R = (3, 4)$. Finally, we reflect through the X-axis to obtain $P + Q = (3, -4) = R'$. The three points P, Q and R on the elliptic curve E are illustrated in Figure 3.3.

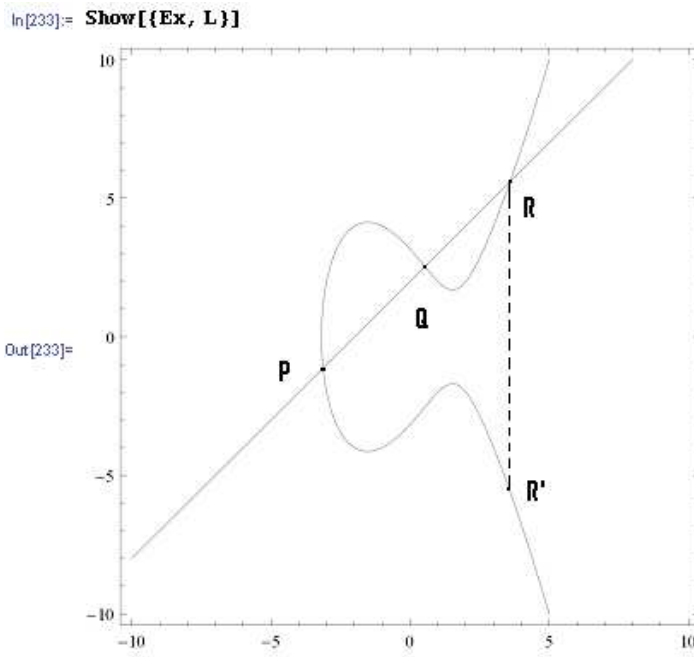

Figure 3.3: $E : Y^2 = X^3 - 7X + 10$ with line $L : Y = X + 1$

3.1.1 Elliptic curve addition

Here is the formal definition.

Definition 3.1 *Let A and B be integers with the discriminant $\Delta = 16(4A^3 - 27B^2)$. An elliptic curve E is the set of solutions to a Weierstrass equation*

$$E : Y^2 = X^3 + AX + B,$$

together with an extra point $\mathcal{O}$, where the constants A and B must satisfy $\Delta \neq 0$.

The extra point $\mathcal{O}$ can be taken as the "point at infinity" in the equivalence class representing the common point at infinity for all lines in $\mathbb{R}^2$ parallel to the Y-axis.

Definition 3.2 *The operation multiplication (i.e. known as scalar*

multiplication) on an elliptic curve defined by kP where k is a positive integer and point $P \in E(\mathbb{Q})$. This operation shows the process of adding P to itself k times.

Definition 3.3 *The point $P' = (x, -y)$ is a reflection of point $P = (x, y)$ on X-axis and elliptic curve.*

Definition 3.4 *The point $P * Q$ denoted as the third point of intersection of the line through an elliptic curve and point P and Q. See the figure below.*

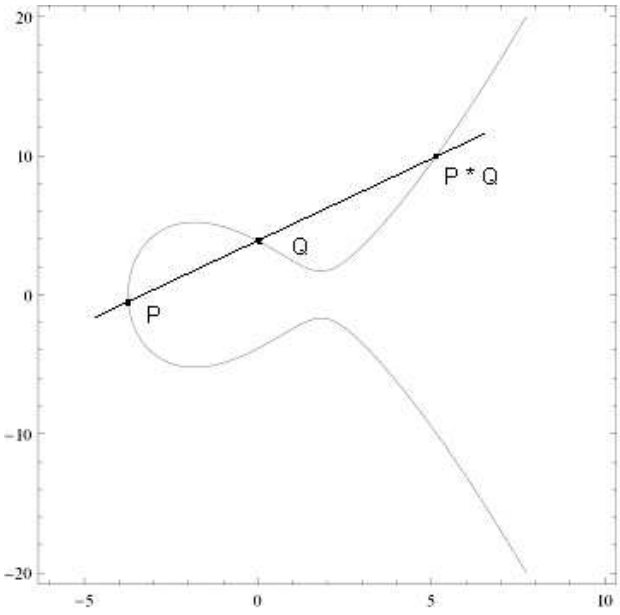

Figure 3.4: The point $P * Q$

Definition 3.5 *The operation addition or '+' on an elliptic curve is defined by geometry and is represented by the addition sign,*

$$+ : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q}).$$

Theorem 3.1 *(Geometric Elliptic Curve Addition Algorithm) [1, Theorem 5.6, p285]*

The operation + on $E(\mathbb{Q})$ make the set of points with rational coordinates on $E \cup \{\mathcal{O}\}$ into an abelian group. Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve and let P and Q be points on E.

(a) If $P = \mathcal{O}$, then $P + Q = Q$.

(b) Otherwise, if $Q = \mathcal{O}$, then $P + Q = P$.

(c) Otherwise, write $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, with $x_1, x_2, x_3, x_4 \in \mathbb{Q}$.

(d) Define λ by

$$\text{If } P \neq Q \text{ and } x_1 \neq x_2 \text{ then } \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \text{ and}$$
$$\text{if } P = Q \text{ then } \lambda = \frac{3x_1^2 + A}{2y_1},$$

and let $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$. Then, $P + Q = (x_3, y_3)$.

(e) If $P \in E$ then $P' \in E$.

(f) If $P = Q'$, then $\mathcal{O} = P + Q$.

(g) $P'' = P$.

Proof. (a) Let $P = \mathcal{O}$, then $Q + \mathcal{O} = Q$. If $Q = (x_2, y_2)$, to obtain $Q + \mathcal{O}$ draw a line through Q parallel to the Y-axis, then the reflection of point Q denoted as $-Q$ implies $Q + (-Q) = \mathcal{O}$.

(b) Similar to (a).

(c) If $P \neq Q$, then $x_1 \neq x_2$ and $y_1 \neq y_2$, where $x_1, x_2, y_1, y_2 \in \mathbb{R}$.

(d) If $x_1 \neq x_2$, then λ is the slope of the line through P and Q.

If $P = Q$, then λ is the slope of the tangent line at $P = Q$.

Either case the line $L : Y = \lambda X + c$ with $c = y_1 - \lambda x_1$, where c is a constant.

Substituting L into E gives:

$$(\lambda X + c)^2 = X^3 + AX + B$$

$$\lambda^2 X^2 + 2\lambda X c + c^2 = X^3 + AX + B$$

$$X^3 - \lambda^2 X^2 + X(A - 2\lambda c) + (B - c^2) = 0$$

So this cubic has roots x_1 and x_2. For the third root x_3, we have the equation $X^3 - \lambda^2 X^2 + X(A - 2\lambda c) + (B - c^2) = (X - x_1)(X - x_2)(X - x_3) =$ $X^3 + X^2(-x_1 - x_2 - x_3) + X(x_1x_2 + x_1x_3) - x_1x_2x_3$.

So, $-\lambda^2 X^2 = X^2(-x_1 - x_2 - x_3)$, implies that $-\lambda^2 = -x_1 - x_2 - x_3$. Then, $x_3 = \lambda^2 - x_1 - x_3$.

Thus, Y coordinate of the third intersection point is $\lambda x_3 + c$ and $P_1 + P_2 = -\lambda x_3 - c$.

(e) Let $P = (x, y)$ on the elliptic curve E. Then, to reflect the point P across the x-axis multiply y-coordinate (i.e. y) by -1. So we obtain a new point $-P = P' = (x, -y)$ which is also on the elliptic curve E as illustrated in Figure 3.5.

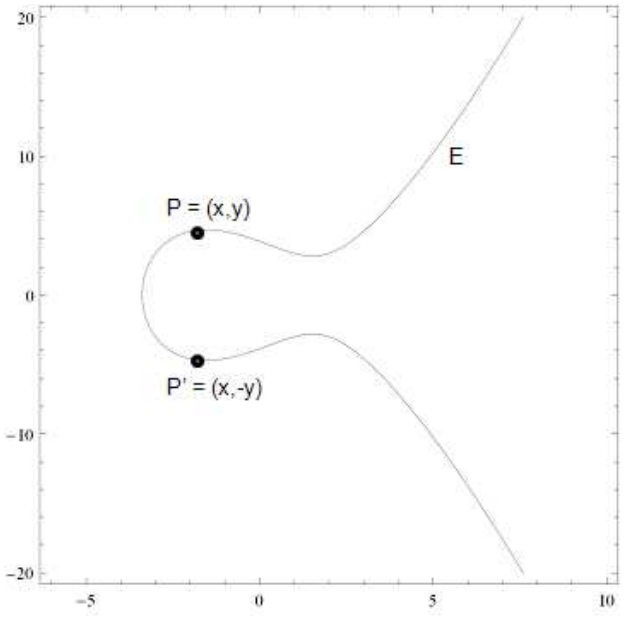

Figure 3.5: The point $P \in E$ implies $P' \in E$.

(f) Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ where $x_1 = x_2$ and $y_1 = -y_2$. Then $Q' = (x_2, -y_2)$ for the curve $y^2 = x^3 + Ax + B$. If $P = Q'$, this means the line through P and Q' is vertical, so the third point of intersection is $\mathcal{O}$ where $x_1 = x_2$ and $y_1 = -y_2$. Thus, $P + Q = Q' + Q = \mathcal{O}$ as illustrated in Figure 3.6.

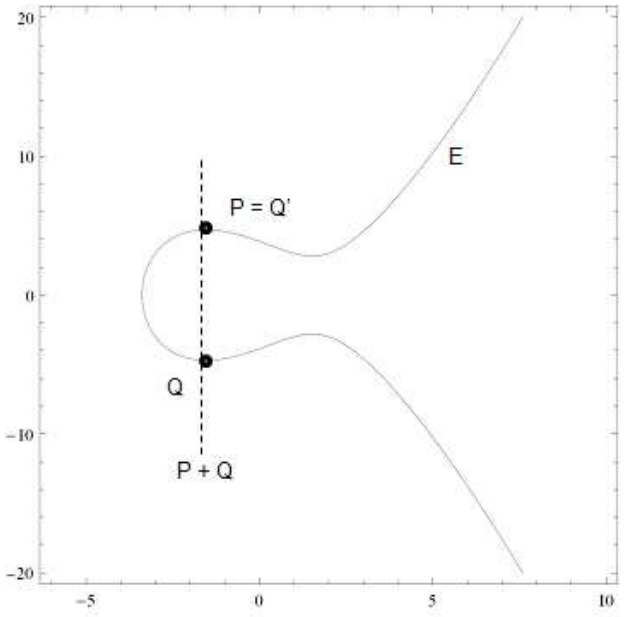

Figure 3.6: When $P = Q'$ implies $P + Q = \mathcal{O}$.

(g) Let $P = (x_1, y_1)$. To get negative of P, we reflect the point P in the x-axis, so $P' = -P = (x_1, -y_1)$. Similarly, the negative of (P') is the reflected point on the x-axis, so

$$P'' = -(-P) = (x_1, -(-y_1)) = (x_1, y_1) = P.$$

□

Theorem 3.2 *(Algebraic Elliptic Curve Addition Algorithm) The following algebraic formulas for the sum of two points and double of a point are derived from the geometric description.*

(a) If $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$*, then* $R' = P + Q = (x_3, y_3)$ *where* $x_1 \neq x_2$*. This implies*

$$x_3 = (\tfrac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \text{ and } y_3 = -(\tfrac{y_2 - y_1}{x_2 - x_1})x_3 - (\tfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}).$$

(b) If $P = Q$*, then* $P + Q = R'$*. This implies*

$$x_3 = (\tfrac{3x_1^2 - A}{2y_1})^2 - x_1 - x_2 \text{ and } y_3 = \tfrac{3x_1^2 - A}{2y_1}(x_1 - x_3) - y_1.$$

Proof. (a) Let $P = (x_1, y_1), Q = (x_2, y_2)$ and $R' = P + Q = (x_3, y_3)$ where $x_1 \neq x_2$ and $y_1 \neq y_2$. Here we want to find the point $R' = (x_3, y_3)$. First, we put the line joining P and Q. The equation for this line L,

$$y = \lambda x + c \text{ where } \lambda = \tfrac{y_2 - y_1}{x_2 - x_1} \text{ and } c = y_1 - \lambda x_1 = y_2 - \lambda x_2 \text{ is constant.}$$

This line is intersect the curve at the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Let the equation $Y^2 = X^3 + A_1X^2 + A_2X + A_3$ be a general (Weierstrass) form. To eliminate the quadratic term, we substitute $Y = y$ and $X = x - \frac{a_1}{3}$.

$$\begin{aligned} y^2 &= (x - \frac{A_1}{3})^3 + A_1(x - \frac{A_1}{3})^2 + A_2(x - \frac{A_1}{3}) + A_3 \\ &= x^3 + A_2x + \frac{2A_1^3}{27} + \frac{A_1A_2}{3} + A_3 - \frac{A_1^3x}{3} \\ &= x^3 + Ax + B. \end{aligned}$$

where $A = A_2 - \frac{A_1^2}{3}$ and $B = \frac{2A_1^3}{27} - \frac{A_1A_2}{3} + A_3$. This is a general equation of an elliptic curve which is also known as cubic equation in x.
To obtain the third point $R' = (x_3, y_3)$, we substitute the line equation into an elliptic curve equation above,

$$y^2 = (\lambda x + c)^2 = x^3 + Ax + B, \text{ where A, B and c are constants.}$$

By putting all in one side yields,

$$\begin{aligned} \lambda^2x^2 - 2\lambda xc + c^2 &= x^3 + Ax + B \\ x^3\lambda^2x^2 + (A - 2\lambda c)x + (B - c^2) &= 0. \end{aligned}$$

Its roots are x_1, x_2 and x_3 which leads us to give the x-coordinates of the three intersections on the elliptic curve. Thus,

$$\begin{aligned} x^3 + (-\lambda^2)x^2 + (A - 2\lambda c)x + (B - c^2) &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - x^2x_3 - x^2x_2 + xx_2x_3 \\ &\quad - x^2x_1 + xx_1x_3 - x_1x_2x_3. \end{aligned}$$

By collecting the coefficients of the x^2, we get

$$-\lambda^2 x^2 = -x^2 x_3 - x^2 x_2 - x^2 x_1$$

$$\lambda^2 = x_1 + x_2 + x_3.$$

So, the point $-R = R' = (x_3, y_3)$ is the reflection of the point R on the x-axis (i.e. by taking the negative of the y-coordinate, see Figure 3.7), we get

$$\begin{aligned}
x_3' &= \lambda^2 - x_1 x_2 \\
x_3 &= (\frac{y_2 - y_1}{x_2 - x_1}) - x_1 - x_2, \text{ and} \\
y_3' &= \lambda x_3 + c \\
y_3 &= -(\frac{y_2 - y_1}{x_2 - x_1}) x_3 - (y_1 - \lambda x_1) \\
y_3 &= -(\frac{y_2 - y_1}{x_2 - x_1}) x_3 - (\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}).
\end{aligned}$$

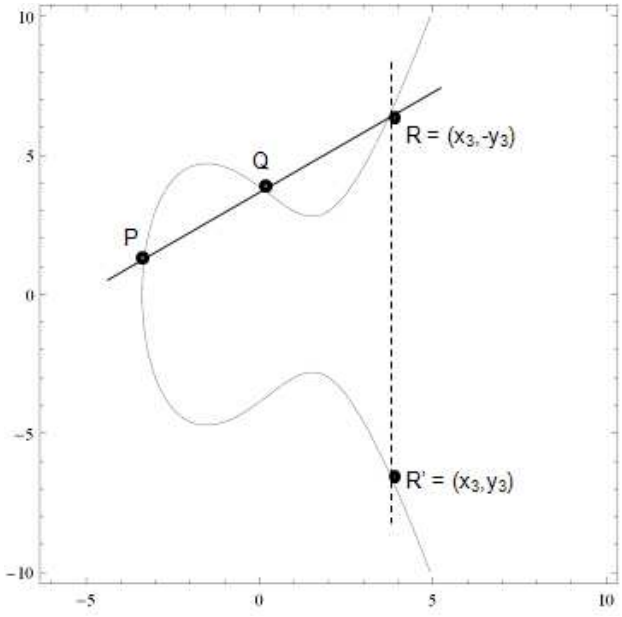

Figure 3.7: The point $R' = P + Q$.

(b) Let the two points be the same,(i.e. $P = Q \Rightarrow (x_1, y_1) = (x_2, y_2)$). Suppose that we have $P \neq -P$. We need to find $P + P = 2P$. By adding these point together, we will get the tangent line at P where this line is joining P to P. First, we need to find the line that joining them. Since $x_1 = x_2$ and $y_1 = y_2$, so we cannot use the same formula for λ like above. Let elliptic curve be $E : y^2 = x^3 + Ax + B$, where A and B are constant. If $P = Q = (x_1, y_1)$ and $P \neq -Q$, then the slope of the tangent line at P is

$$\begin{aligned}\lambda = \frac{dy}{dx} &= \frac{1}{2}(x^3 + Ax + B)^{-1/2}(3x^2 + A) \\ &= 2yy' = 3x^2 + A \\ &= y' = \frac{3x_1^2 + A}{2y_1}, \text{ where } y_1 \neq 0.\end{aligned}$$

Same like proof above (i.e. in part $P + Q = R'$), after we collecting the coefficients of x^2, we get

$$\lambda^2 = x_1 + x_2 + x_3.$$

So, the point $2P = P + P = Q + Q = R' = (x_3, y_3)$ is the reflection of the point R on the x-axis (i.e. by taking the negative of the y-coordinate, see Figure 3.8), we get

$$\begin{aligned}x_3' &= \lambda^2 - x_1 - x_2 \\ x_3 &= (\frac{3x_1^2 + A}{2y_1})^2 - x_1 - x_2, \text{ and} \\ y_3' &= \lambda(x_3 - x_1) + y_1 \\ y_3 &= (\frac{3x_1^2 + A}{2y_1})(x_1 - x_3) - y_1.\end{aligned}$$

□

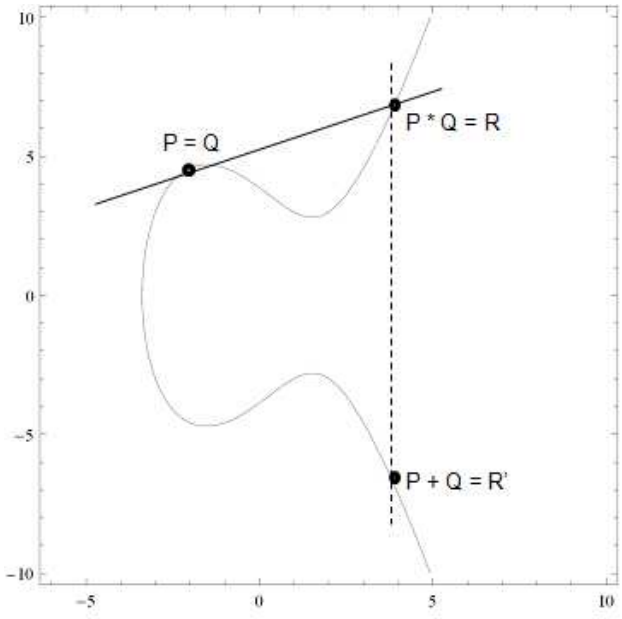

Figure 3.8: The points $P = Q$ implies $P + Q = R'$.

Note: The following properties of the group law of $+$.

1. $+$ takes a point with rational coordinate to a point with rational coordinates,

$$+ : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q}) \tag{3.1}$$

Proof. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be the rational coordinates. We apply three conditions of definition of $+$.

- If $x_1 \neq x_2$, then third point $R = (x_3, y_3) = P + Q$ is a rational coordinate since P and Q are rational coordinates by equation (3.1). Then reflect the point R on the x-axis to give $R' = (x_3, -y_3)$ also with rational coordinates.
- If $x_1 = x_2$ and $y_1 = y_2$, then $P + Q = 2P = 2Q = R$, the third

point, which has rational coordinates. When reflected in x-axis, we also get a point with rational coordinates.

- Similarly, if $x_1 = x_2$ and $y_1 \neq y_2$, then the third point also has rational coordinates.

□

2. Write $2P$ instead of $P + P$.

Proof. When we defined the addition of two points, we can also define a multiplication kP where k is a positive integer and P is a point as the sum of k copies of P. Thus, $2P = P + P$. □

3. For $n \geq 2$, define nP as $P + (n-1)P$.

Proof. For $n \geq 2$. Then for all $n, m \in \mathbb{Z}$, $(n+m)P = nP + mP$. Thus,

$$\begin{aligned} P + (n-1)P &= P + nP - P \\ &= nP. \end{aligned}$$

□

4. Define $-P = P'$, $-2P = -P + (-P)$ etc.

Proof. Similar to (2). □

5. Commutativity, $Q + P = P + Q$.

Proof. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. First, we solve for $Q + P$. The line that joining $Q + P = R$ is

$L : y = \lambda x + c$ where $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ and $c = y_1 - \lambda x_1 = y_2 - \lambda x_2$ is constant.

So the coordinate for the third point $R = (x_3, y_3)$ as illustrated in Figure 3.9 is

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ &= (\frac{y_1 - y_2}{x_1 - x_2})^2 - x_1 - x_2 \\ y_3 &= \lambda x_3 + c \\ &= -(\frac{y_1 - y_2}{x_1 - x_2})x_3 - (y_1 - \lambda x_1) \\ &= -(\frac{y_1 - y_2}{x_1 - x_2})x_3 - (y_1 - (\frac{y_1 - y_2}{x_1 - x_2})x_1) \\ &= -(\frac{y_1 - y_2}{x_1 - x_2})x_3 - (\frac{y_2 x_1 - y_1 x_2}{x_1 - x_2}). \end{aligned}$$

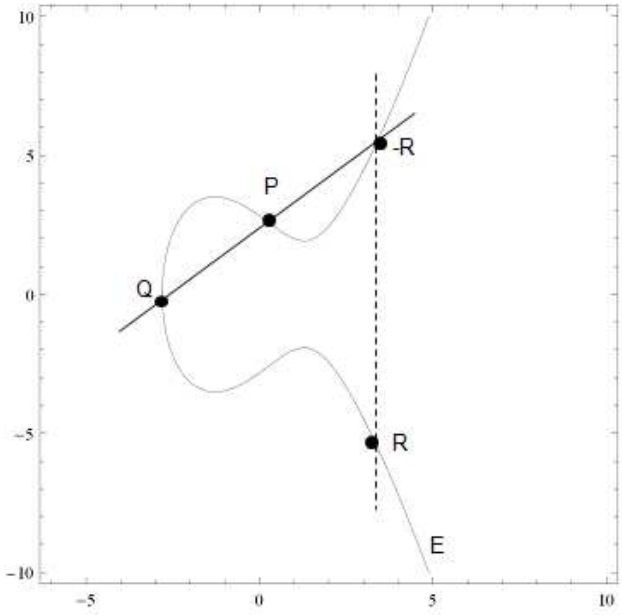

Figure 3.9: $Q + P = R$.

Next, we solve for $P + Q = R$. The equation of the line joining P and Q is

$y = \lambda x + c$ where $\lambda = \frac{y_2 - y_2}{x_2 - x_1}$ and $c = y_1 - \lambda x_1 = y_2 - \lambda x_2$ is constant.

The third point $R = (x_3, y_3)$ as illustrated in Figure 3.10, we reflected on x-axis which is

$$\begin{aligned}
x_3 &= \lambda^2 - x_1 - x_2 \\
&= (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\
y_3 &= \lambda x_3 + c \\
&= -(\frac{y_2 - y_1}{x_2 - x_1})x_3 - (y_1 - \lambda x_1) \\
&= -(\frac{y_2 - y_1}{x_2 - x_1})x_3 - (y_1 - (\frac{y_2 - y_1}{x_2 - x_1})x_1) \\
&= -(\frac{y_2 - y_1}{x_2 - x_1})x_3 - (\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1})
\end{aligned}$$

Thus,

$$\begin{aligned}
Q + P &= ((\frac{y_1 - y_2}{x_1 - x_2})^2 - x_1 - x_2, -(\frac{y_1 - y_2}{x_1 - x_2})x_3 - (\frac{y_2 x_1 - y_1 x_2}{x_1 - x_2})) \\
&= ((\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2, -(\frac{y_2 - y_1}{x_2 - x_1})x_3 - (\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1})) \\
&= P + Q.
\end{aligned}$$

Therefore, commutativity holds.

□

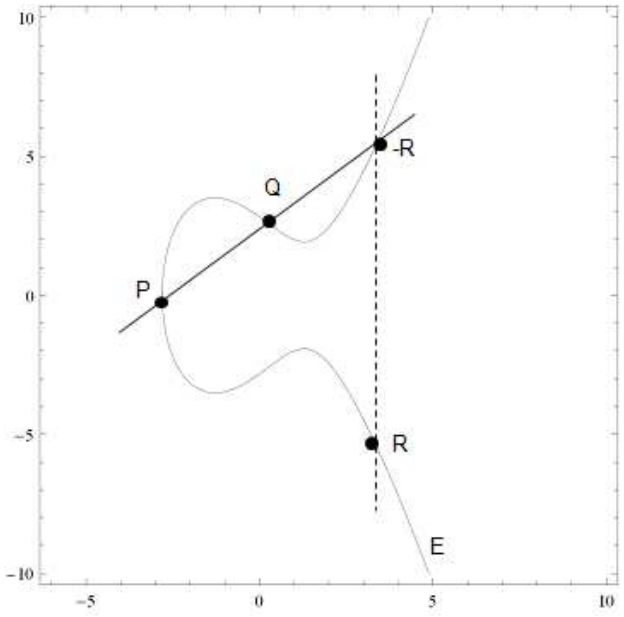

Figure 3.10: $P + Q = R$.

6. Associativity, $(P + Q) + R = P + (Q + R)$.

   Proof. It is enough to show that $(P + Q) * R = P * (Q + R)$ where P, Q and R are finite points on an elliptic curve E.

   (a) To get $P + Q$, we form $P * Q$ and take the third intersection of the line connecting it to $\mathcal{O}$.

   (b) To add $(P + Q)$ to R, we draw a line from R through $(P + Q)$ and that meets the curve at $(P + Q) * R$. To get $(P + Q) + R$, join the line between point $(P + Q) * R$ to $\mathcal{O}$ and take the third intersection.

   (c) Next, to get $P * (Q + R)$, first we need to find $(Q * R)$ and then joining them to $\mathcal{O}$ and take the third intersection on elliptic curve E which is point $Q + R$.

(d) To get the point $P * (Q + R)$, joining the point P to $Q + R$, which leads us to get the same as $(P + Q) * R$.

Thus, the associativity holds. □

We might have $nP = \mathcal{O}$ and $P \neq 0$ for some $n > 1$ which leads us to describe in the next section.

3.1.2 Torsion points

The point P is a torsion point if $nP = \mathcal{O}$ and $P \neq 0$. Each point on an elliptic curve is based of two kinds of order:

1. a point of finite order.

2. a point of infinite order.

If P is a point of finite order, then there exists a smallest integer n such that $nP = \mathcal{O}$. If no such n exists, then P is a point of infinite order (i.e. we can never find the point at infinity by adding P to itself).

Definition 3.6 *A point $P \in E(\mathbb{Q})$ is called a torsion point of order n if P has order n.*

$$E(\mathbb{Q})_{tors} = \{P \in E(\mathbb{Q}) |\ \textit{there exist } n \in \mathbb{N} \textit{ such that } nP = \mathcal{O}\} \subseteq E(\mathbb{Q}).$$

$E(\mathbb{Q})_{tors}$ is the set of all torsion points.

If A and B are large in the elliptic curve equation (i.e. $E : y^2 = x^3 + Ax + B$), then there could be many such points. However, Mazur showed that the size and structure of such a torsion subgroup is very limited. Mazur's theorem, created by Barry Charles Mazur in 1976, [84] describes what torsion subgroups that are possible for an elliptic curve over $\mathbb{Q}$.

Theorem 3.3 *(Mazur's Theorem)[80, Theorem 4.1, p11]*
Let $E(\mathbb{Q})$ be an elliptic curve. Then the torsion subgroup must be one of the following 15 groups:
(i) $\mathbb{Z}/n\mathbb{Z}$, for $n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$,
(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, for $n \in \{2, 4, 6, 8\}$.

Theorem 3.3 tells us that there are no rational torsion points of order greater than 12, (i.e. all other points are of infinite order).
The following theorem was proved by E. Lutz and T. Nagell in 1930s, [85]. It gives an efficient method to compute the torsion subgroup of an elliptic curve E over $\mathbb{Q}$, (i.e. $E(\mathbb{Q})_{tors}$).

Theorem 3.4 *(Nagell-Lutz Theorem) [80, Theorem 5.1, p12]*
Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation

$$E : y^2 = x^3 + Ax + B \text{ where } A, B \in \mathbb{Z}.$$

Then, the coordinates of a non-zero torsion point $P = (x, y) \in E(\mathbb{Q})$ are in $\mathbb{Z}$. Furthermore, a torsion point P is either of order 2 (i.e. if $y = 0$) or else $y^2|D$ where $D = 4A^3 + 27B^2$.

Example 3.2 *Let an elliptic curve $E : y^2 = x^3 + 4$ and suppose that a point $P = (x, y) \in E(\mathbb{Q})$ has finite order. By the Nagell-Lutz theorem, we know that either $y = 0$ or $y^2|4A^3 + 27B^2 = 2^4 \cdot 3^3 = 432$. Thus, the possibilities for y occur in the following list:*

$$0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12.$$

Consider the following values of y in the rightmost column below:

$$0 \Rightarrow 0 = x^3 + 4 \Rightarrow -4 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow \text{ no points with } y = 0,$$

$$\pm 1 \Rightarrow 1 = x^3 + 4 \Rightarrow -3 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow \text{ no points with } y = \pm 1,$$

$$\pm 2 \Rightarrow 4 = x^3 + 4 \Rightarrow 0 = x^3 \Rightarrow x = 0 \in \mathbb{Z} \Rightarrow (0, 2) \text{ and } (0, -2) \in E,$$

$$\pm 3 \Rightarrow 9 = x^3 + 4 \Rightarrow 5 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow \text{ no points with } y = \pm 3,$$

$$\pm 4 \Rightarrow 16 = x^3 + 4 \Rightarrow 12 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow \text{ no points with } y = \pm 4,$$

$$\pm 6 \Rightarrow 36 = x^3 + 4 \Rightarrow 32 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow \text{ no points with } y = \pm 6,$$

$$\pm 12 \Rightarrow 144 = x^3 + 4 \Rightarrow 140 = x^3 \Rightarrow x \notin \mathbb{Z} \Rightarrow \text{ no points with } y = \pm 12.$$

Trial and error shows that only $y = \pm 2$ gives x to be an integer. Hence the only possible points here that need to be checked are $(0, \pm 2)$. Since $(0, -2) = -(0, 2)$, it is suffices to check only one of the P, P' points, say, $P = (0, 2)$. By the addition algorithm, it can be checked that

$$2P = P + P = (0, 2) + (0, 2) = (0, -2) = -P,$$

hence $3P = 2P + P = -P + P = \mathcal{O}$.

Thus, P and $-P$ have order 3. Therefore the torsion subgroup of $E(\mathbb{Q})$ is

$$\{\mathcal{O}, (0, 2), (0, -2)\},$$

which is isomorphic to the additive group $\mathbb{Z}/3\mathbb{Z}$.

3.2 Elliptic curves over finite fields

Introduction: Elliptic curve cryptography (ECC) is a form of public-key cryptography where the coordinates are in a finite field, $\mathbb{F}_p$. ECC was developed by Neal Koblitz and Victor Miller in 1985, [39]. It is based on the difficulty of solving the *Elliptic Curve Discrete Logarithm Problem.* The elliptic curve equation is defined by,

$$E : Y^2 = X^3 + AX + B \text{ with } A, B \in \mathbb{F}_p,\ 4A^3 + 27B^2 \neq 0,\ p \neq 2, 3.$$

In practice we use the geometric definition of + to derive formulas for the coordinates of $P + Q$ in the form of rational functions with integer coefficients. These formulas make sense in any suitable field, even a finite field (provided the characteristic $p \neq 2, 3$), and we use them to define + over such a field.

Definition 3.7 *Define the equation of an elliptic curve over finite field $\mathbb{F}_p$ as $E : Y^2 = X^3 + AX + B$ where $A, B \in \mathbb{F}_p$ and satisfying $\Delta = 16(4A^3 - 27B^2) \neq 0$, and the group operation + is defined by the algebraic rules of Theorem 3.2. Therefore the set $E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p$ where (x, y) satisfy $Y^2 = X^3 + AX + B\} \cup \mathcal{O}$ is an abelian group.*

Example 3.3 *Elliptic curve, $E : Y^2 = X^3 + 4X + 9$ over $\mathbb{F}_{13}$, to add points $P = (10, 8)$ and $Q = (2, 9)$ in $E(\mathbb{F}_{13})$, I first compute*

$$\lambda = \tfrac{y_2 - y_1}{x_2 - x_1} = \tfrac{9-8}{2-10} \equiv 8 \ (mod\ 13).$$

Next compute

$$\nu = y_1 - \lambda x_1 = 8 - 8(10) \equiv 6 \ (mod\ 13).$$

Finally, the addition algorithm tells us to compute

$$x_3 = \lambda^2 - x_1 - x_2 = 64 - 10 - 2 \equiv 0 \ (mod\ 13),$$
$$y_3 = -(\lambda x_3 + \nu) = -(0 + 6) \equiv 2 \ (mod\ 13)$$

This completes the computation of

$$P + Q = (10, 8) + (2, 9) = (0, 2) \in E(\mathbb{F}_{13}).$$

Example 3.4 *Let E be the elliptic curve, $E : y^2 = x^3 + x + 1$. Compute the number of points in the group $E(\mathbb{F}_p)$ when $p = 5$ and $p = 7$.*

To find the points of $\mathbb{F}_5$*, we need to substitute all possible values* $x = 0, 1, 2, 3, 4$*, and checking for which* x *value the quantity is* $x^3 + x + 1 = a \equiv b^2 \ (mod\ 5)$.

$$x = 0 \Rightarrow 0 + 0 + 1 = 1 \equiv 1 \ (mod\ 5) = 1^2, 4^2.$$

$$x = 1 \Rightarrow 1^3 + 1 + 1 = 3 \equiv 3 \ (mod\ 5).$$

$$x = 2 \Rightarrow 2^3 + 2 + 1 = 11 \equiv 1 \ (mod\ 5) = 1^2, 4^2.$$

$$x = 3 \Rightarrow 3^3 + 3 + 1 = 31 \equiv 1 \ (mod\ 5) = 1^2, 4^2.$$

$$x = 4 \Rightarrow 4^3 + 4 + 1 = 69 \equiv 4 \ (mod\ 5).$$

Thus, $E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4)\}$ *so has* 7 *elements. For* $E(\mathbb{F}_7)$*, the values of* x *are* $0, 1, 2, 3, 4, 5, 6$.

$$x = 0 \Rightarrow 0 + 0 + 1 = 1 \equiv 1 \ (mod\ 7) = 1^2, 6^2.$$

$$x = 1 \Rightarrow 1^3 + 1 + 1 = 3 \equiv 3 \ (mod\ 7).$$

$$x = 2 \Rightarrow 2^3 + 2 + 1 = 11 \equiv 4 \ (mod\ 7) = 1^2, 5^2.$$

$$x = 3 \Rightarrow 3^3 + 3 + 1 = 31 \equiv 3 \ (mod\ 7).$$

$$x = 4 \Rightarrow 4^3 + 4 + 1 = 69 \equiv 6 \ (mod\ 7).$$

$$x = 5 \Rightarrow 5^3 + 5 + 1 = 131 \equiv 5 \ (mod\ 7).$$

$$x = 6 \Rightarrow 6^3 + 6 + 1 = 223 \equiv 6 \ (mod\ 7).$$

Thus, $E(\mathbb{F}_7) = \{\mathcal{O}, (0,1), (0,6), (2,1), (2,5)\}$ *so has* 5 *elements.*

3.3 The elliptic curve discrete logarithm problem (ECDLP)

Introduction: The ECDLP is a variation of the discrete logarithm problem. The ECDLP is defined over the points of an elliptic curve. The security of

elliptic curve cryptography depends on ECDLP, which is the discrete logarithm problem applied to elliptic curves, [8].

Definition 3.8 *Let E be an elliptic curve over the finite field $\mathbb{F}_p$ and let P and Q be points in $E(\mathbb{F}_p)$. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem of finding an integer n such that $Q = nP$. By analogy with the discrete logarithm problem for $\mathbb{F}_p^*$, we denoted this integer n by*

$$n = log_P(Q)$$

and we call n the elliptic discrete logarithm of Q with respect to P.

Example 3.5 *Let E be the elliptic curve, $E : y^2 = x^3 + x + 1$ and let $P = (4, 2)$ and $Q = (0, 1)$ be points on E modulo 5. I solve the elliptic curve discrete logarithm problem for P and Q, by finding a positive integer n such that $Q = nP$.*

Solution:

First, we need to find $2P = P + P$:

$$\lambda = \frac{3(x(P))^2+A}{2y(P)} = \frac{49}{4} = 1,$$

where $x(P)$ and $y(P)$ are values of x and y respectively of the point P. By using the addition algorithm (refer to Theorem 3.1),

$$x(2P) = \lambda^2 - 2x(P) = 1^2 - 2(4) = 3.$$
$$y(2P) = \lambda(x(P) - x(2P)) - y(P) = 1(4 - 3) - 2 = 4$$

Thus, $2P = (3, 4)$.

Next, find $3P = 2P + P$.

$$\lambda = \frac{y(2P)-y(P)}{x(2P)-x(P)} = \frac{4-2}{3-4} = 3.$$

In a similar manner, we apply the addition algorithm to get the next coordinate:

$$x(3P) = \lambda^2 - x(2P) - x(P) = 3^2 - 3 - 4 = 2.$$
$$y(4P) = \lambda(x(P) - x(3P)) - y(P) = 3(4 - 2) - 2 = 4.$$

Thus, $3P = (2, 4)$.

By using the same steps as above, we continue to calculate coordinates until we find the integer n.

$$4P = (0, 4)$$
$$5P = (0, 1) = Q.$$

Therefore, the integer n *is* 5.

3.4 Application of elliptic curves to cryptography

Introduction: This explains how elliptic curves are applied to cryptography. We consider two applications, the Diffie-Hellman key exchange and the El-Gamal public key cryptosystem.

3.4.1 Elliptic Diffie-Hellman key exchange

(a) Public parameter creation

Alice and Bob choose and publish a large prime p, an elliptic curve E over $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$.

(b) Private computations

Alice: chooses a secret integer n_A. Then, computes the point on the curve $Q_A = n_A P$.

Bob : chooses a secret integer n_B. Then, computes the point on the curve $Q_B = n_B P$.

(c) Public exchange of values

Then, they exchange the values of Q_A and Q_B. In other words, Alice sends Q_A to Bob and Bob sends Q_B to Alice.

(d) Further private computations

Alice then uses her secret multiplier to compute the point n_AQ_B. While Bob computes the corresponding, n_BQ_A. So now, they are able to share the secret value which is

$$n_AQ_B = (n_An_B)P = n_BQ_A.$$

They can then use this value as a key to communicate privately.

Example 3.6 *Alice and Bob decide to use elliptic Diffie-Hellman key exchange with the following prime, curve and point.*

$$p = 3889,\ E : Y^2 = X^3 + 354X + 1234,\ P = (921, 304) \in E(\mathbb{F}_{3889}).$$

Alice and Bob choose respective secret values $n_A = 123$ *and* $n_B = 456$ *and then*

$$\begin{aligned}
\textit{Alice computes } Q_A = 123P &= 2^6P + 2^5P + 2^4P + 2^3P + 2P + P \in E(\mathbb{F}_{3889}) \\
&= 64P + 32P + 16P + 8P + 2P + P \in E(\mathbb{F}_{3889}) \\
&= (1717, 3600) + (219, 3579) + (361, 1165) + (2043, 2691) \\
&\quad + (2270, 3888) + (921, 304) \in E(\mathbb{F}_{3889}) \\
&= (721, 2157) \in E(\mathbb{F}_{3889}). \\
\textit{Bob computes } Q_B = 456P &= 2^8P + 2^7P + 2^6P + 2^3P \in E(\mathbb{F}_{3889}) \\
&= 256P + 128P + 64P + 8P \in E(\mathbb{F}_{3889}) \\
&= (1229, 2109) + (2132, 837) + (1717, 3600) \\
&\quad + (2043, 2691) \in E(\mathbb{F}_{3889}) \\
&= (1383, 936) \in E(\mathbb{F}_{3889}).
\end{aligned}$$

Bob and Alice have exchanged the secret point

$n_AQ_B = 123(1383, 936) = 456(721, 2157) = n_BQ_A = (3160, 722).$

3.4.2 Elliptic El-Gamal public key cryptosystem

The direct analogue of the classical El-Gamal public key cryptosystem.

(a) Public parameter creation

A trusted people choose and publish a large prime p, an elliptic curve over $\mathbb{F}_p$ and a point P in $E(\mathbb{F}_p)$.

(b) Key creation

Alice chooses a private key n_A and publishes the point $Q_A = n_A P$ as a public key.

(c) Encryption

Bob chooses plaintext encoded as $M \in E(\mathbb{F}_p)$ and chooses an integer k as a temporary key. By using Alice's public key Q_A, Bob computes

$$c_1 = kP \in E(\mathbb{F}_p) \text{ and } c_2 = M + kQ_A \in E(\mathbb{F}_p).$$

Then he sends the two points (c_1, c_2) to Alice.

(d) Decryption

Alice computes

$$\begin{aligned} c_2 - n_A c_1 &= (M + kQ_A) - n_A(kP) \\ &= M + k(n_A P) - n_A(kP) \\ &= M \in E(\mathbb{F}_p), \text{which is the plaintext.} \end{aligned}$$

3.5 Applications of elliptic curve cryptography

Introduction: Elliptic curve cryptography is becoming more popular because of the small number of bits required to generate keys compared to other cryptosystems. Thus, it has been used frequently. Here are some examples of elliptic curve cryptography where it has been applied.

1. **Wireless security / communication**

   - Wireless devices have become prevalent for communication. Basically, these devices need less memory and low computational power but require a high level of security, [77, 6].

   - When wireless messages are sent or shared, we need to be sure that our communications are secure and the message remains secret. So, elliptic curve cryptography is one way to solve security problems. Since the key size of elliptic curve cryptography is relatively small, the encrypted/decrypted message and computational power are small, [78, 79].

   - Applying elliptic curve cryptography to wireless communication is very efficient for large data files and encrypted files. Also, elliptic curve cryptography involves low data rate transmissions and low power requirements, [7].

2. **Smart cards**

   - Smart cards such as those used for telephone calling, electronic cash payments, health care, identification and other applications is a plastic card with a built in microchip that can be loaded with data/information. The advantage of a smart card is it can store sensitive data that can be protected from unauthorized access.

   - Elliptic curve cryptography is compatible for smart card because, [5, p10].

     (a) it requires less memory and shorter transmission times

- Since the elliptic curve discrete logarithm problem algorithm uses small keys, it requires a small amount of memory to store those keys and to transfer data.

(b) Scalability for system resources

- A smart card would need a strong security and large storage to keep long keys, but in contrast by using elliptic curve cryptography which has small keys, this problem can be solved resulting in low-cost of production and a higher level of security.

(c) No coprocessor required

- When using elliptic curve cryptography for a smart card, there is no additional hardware required in the CPU (central processing unit) because elliptic curve cryptography reduces processing times.

(d) On card key generation

- The private key on a smart card must be kept secret from unauthorized users to ensure security. Basically, a key is embedded into a card to be ensure it is personalized and authenticated.
- Provided a good random number generator is available with elliptic curve cryptography, the time required to generate the private key is short and generation only requires low computing power that is typically available on of a smart card. This means that the card personalization process can be more efficient for applications in which nonrepudiation is important.

3. **Network security/securing the web**

   - Since the keys of elliptic curve cryptography are small, the effect of its application is faster computations, lower power consumption and memory and bandwidth savings, [10].

Chapter 4

Encryption and decryption using the RSA cryptosystem and elliptic curve cryptography

Introduction: In cryptography, there are many ways to send or receive messages. In this chapter we give some examples using RSA cryptosystems and elliptic curve cryptography to encrypt and decrypt messages.

4.1 The RSA cryptosystem

Question 1:

Alice publishes her RSA public key: modulus $N = 1351500281$ and exponent $e = 5441$.

(a) Bob wants to send Alice the message $m = 234698$. What ciphertext does Bob send to Alice?

Solution:

The public key is $(N, e) = (1351500281, 5441)$. By the way,

$p \cdot q = N = 1351500281$. We know that the ciphertext, $c \equiv m^e \pmod{N}$. So,

by using software we get $c \equiv 234698^{5441} \equiv 107925960 \pmod{1351500281}$.

Thus, the ciphertext is 107925960.

(b) Alice knows that her modulus factors into a product of two primes, one of which is $p = 124459$. Find the decryption exponent d for Alice.

Solution:

We have $p \cdot q = N = 1351500281$. Then $124459 \cdot q = 1351500281$. So $q = 10859$.

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}.$$
$$(p-1) \cdot (q-1) = (124458)(10858) = 1351364964.$$
$$5441 \cdot d \equiv 1 \pmod{1351364964}.$$

By using extended Euclidean algorithm of software, we have $d = 23098133$.

(c) Alice receives the ciphertext $c = 107925960$ from Bob and decrypt the message.

Solution:

$$c^d \pmod{N} \equiv 107925960^{23098133} \pmod{1351500281}.$$
$$\equiv 234698 \pmod{1351500281}.$$

So, the message is 234698.

Question 2:

Bob's RSA public key has modulus $N = 555722767441851267329933783$ and exponent $e = 738083$. Alice sends Bob the ciphertext $c = 127053668429207502906717463$. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message.

Solution:

Given that $N = 555722767441851267329933783 = p \cdot q$. Then, we can factorize N:

$555722767441851267329933783 = 23579273408279 \cdot 23568273619777$.

We must check that

$gcd(e,(p-1)(q-1)) = gcd(738083, 555722767441804119782905728) = 1$. So,

$c \equiv 1270536684292075029067174 63 \pmod{555722767441851267329933783}$.

Bob knows $(p-1)\cdot(q-1) = 23579273408278 \cdot 23568273619776 =$

555722767441804119782905728.

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$$

$$738083 \cdot d \equiv 1 \pmod{555722767441804119782905728}.$$

So, $d = 1746640521339059695281404 27$.

Then,

$$c^d \pmod N \equiv 1270536684292075029067174 63^{1746640521339059695281404 27} \pmod N$$

$$\equiv 234580277294629 \pmod{555722767441851267329933783}.$$

So, the message is $m = 234580277294629$.

Question 3:

(a) Use Alice's RSA public encryption key

$(N,e) = (931193664662420801428126247840126135129, 6283649)$ to encrypt the word 'SEE YOU LATER'.

(First change the letters to numbers using

$space = 00, a = 01, b = 02, c = 03, ...$).

Solution:

By using software, we factorize N to get $p = 23459512369369265081$ and $q = 39693649637759157409$ where $N = p \cdot q$. Then choose $e = 6283649$.

$\phi(n) = (p-1)\cdot(q-1) = 23459512369369265080 \cdot 39693649637759157408 =$

931193664662420801364973085832997712640. The encryption key is

$(N,e) = (931193664662420801428126247840126135129, 6283649)$. We need to change the word 'SEE YOU LATER' to numbers: SEE YOU LATER =

190505002515210012012005 18. To encrypt the message, we must use the

encryption key (N, e).

$$\begin{aligned} c &\equiv m^e \pmod N \\ &\equiv 190505002515210012012005 18^{6283649} \pmod N \\ &\equiv 526488788787428752841541917320444425 09 \\ &\pmod{931193664662420801428126247840126135129}. \end{aligned}$$

So, the encoded message is 'YJGXFFOFYCONJSTQQYI'.

(b) Bob encrypted a word with Alice's encryption key $(N, e) = (931193664662420801428126247840126135129, 6283649)$. He obtains the number 526488788787428752841541917320444425 09. Use Alice's decryption key $d = 501469130233221884785435566252401557889$ to decrypt this number and get back Bob's message.

Solution:

$$\begin{aligned} m &\equiv c^d \pmod N \\ &\equiv 526488788787428752841541917320444425 09^{501469130233221884785435566252401557889} \pmod N \\ &\equiv 190505002515210012012005 18 \pmod{931193664662420801428126247840126135129}. \end{aligned}$$

So the message is 'SEE YOU LATER'.

4.2 Elliptic curve cryptography

Question 1:

Alice and Bob agree to use elliptic Diffie-Hellman key exchange with the prime, elliptic curve and point $p = 2671$, $E : Y^2 = X^3 + 171X + 853$, $P = (1980, 431) \in E(\mathbb{F}_{2671})$.

(a) Alice sends Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 1943$. What point should Bob send to Alice?

Solution:

To answer this question, we used Mathematica software to make the job easier.

$1943 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^4 + 2^2 + 2^1 + 2^0$. Then, Bob needs to compute Q_B to send to Alice.

$Q_B = n_B P = 1943(1980, 431)$.

$P = (1980, 431)$, $9P = (1124, 363)$

$2P = (1950, 1697)$, $10P = (2431, 1318)$

$3P = (415, 301)$, $11P = (1858, 644)$

$4P = (1894, 1829)$, $12P = (1490, 1078)$

$5P = (45, 166)$, $13P = (143, 27)$

$6P = (536, 312)$, $14P = (289, 578)$

$7P = (2288, 2333)$, $15P = (763, 9)$

$8P = (1160, 1268)$, $16P = (1116, 2037)$

$1943P = 2^{10}P + 2^9P + 2^8P + 2^7P + 2^4P + 2^2P + 2^1P + 2^0P$

$1943P = (175, 1556) + (970, 2139) + (2142, 864) + (2006, 430) + (1116, 2037) + (1894, 1829) + (1950, 1697) + (1980, 431)$. So, Bob sends point Q_B to Alice, $Q_B = 1943P = (2580, 1400)$.

(b) What is their secret shared value?

Solution:

Alice sends to Bob, $Q_A = (2110, 543)$. Bob sends to Alice, $Q_B = (2580, 1400)$. So, Bob computes $n_B Q_A = 1943(2110, 543)$.

Use the same method as above to get their shared value $n_B Q_A = (656, 1205)$.

Question 2:

The cryptosystem parameter are $E_{11}(1, 6)$ and $G = (2, 7)$. Bob's secret key in $n_B = 7$.

(a) Find Bob's public key P_B.

Solution:

We know that $P_B = n_B G = 7(2, 7)$. By using software, we get

$$G = (2, 7)$$

$$2G = (5, 2)$$

$$3G = (8, 3)$$

$$4G = (10, 2)$$

$$5G = (3, 6)$$

$$6G = (7, 9)$$

$$7G = (7, 2)$$

So, the value of P_B is $(7, 2)$.

(b) Alice wishes to encrypt the message $P_m = (10, 9)$ and chooses the random value $k = 3$. Determine the ciphertext C_m.

Solution:

Bob's public key is $P_B = (7, 2)$. We have,

$$3(2, 7) = (8, 3), \text{ and}$$

$$(10, 9) + 3(7, 2) = (10, 9) + (3, 5).$$

To find addition point $(10, 9) + (3, 5)$, $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-10}{3-9} = 10$.

$\nu = y_1 - \lambda x_1 = 9 - 10(10) = 3$.

$x_3 = \lambda^2 - x_1 - x_2 = 10^2 - 10 - 3 = 10$.

$y_3 = -(\lambda x_3 + \nu) = -(10(10) + 3) = 7$.

So, (10,9) + 3(7,2) = (10,7). Thus, Alice sends the ciphertext $(8, 3), (10, 7)$.

Question 3:

Let E be the elliptic curve $E : Y^2 = X^3 + 1541x + 1335$ and let $P = (2898, 439)$. The prime $p = 3221$ and $n = 3211$. By using the elliptic curve addition algorithm, compute nP in $E(\mathbb{F}_p)$.

Solution:

The binary expansion of n is

$$n = 3211 = 2^{11} + 2^{10} + 2^7 + 2^3 + 2^1 + 2^0.$$

Then we can compute

$$\begin{aligned} 3211P &= 2^{11}P + 2^{10}P + 2^7P + 2^3P + 2P + P \\ &= 2048P + 1024P + 128P + 8P + 2P + P. \end{aligned}$$

First we need to find all the values that are related to get $3211P$.

$$P = (2898, 439)$$

$$2P = (1951, 1370)$$

$$3P = (2438, 608)$$

$$8P = (2937, 310)$$

$$128P = (2475, 2561)$$

$$1024P = (1596, 2944)$$

$$2048P = (1566, 2267)$$

Then, we combine all together yields

$$\begin{aligned} 3211P = &= 2048P + 1024P + 128P + 8P + 2P + P \\ &= (1566, 2267) + (1596, 2944) + (2475, 2561) + (2937, 310) \\ &\quad + (1951, 1370) + (2898, 439) \\ &= (1388, 1990). \end{aligned}$$

Thus, $nP = 3211P = (1388, 1990)$.

Chapter 5

Conclusions

In this thesis, I studied the mathematics of the two public-key cryptosystems, the RSA cryptosystem and elliptic curve cryptography. These are the most well-known cryptosystems used currently throughout the world. The RSA cryptosystem is based on elementary number theory. However, RSA can be broken, in two cases; either a brilliant mathematician knows how to factor large integers very quickly or this factoring can be performed by high speed computers. Therefore, mathematicians and scientists have designed new approaches to message encryption like elliptic curve cryptography.

Elliptic curve cryptography is another cryptosystem that is very efficient and is frequently used nowadays. I explained how elliptic curves can be used to create public key systems for encryption and decryption. Since there is an infinite set of elliptic curves, it makes it difficult for an adversary or eavesdropper to decrypt a communication. In addition, elliptic curve cryptosystems are efficient because they use smaller key sizes, have low computational power requirements and give better performance than RSA cryptosystem.

References

[1] Jeffrey H., Jill P., Joseph H.S *An Introduction to Mathematical Cryptography*, Springer, 2008.

[2] Lawrence C.Washington, *Elliptic curves: Number Theory and Cryptography*, Chapman & Hall / CRC, 2003.

[3] Lecture Notes: INFO412 - Mathematical and Cryptography, School of Mathematics & Applied Statistics, University of Wollongong, Australia.

[4] Abdullatif Shikfa *Bilinear pairings on elliptic curves*, Research Master Thesis, Ecole doctorale STIC de Nice Sophia-Antipolis, June 2005.

[5] Ahmed Khaled M. Al-Kayali *Elliptic curve cryptography and Smart card*, SANS Institute InfoSec Reading Room, SANS Institute, 17 February 2004.

[6] Kristin Lauter *The advantages of elliptic curve cryptography for wireless security*, Microsoft Corporation, February 2004.

[7] G.V.S Raju (Department of Electrical Engineering) & Rehan Akbani (Department of Computer Science) *Elliptic curve cryptosystem and its application*, University of Texas, San Antonio, TX 78249-0669, Proceedings of the IEEE International Conference on Systems, Man & Cybernetics (IEEE-SMC), 2003.

[8] Amol Dabholkal & Kin Choong Yow *Efficient implementation of elliptic curve cryptography and personal digital assistance (PDAs)*, School of Computer Engineering, Nanyang Technological University, Singapore, 2004.

[9] Mathieu Ciet & Marc Joye *(Virtually) Free randomization techniques for elliptic curve cryptography*, Springer-Verlag Berlin Heidelberg, 2003.

[10] Kiyomichi Araki, Takakazu Satoh & Shinji Miura *Overview of elliptic curve cryptography*

[11] Tom Davis *RSA Encryption*, October 10, 2003.

[12] Lejla Batina, Geeke Bruin-Muurling & Siddika Berna Ors *Flexible hardware design for RSA and elliptic curve cryptosystems*, T.Okamoto(Ed):CT-RSA 2004, LNCS 2964, pp. 250-263, Springer-Verlag Berlin Heidelberg, 2004.

[13] Xin Guo *RSA Cryptosystem*, Dept of IEOR, UC Berkeley, CA, Course: CS6520, 8 Dec 2004.

[14] Weihu Hong *RSA cryptosystem & its applications*, Department of Mathematics, Clayton College & State University, Oct 28-31, 2004.

[15] Anoop MS *Elliptic curve cryptography (An implementation guide)*, January 5, 2007.

[16] R. Sedgewick *Lecture 22: Cryptology*, COS126: General Computer Science, Department of Computer Science, Princeton University, http://www.cs.princeton.edu/courses/archive/spr05/cos126/lectures/22.pdf

[17] Thomas Baignères, Pascal Junad, Yi Lu & Serge Vaudenay *A classical introduction to cryptography exercise book*, Springer Science + Business Media, Incorporation, 2006.

[18] Beissinger, Janet, Pless & Vera *Cryptoclub: Using mathematics to make and break secret codes, workbook*, AK Peters Limited, 2006.

[19] Ryabko, Boris, Fionov & Andrey *Basics of contemporary cryptography for IT practitioners*, World Scientific Publishing Company, Incorporated, 2005.

[20] Moldovyan, Alex & Nick *Innovative cryptology (2nd Edition)*, Course technology, 2006.

[21] Henk C. A van Tilborg *Fundamentals of cryptology: A professional reference and interactive tutorial*, Kluwer Academic Publishers, 2000.

[22] Silvia Robles *The RSA Cryptosystem*, May 9, 2006.

[23] *Mathematics concepts: The Division Algorithm*, Copyright 2001-MathPath, January 24, 2005, http://www.mathpath.org/concepts/divisionalgo.htm.

[24] *Section 1.5: The Division Algorithm*, Copyright 2001 by W. H. Freeman and Company, http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/divis5.html.

[25] Quo-Shin Chi *Math 310 Class Notes 4: The Well-ordering Principle*, Department of Mathematics, Washington University, http://www.math.wustl.edu/∼chi/310notesIV.pdf.

[26] David Joyner *The Euclidean algorithm*, 2002-08-23, http://www.usna.edu/Users/math/wdj/book/node13.html.

[27] Martyn Quick *Section 2: Greatest Common Divisors and the Euclidean Algorithm*, School of Mathematics and Statistics, University of St Andrews, http://www-groups.dcs.st-and.ac.uk/∼martyn/teaching/1003/1003EuclideanAlgorithm.pdf

[28] Dr. Ernst Kani *The Extended Euclidean Algorithm*, Math 418/818, Number Theory and Cryptography, Fall 2009, Department of Mathematics & Statictics, Queen's University, Kingston, http://www.mast.queensu.ca/∼math418/m418oh/m418oh04.pdf

[29] William Cherowitzo*The Extended Euclidean Algorithm*, Mathematics Department, University of Colorado, Denver, http://www-math.cudenver.edu/ wcherowi/courses/m5410/exeuclid.pdf

[30] Bob Howlett *1. Extended Euclidean Algorithm, 2. Congruence notation*, MATH2068 Number Theory & Cryptography Week 2 Lecture 1, University of Sydney, NSW 2006 Australia, 3rd August 2009.

[31] Bruce Ikenaga *The Extended Euclidean Algorithm*, Millersville University 2008, http://marauder.millersville.edu/∼bikenaga/numbertheory/exteuc/exteuc.html

[32] Monther Rateb Enayah & Azman Samsudin *Securing Telecommunication based on Speaker Voice as the Public Key*, Universiti Sains Malaysia, Penang, Malaysia, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.

[33] Franz Lemmermeyer *Lecture Notes on Elliptic Curves*, Department of Mathematics, http://www.fen.bilkent.edu.tr/∼franz/LN/LN-ellc.html

[34] Avi Kak *Lecture 14: Elliptic Curve Cryptography, Lecture Notes on "Computer and Network Security"*, © Avinash Kak, Purdue University, April 26, 2009.

[35] Keith Matthews *Online number theory lecture notes and teaching materials*, Bribane, Australia, http://www.numbertheory.org/ntw/*lecture_notes*.html

[36] David Loeffler *Elliptic Curves, Notes for the 2004-5 Part III course*, 28/01/2005 - 16/03/2005, http://www.dpmms.cam.ac.uk/∼dl267/maths/lecturenotes/ellipticnotes.pdf

[37] Tanja Lange *Elliptic Curve Cryptography*, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, 20.03.2009.

[38] Dr. F. Vercauteren *Elliptic Curve Cryptography, An Introduction*, Katholieke Universiteit Leuven, 22 April 2008, http://www.cosic.esat.kuleuven.be/publications/talk-95.pdf

[39] *Elliptic curve cryptography*, Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/*Elliptic_curve_cryptography*

[40] *An intro to Elliptic Curve Cryptography*, Jul. 20, 2004, http://www.deviceforge.com/articles/AT4234154468.html

[41] *Overview of Elliptic Curve Cryptosystems*, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2013

[42] *Securing the Web with Elliptic Curve Cryptography*, Copyright 1994-2009 Sun Microsystems, Inc., http://research.sun.com/projects/crypto/

[43] Steven Galbraith *Elliptic Curve Cryptography*, Mathematics Department, University of Auckland, New Zealand, http://www.isg.rhul.ac.uk/∼sdg/ecc.html

[44] Jozef Gruska *Chapter 6 - RSA Cryptosystem*, Faculty of informatics, Masaryk University, Botanicka 68a, Brno, 60200 Czech Republik, http://www.fi.muni.cz/usr/gruska/crypto04/CHAPTER06-RSAcryptosystem.ppt

[45] Marcus Griep *An Introduction to the RSA Cryptosystem*, http://www.devhood.com/Tutorials/*tutorial_details.aspx?tutorial_id* = 544

[46] David Evans *Lecture 12:Non-secret Key Cryptosystems (How Euclid, Fermat and Euler Created E-Commerce)*, CS588: Security and Privacy, University of Virginia, Computer Science, http://www.cs.virginia.edu/cs588/lectures/lecture12.ppt

[47] *Public Key Cryptography (PKC) History*, http://www.livinginternet.com/i/*is_crypt_pkc_inv.htm*

[48] Bob Sedgewick & Kevin Wayne *RSA Public-Key Cryptosystem*, Copyright 2000, http://www.cs.princeton.edu/courses/archive/spring03/cs126/assignments/rsa.html

[49] R.L. Rivest, A. Shamir, and L. Adleman *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, September 1, 1977, http://people.csail.mit.edu/rivest/Rsapaper.pdf

[50] *1.4 How is cryptography applied?*, Feb 5, 2009, RSA conference, https://365.rsaconference.com/docs/DOC-1345

[51] Kevin Wayne & Robert *Security*, Sedgewick at Princeton University, 2004, http://www.cs.duke.edu/courses/spring04/cps001/notes/Security-4up.pdf

[52] E. L. Lady *The Division Algorithm*, July 11, 2000, http://www.math.hawaii.edu/ lee/courses/Division.pdf

[53] Kevin Jeffay *The RSA Public Key Cryptosystem*, Computer and Network Security, Department of Computer Science, University of North Carolina, March 18, 2009.

[54] Martin Leslie *Elliptic Curve Cryptography*, Advanced Combinatorics, June 5, 2006.

[55] Elisabeth Oswald *Introduction to Elliptic Curve Cryptography*, Institute for Applied Information Processing and Communication, Austria, July 29, 2005.

[56] Broughan, K. A. *Number theory lecture notes*, 1998-2003.

[57] Johannes Buchman *Introduction to cryptography*, Springer, 2004.

[58] *Cryptography*, Cryptography portal, http://en.wikipedia.org/wiki/Cryptography

[59] David Terr *History of cryptography*, http://www.davidterr.com/science-articles/cryptography.html

[60] *RSA*, Wikipedia, 30 November 2009, http://en.wikipedia.org/wiki/RSA

[61] Michael Calderbank *The RSA cryptosystem: History, Algorithm, Primes*, August 20, 2007.

[62] *A brief history: The origins of public-key cryptography and ECC*, http://www.certicom.com/index.php/a-brief-history

[63] Charles Edge, William Barker & Zack Smith *A brief history of cryptography*, Foundation of Mac OS X Security, October 23 2007.

[64] *El-Gamal encryption*,Wikipedia, http://en.wikipedia.org/wiki/$ElGamal\_encryption$

[65] *Pollard's* $p-1$ *algorithm*, Wikipedia, http://en.wikipedia.org/wiki/$Pollard'sp-1algorithm$.

[66] *Integer factorization*, Wikipedia, http://en.wikipedia.org/wiki/$Integer\_factorization$.

[67] Boris S. Verkhovsky *Integer factorization: Solution via algorithm for constrained discrete logarithm problem*, Department of Computer Science, New Jersey Institute of Technology, USA, Journal of Computer Sciences 5 (9): 674-679, 2009.

[68] *Integer factorization*, Wapedia, http://wapedia.mobi/en/$Prime\_factorization$

[69] *Integer factorization*, Indopedia, the Indological knowledgebase, http://www.indopedia.org/$Integer\_factorization$.html.

[70] *Factorization attacks on RSA*, CISC, http://www.cs.hku.hk/cisc/projects/va/$fact\_index2$.htm

[71] Susan Schmit & Horst G. Zimmer *Elliptic curves, A computational approach*, Copyright 2003, Berlin, Germany.

[72] Joseph H. Silverman & John Tate *Rational points on elliptic curves*, Undergraduate texts in Mathematics, Copyright 1992 Springer-Verlag, New York Incorporation.

[73] Richard A. Mollin *An introduction to cryptography*, Chapman & Hall, 2001.

[74] Venkat Suryadevara *Efficient on-board RSA key generation with smart cards*, School Electrical Engineering and Computer Sciences, Oregon State University, Corvallis, 2004, http://islab.oregonstate.edu/koc/ece679/2004/suryadevara1.pdf.

[75] *Lenstra elliptic curve factorization*, Wikipedia, http://en.wikipedia.org/wiki/*Lenstra_elliptic_curve_factorization*

[76] *1.4 How is cryptography applied?*, RSA Laboratories, RSA Security 2010, http://www.rsa.com/rsalabs/node.asp?id=2159

[77] Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel & Ingrid Verbauwhede *Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks*, L. Buttyan, V. Gligor, and D. Westhoff (Eds.): ESAS 2006, LNCS 4357, pp. 617, 2006, Springer-Verlag Berlin Heidelberg 2006.

[78] Dr S.A. Vanstone *Next generation security for wireless: elliptic curve cryptography*, 0167-4048/03, Copyright 2003 Elsevier Ltd.

[79] M. Aydos, B. Sunar & C. K. Koc *An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication*, Electrical & Computer Engineering Oregon State University Corvallis, 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October 30, 1998.

[80] Seth Kleinerman *On the torsion points of elliptic curves and modular abelian varieties*, http://modular.math.washington.edu/projects/*kleinerman_senior_thesis.pdf*

[81] Christine Croll *Torsion points of elliptic curves over number theory*, Department of Mathematics, Amherst, Massachusettes, April 21, 2006.

[82] Alvaro Lozano Robledo *Finding points on elliptic curves: Very explicit methods*, November 3, 2003.

[83] Karl Rubin & Alice Silverberg *Ranks of elliptic curves*, Bulletin (New Series) of The American Mathematical Society, Volume 39, Number 4, Pages 455-474, July 8, 2002.

[84] William Stein *Lecture 27: Torsion points on elliptic curves and Mazur's big theorem*, Math 124, Harvard University, 2001.

[85] *NagellLutz theorem*, Wikipedia, http://en.wikipedia.org/wiki/$Nagell - Lutz\_theorem$