5-2013

Number Theory Applications in Cryptography

Francesca Pizzigoni

MONTCLAIR STATE UNIVERSITY

Number Theory Applications in Cryptography

by

Francesca Pizzigoni

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Mathematics

May 2013

College of Science and Mathematics

Department of Mathematics

Certified by:

[redacted]

Dr. Robert Prezant
Dean of College

5/8/13

Date

Thesis Committee:

[redacted]

Dr. Aihua Li
Thesis Sponsor

[redacted]

Dr. Jonathan Cutler
Committee Member

[redacted]

Dr. Diana Thomas
Committee Member

[redacted]

Dr. Helen M. Roberts
Department Chair

NUMBER THEORY APPLICATIONS IN CRYPTOGRAPHY

A THESIS

Submitted in partial fulfillment of the requirements
for the degree of Masters in Pure and Applied Mathematics

by

Francesca Pizzigoni
Montclair State University
Montclair, New Jersey
May, 2013

Abstract

This thesis provides a unique cryptosystem comprised of different number theory applications. We first consider the well-known Knapsack Problem and the resulting Knapsack Cryptosystem. It is known that when the Knapsack Problem involves a superincreasing sequence, the solution is easy to find. Two cryptosystems are designed and displayed in this thesis that allow two parties often called Alice and Bob use a common superincreasing sequence in the encryption and decryption process. They use this sequence and a variation of the Knapsack Cryptosystem to send and receive binary messages. The first cryptosystem assumes that Alice and Bob agree on a shared superincreasing sequence prior to beginning encryption. The second cryptosystem involves Alice and Bob constructing a common, secret, superincreasing sequence built from subsequences of the Fibonacci sequence during the encryption process. Elliptic curves were explored on a smaller scale as they are also applied in cryptography. For a fixed prime number p and a special class of elliptic curves over $\mathbb{Z}_p$, we investigate how many of them intercept the y-axis. Additionally, the research presented in this paper was successfully implemented into a middle school classroom.

Chapter 1 includes introductory material about cryptography. Chapter 2 discusses superincreasing sequences and their appearance in Fibonacci subsequences. It also includes important properties of the Fibonacci sequence. The two cryptosystems are presented in Chapter 3 followed by the brief findings of the intersection of elliptic curves with y-axis in Chapter 4. Finally, Chapter 5 introduces a middle school lesson plan that provided students the experience of cryptography and increased their appreciation of mathematics. A few other lesson plans are provided in the appendix.

Acknowledgments

I would first and foremost like to thank my advisor, Dr. Aihua Li. Her patience and persistence has made this thesis possible. She acted as an inspiring mentor both in and out of the classroom. Her assistance and motivation is truly immeasurable and I am extremely grateful to her.

I would also like to show my appreciation to my parents, family, and friends. Their continued support and words of encouragement truly made an impact on my academic achievements.

A very special thanks to my committee members, Dr. Jonathan Cutler and Dr. Diana Thomas. Their review and helpful suggestions of this thesis were a crucial piece to its completion.

Furthermore, I would like to extend a great deal of thanks to the National Science Foundation and the GK-12 program for the funding of this research. I especially want to thank Dr. Mika Munakata and Eliza Leszczynski for their support throughout the year. I also owe thanks to the other 2012-2013 GK-12 Fellows: Jessica Evans, Alexander Cali, and Anna Slusarczyk for their continued support and comraderie.

Contents

1 Introduction to Cryptography

Cryptography is a branch of mathematics that has been incorporated into our daily lives. As the science of creating secure and efficient codes, it uses various algorithms, known as cryptosystems, to send and receive secret messages. Originated in ancient civilizations, cryptography plays an ever important role in today's society. Every time a credit card is swiped or a computer is used, a security method built from a cryptosystem is applied. It is most significant in matters related to cyber and national security. Deeply rooted in the processes of cryptography is a discrete branch of mathematics known as Number Theory. This project will focus on specific applications of Number Theory in their relevance to cryptography.

Basic Terminology

It is important to be familiar with the various terminology of crytography. Two parties, often named Alice and Bob, are trying to communicate in such a way that an adversary, often named Eve, cannot understand the message. Ideally, the cryptosystem should be built so that even if Eve intercepts a message, he or she cannot uncover its meaning. Therefore, it is crucial that a cryptostem is both efficient and secure.

Encryption

Encryption is the process of taking a *plaintext* piece of information and encoding it in such a way that only the intended recipient can receive and understand the message. The *plaintext* is coded using an algorithm and turned into a *ciphertext.*

Decryption

Decryption is the method used to uncover a *ciphertext.* Through a reverse algorithm,the message is discovered and translated back into the *plaintext* message.

Keys

The algorithm involved in encryption and decryption often uses a key. There are two types of keys: public and private. A *public* key is one that can be known to someone other than the two communicating parties. A *private* key can be used by a single communicating member. It is kept secret for all other members and outsiders. Cryptosystems can often use a combination of both public and private keys.

Throughout the project, we assume the message space is built from integers, integers *mod* a positive integer, or vectors of integers.

2 Superincreasing Sequences

Preliminaries

The first application in Number Theory involves a superincreasing sequence which is defined below.

Definition 1. *A sequence* $r = \{r_1, r_2, ..., r_n\}$ *of positive integers is superincreasing if* $r_{i+1} \geq r_i + r_{i-1} + \cdots + r_1$ *for all* i *with* $1 \leq i \leq n-1$.

An example of a superincreasing sequence is $\{2, 3, 7, 15, 31\}$ as each number is greater than the sum of the numbers before it. These sequences are relatively easy to create and are of great importance to the well-known Knapsack Problem [5]. A simple decipher method is based on the following problem:

Problem 2.1. *The Knapsack Problem*

Given a vector $\vec{a} = (a_1, a_2, \ldots, a_k)$ *of positive integers and a positive integer* A*, the Knapsack Problem for* $(\vec{a}, A)$ *is to find a* k*-vector* $\vec{b} = (b_1, b_2, \ldots, b_k) \in \mathbb{Z}_2^k$ *such that* $\sum_{i=0}^{k-1} a_i b_i = A$ *and* k *is a positive integer.*

Example 1. *The solution to* $((1,3,7,20,42,107),115)$ *is* $(1,0,1,0,0,1)$.

Note that the Knapsack Problem may have no solution, exactly one solution, or more than one solution. It is known that when the vector $\vec{a}$ is formed by a superincreasing sequence and the solution to the Knapsack Problem exists, then the solution is unique [4]. In this case, a simple algorithm can be applied to find the solution. This algorithm is a key player in the Knapsack Cryptosystem which will be explained shortly.

The Knapsack Problem was first recognized in 1957 by George Dantzig. Dantzig, known for his contributions to Operations Research, connected this problem with other maximization problems in the field. Work on the Knapsack Problem continued in the direction of approximation algorithms and other solution methods in the 1980's [2]. The work on various solution techniques may have been sparked by the use of the Knapsack Problem in a public key cryptosystem. This system, as previously mentioned, is known as the Knapsack Cryptosystem and is shown below.

The basic premise of the Knapsack Cryptosystem is provided [4]:

1. Alice has a secret key that is a superincreasing sequence $r = \{r_1, r_2, \ldots, r_n\}$.

2. Alice chooses two private, large integers A and B such that $B > 2r_n$ and $gcd(A, B) = 1$.

3. Alice creates a public key $\vec{M} = (M_1, M_2, \ldots M_n)$, which is an n-vector in $\mathbb{Z}^n$, by calculating $M_i \equiv A \cdot r_i \mod B$ with $0 \leq M_i < B$.

4. Encryption process: Bob chooses a plaintext message $\vec{x} = (x_1, x_2, \ldots, x_n)$ which is a binary $n-$vector. He computes and publishes the ciphertext $C = \vec{x} \cdot \vec{M} = \sum_{i=1}^{n} x_i \cdot M_i$

5. Decryption process: Alice computes

$$C' \equiv A^{-1}C \equiv A^{-1}\sum_{i=1}^{n} x_i M_i \equiv A^{-1}\sum_{i=1}^{n} x_i A r_i \equiv \sum_{i=1}^{n} x_i r_i \mod B.$$

As Alice knows r, she can use Proposition 2.2 below to uncover the plaintext $\vec{x}$ from C'.

Note that in Step 5, $C' \equiv \sum_{i=1}^{n} x_i r_i \mod B$. As $B > 2r_n, C' \leq \sum_{i=1}^{n} r_i \leq r_n + r_n = 2r_n < B$ Therefore, the solution to $C' \equiv \sum_{i=1}^{n} x_i r_i \mod B$ is equivalent to $C' = \sum_{i=1}^{n} x_i r_i$ so Proposition 2.2 can be used.

Proposition 2.2. *[4] Let $r = \{r_1, \ldots, r_n\}$ be a superincreasing sequence and let C' be a positive integer. Consider the Knapsack Problem for $\vec{r}$ and C'. Assuming that a binary solution $\vec{x} = (x_1, \ldots, x_n)$ exists, then it is unique and can be computed with the following steps:*

1. *Determine x_n first.*

   If $C' \geq r_n$, $x_n = 1$. If $C' < r_n$, $x_n = 0$.

2. *A new sum is assigned:*

$$C' := \sum_{i=1}^{n} x_i r_i = C' - r_n x_n.$$

   Repeat the same procedure in Step 1 to find x_{n-1}.

3. *Continue through the procedure until all x_i's are determined.*

The steps above are based on a well-known algorithm for solving the Knapsack Cryptosystem. It is important to note that this algorithm not only finds a solution, but that solution is in fact unique. A proof for the uniqueness of $\vec{x}$ follows:

Proof. Let $C' = x_1 r_1 + x_2 r_2 + \cdots + x_n r_n = y_1 r_1 + y_2 r_2 + \cdots + y_n r_n$ where $\vec{x} = (x_1, x_2, \ldots, x_n)$ and $\vec{y} = (y_1, y_2, \ldots y_n)$ are both in $\mathbb{Z}_2^n$.
Then

$$(y_n - x_n) r_n = (x_1 - y_1) r_1 + \cdots + (x_{n-1} - y_{n-1}) r_{n-1}$$

which implies

$$|y_n - x_n|r_n \leq \sum_{i=1}^{n-1} |x_i - y_i|r_i \leq \sum_{i=1}^{n-1} r_i \quad \text{since} \quad |x_i - y_i| \leq 1 \text{ for all } i = 1, 2, \ldots, n-1$$

If $x_n \neq y_n$, then $|x_n - y_n| = 1$. Thus $r_n \leq \sum_{i=1}^{n-1} r_i$. This is a contradiction as r is a superincreasing sequence. Thus, $x_n = y_n$. By mathematical induction, $x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$ so $\vec{x} = \vec{y}$. □

Example 2. *Consider the Knapsack Problem in Example 1:* $((1, 3, 7, 20, 42, 107), 115)$. *Following Step 1 shown above, we compare* 115 *and* 107. *As* $115 \geq 107$, *we assign* $x_6 = 1$. *For Step 2, our new* $C' = 115 - 107 = 8$. *Continuing to* $r_5 = 42$, *we compare* 8 *and* 42. *As* $8 < 42$, *we assign* $x_5 = 0$ *and therefore* C' *remains 8. Similarly, we would find* $x_4 = 0$. *Comparing* r_3, $8 \geq 7$ *so* $x_3 = 1$. *Our new* $C' = 1$ *and trivially,* $x_2 = 0$ *and* $x_1 = 1$. *Therefore, the solution is* $(1, 0, 1, 0, 0, 1)$.

For convenience, with superincreasing sequence $r = \{r_1, r_2, \ldots, r_n\}$, we denote $\vec{r} = (r_1, r_2, \ldots, r_n)$ and call it a superincreasing vector. We will now show an example of the Knapsack Cryptosystem.

Example 3.

1. *Alice has a secret key* $\vec{r} = (1, 2, 5, 13, 34, 89, 233, 610)$ *which is superincreasing.*

2. *She chooses* $A = 101$ *and* $B = 1221$. *Note that* $B > 2r_n$ *and* $gcd(A, B) = 1$.

3. *Alice calculates the non-negative residue of* $\vec{M} \equiv A \cdot r_i \mod B$ *and obtains* $\vec{M} = (101, 202, 505, 92, 992, 442, 334, 560)$ *and sends this to Bob.*

4. *Encryption: Bob has a plaintext message* $\vec{x} = (0, 0, 1, 1, 0, 0, 1, 0)$. *He computes* $C = \vec{x} \cdot \vec{M} = 931$ *and sends it over to Alice.*

5. *Alice computes* $C' \equiv A^{-1}C \mod B$. *Here,* $A^{-1} = 677$ *which can be found using the Euclidean Algorithm. Thus,* $C' \equiv (677)(931) \mod 1221 \equiv 251$. *Using Proposition 2.2, she achieves the plaintext message* $\vec{x} = (0, 0, 1, 1, 0, 0, 1, 0)$.

Properties of the Fibonacci Sequence and Related Sequences

Because superincreasing sequences are so relevant to the Knapsack Cryptosystem, we examined a few different sequences for their superincreasing nature. One of the most commonly known sequences is the Fibonacci sequence $\{F_n\}_0^\infty$. The numbers in this sequence are created by adding the two previous numbers in the sequence. The first few terms are $\{0, 1, 1, 2, 3, 5, 8, 13, \dots\}$.

Definition 2. *The Fibonacci sequence is defined as:* $F_0 = 0, F_1 = 1, F_{n+2} = F_n + F_{n+1}$ *for all non-negative integers* n.

The Fibonacci sequence has several important properties. The following property is of utmost importance to this paper.

Property 2.3. *[12]* $F_{n+2} = F_1 + F_2 + \cdots + F_n + 1$.

On the surface, the Fibonacci sequence appears to follow a recursive formula. However, Binet derived an explicit formula for the sequence in 1843 based on the Golden ratio $\alpha = \frac{1+\sqrt{5}}{2}$. The formula follows.

Proposition 2.4. *Let* $\alpha = \frac{1+\sqrt{5}}{2}$ *and* $\beta = \frac{1-\sqrt{5}}{2}$ *so that* α *and* β *are roots of the equation* $x^2 = x + 1$. *Then* $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$ *for all* $n \geq 1$.

The number α is known as the Golden Ratio. The following corollary is a direct result of the above formula.

Corollary 2.5. *For any* $n \in \mathbb{Z}^+, F_n < \frac{2^{n+1}}{\sqrt{5}}$.

Proof. From Binet's formula, we know that $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$ and $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$. Now since $|\alpha| > |\beta|$, and $|\alpha| \geq 1$, we can say that $|\alpha|^n > |\beta|^n$. Therefore, $\alpha^n + |\beta|^n < 2\alpha^n$. Because of this, we can say that $F_n = \frac{\alpha^n - |\beta|^n}{\sqrt{5}} < \frac{2\alpha^n}{\sqrt{5}}$ and since $\alpha < 2$, we can conclude that $F_n < \frac{2^{n+1}}{\sqrt{5}}$. □

Lemma 2.6. *Consider positive integers $n, g > 1$. Let p be a prime number such that $p > g$. Then if $0 < R < \left\lfloor \frac{log_2(\sqrt{5}p) - g - 1}{n-1} \right\rfloor$, then $F_{g+R(n-1)} < p$*

Proof. We know that $R < \left\lfloor \frac{log_2(\sqrt{5}p) - g - 1}{n-1} \right\rfloor < \frac{log_2(\sqrt{5}p) - g - 1}{n-1}$ so $R(n-1)+g+1 < \log_2(\sqrt{5}p)$ which implies $2^{R(n-1)+g+1} < \sqrt{5}p$.

$$\text{Thus from Corollary 2.5, } F_{g+R(n-1)} < \frac{2^{R(n-1)+g+1}}{\sqrt{5}} < p.$$

□

As previously mentioned, superincreasing sequences play a key role in the Knapsack Cryptosystem. As we move to the Fibonacci sequence, it can be shown that this is not a superincreasing sequence. We will also prove that any consecutive subsequence of length at least three is also not superincreasing.

Lemma 2.7. *The Fibonacci sequence is not a superincreasing sequence. In particular, any consecutive finite subsequence $\{F_m, F_{m+1}, \ldots, F_{m+r}\}$ where $r > 2, m > 0$ is not superincreasing.*

Proof. A simple counterexample will prove that Fibonacci sequence is not superincreasing. Consider the first few terms of the sequence: $\{0, 1, 1, 2, 3, 5, \ldots\}$. It can easily be seen that $3 < 0 + 1 + 1 + 2$. In other words, $F_4 \not> \sum_{i=0}^{3} F_i$.

Now consider the sequence $\{F_m, F_{m+1}, \ldots, F_{m+r}\}$ for $m > 0, r > 2$. A simple check shows that $F_{m+3} = F_{m+2} + F_{m+1} < F_{m+2} + F_{m+1} + F_m$. Thus, $F_{m+3} \not> F_{m+2} + F_{m+1} + F_m$. □

This project considers not only the Fibonacci sequence, but also Lucas sequence. The Lucas sequence $\{L_n\}_0^\infty$, while very similar to the Fibonacci sequence, begins with the integers 2 and 1 and follows the same rule after the first two numbers. Thus by definition, $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_n + L_{n+1}$ if $n \geq 0, n \in \mathbb{Z}$. Therefore, Lucas sequence is as follows: {2,1,3,4,7,11, ...} which is not superincreasing. Lucas sequence can be directly linked to the Fibonacci sequence with the following formula.[12]

Lemma 2.8. $L_n = F_{n-1} + F_{n+1} = F_n + 2F_{n-1}$

Lucas sequence is expressed in Lemma 2.8 as a linear combination of certain Fibonacci numbers. Therefore, it is no surprise that Lucas is not a superincreasing sequence.

Superincreasing Subsequences of the Fibonacci Sequence and Lucas Sequence

Although the Fibonacci sequence is not a superincreasing sequence, a closer look shows that it does have many superincreasing subsequences. For example, the even terms of the Fibonacci sequence, $\{0, 1, 3, 8, 21, \ldots, \}$, form a superincreasing sequence. In fact, any subsequence that does not use consecutive Fibonacci numbers forms a superincreasing sequence.

Theorem 2.9. *A subsequence* $S = \{F_m, F_{m+r_1}, F_{m+r_1+r_2}, \ldots, F_{m+r_1+r_2+\cdots+r_d}, \ldots\}$ *of the Fibonacci sequence is a superincreasing sequence if* $d \geq 1$, *with all* $r_i \geq 2$.

Proof. Let d be a positive integer. Then by Property 2.3 above,

$$F_{m+r_1+r_2+\cdots+r_d} = F_1 + F_2 + \cdots + F_{m+r_1+r_2+\cdots+r_d-2} + 1.$$

Since all $r_i \geq 2$ and $r_d - 2 \geq 0$, then $m+r_1+r_2+\cdots+r_{d-1}+r_d-2 \geq m+r_1+r_2+\cdots+r_{d-1}$

which implies that

$$F_{m+r_1+r_2+\cdots+r_{d-1}+r_d} > F_m + F_{m+r_1} + \cdots + F_{m+r_1+r_2+\cdots+r_{d-1}}.$$

for all positive integers d. Thus, $S = \{F_m, F_{m+r_1}, F_{m+r_1+r_2}, \ldots, F_{m+r_1+r_2+\cdots+r_d}, \ldots\}$ is superincreasing. □

If all r_i are the same, we obtain a special case of the above theorem. This case creates a subsequence of the Fibonacci sequence with evenly spaced terms. For example, 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89... is Fibonacci Sequence out to the 12th term. Consider the subsequence created with every third number: 1, 5, 21, 89. This subsequence is a superincreasing sequence.

Corollary 2.10. *A subsequence $D = \{F_m, F_{m+d}, F_{m+2d}, F_{m+3d}, \ldots, F_{m+kd}\}$ of the Fibonacci sequence is a superincreasing sequence for all $d > 1$ and $k \geq 0$.*

Proof. If $k = 0$, we have $\{F_m\}$ which is trivially superincreasing. If $k > 0$, this is a direct result of the previous theorem. □

The above theorems show that there are an infinite number of superincreasing subsequences of the Fibonacci sequence. Moving on to Lucas sequence, we can follow the same logic. As previously stated, Lucas sequence is a linear combination of Fibonacci sequences. Consider the following lemma.[12]

Lemma 2.11. *If α_n and β_n are superincreasing sequences, then $a\alpha_n + b\beta_n$ is superincreasing for all $a, b > 0$.*

We can create superincreasing subsequences of Lucas sequence if we use a linear combination of superincreasing Fibonacci subsequences.

Generalized t-Superincreasing Sequences

Proposition 2.2 is the main piece to the Knapsack Cryptosystem but the solution must be binary. With such a valuable proposition, one might ask, "Can we find other sequences that guarantee the uniqueness of the solution to a Knapsack Problem and the solution can be retrived similarly?" A generalization of superincreasing sequences, callled $t-$superincreasing sequences, is defined below.

Definition 3. *A sequence $r = \{r_1, r_2, ..., r_n\}$ of positive integers is t-superincreasing if $r_n \geq (t-1)(r_1 + r_2 + \cdots + r_{n-1})$.*

The superincreasing sequence, defined earlier in this paper, is a 2-superincreasing sequence. We now consider a 3-superincreasing sequence $r = \{r_1, r_2, \ldots, r_n\}$ such that $r_i \geq 2(r_1 + r_2 + \cdots + r_{i-1})$ for all $i = 2, 3, \ldots, n$.

Theorem 2.12. *Consider the Knapsack Problem for a 3-superincreasing sequence $r = \{r_1, r_2, \ldots, r_n\}$ and a positive integer S.*

1. *If a solution exists in $\mathbb{Z}_3^n$, then it is unique.*

2. *Let $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_3^n$ be a solution then*

$$x_n = \begin{cases} 0 & \text{if } S < r_n \\ 1 & \text{if } r_n \leq S < 2r_n \\ 2 & \text{if } S \geq 2r_n. \end{cases} \tag{1}$$

Proof. 1. $S < r_n$ if and only if $x_n = 0$ because

$S < r_n \Leftrightarrow x_1r_1 + x_2r_2 + \cdots + x_nr_n < r_n$

$\Leftrightarrow x_1r_1 + x_2r_2 + \cdots + x_{n-1}r_{n-1} < r_n(1 - x_n)$

$\Leftrightarrow x_n = 0$ since $x_1r_1 + x_2r_2 + \cdots + x_{n-1}r_{n-1} \geq 0$.

2. $r_n \leq S < 2r_n$ if and only if $x_n = 1$ since

   $r_n \leq S < 2r_n \Leftrightarrow r_n \leq x_1r_1 + x_2r_2 + \cdots + x_nr_n < 2r_n$

   $\Leftrightarrow r_n(1 - x_n) \leq x_1r_1 + x_2r_2 + \cdots + x_{n-1}r_{n-1} < r_n(2 - x_n)$

   $\Leftrightarrow x_n = 1$ since $x_1r_1 + x_2r_2 + \cdots + x_{n-1}r_{n-1} \geq 0$ and

   $r_n > 2(r_1 + r_2 + \cdots + r_{n-1}) \geq x_1r_1 + x_2r_2 + \cdots + x_{n-1}r_{n-1}$.

3. $S \geq 2r_n$ if and only if $x_n = 2$ because

   $S \geq 2r_n \Leftrightarrow x_1r_1 + x_2r_2 + \cdots + x_{n-1}r_{n-1} \geq r_n(2 - x_n)$

   $\Leftrightarrow x_n = 2$ for similar reasons named above.

□

This algorithm can truly be applied to any $t-$superincreasing sequence.

Theorem 2.13. *Consider a Knapsack Problem (r, S) where r is the t-superincreasing sequence created from $\vec{r}$ and S is a positive integer.*

1. *If a solution exists in $\mathbb{Z}_t^n$, then it is unique.*

2. *Let $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_t^n$ be a solution then*

$$x_n = \begin{cases} 0 & \text{if } S < r_n \\ 1 & \text{if } r_n \leq S < 2r_n \\ 2 & \text{if } 2r_n \leq S < 3r_n \\ \vdots & \\ t-1 & \text{if } S \geq (t-1)r_n \end{cases} \tag{2}$$

The proof of this theorem is similar to the previous proof. Therefore, it has been omitted.

3 Cryptosystem using the Fibonacci Sequence

Two Variations of the Cryptosystem

Using our knowledge of the Knapsack Cryptosystem and superincreasing sequences, we created the following cryptosystems. The first cryptosystem assumes that Alice and Bob possess a common key in the form of a superincreasing sequence before any interactions take place. The second cryptosystem allows Alice and Bob to create a common shared key amidst the system.

Cryptosystem Version 1: Secret Key Provided

Alice and Bob share a common key in the form of a superincreasing sequence which is provided beforehand and represented by the vector $\vec{r} = (r_1, r_2, \ldots, r_n)$.

The public keys include $g \in \mathbb{Z}^+, g \neq 1$, and a large prime p such that $p > 2r_n$. Alice has a secret key $a \in \mathbb{Z}^+$ such that $gcd(a, p-1) = 1$ and Bob has a secret key $k \in \mathbb{Z}^+$ such that $gcd(k, p-1) = 1$.

1. Alice computes $A \equiv g^a \mod p$ and sends A to Bob.
2. Bob encrypts his plaintext message $\vec{x} \in \mathbb{Z}_2^n$ by sending (c_1, c_2) to Alice where $c_1 \equiv g^k \mod p$ and $c_2 \equiv A^k(\vec{x} \cdot \vec{r}) \mod p$.
3. Alice decrypts the messages by doing $C' \equiv (c_1)^{-a}(c_2) \mod p$. She then solves the Knapsack Problem with $\{\vec{r}, C'\}$ to get back to the plaintext message $\vec{x}$.

Proof.

$$(c_1)^{-a}(c_2) \mod p \equiv (g^{ka})^{-1} g^{ka} \vec{x} \cdot \vec{r} \equiv \vec{x} \cdot \vec{r}$$

Because $p > 2r_n$, this result is just a Knapsack problem with $(\vec{r}, \vec{x} \cdot \vec{r})$ and Proposition 2.2 can be used to solve for $\vec{x}$. □

Example 4. *Alice and Bob have the common, secret key* $\vec{r} = (1, 2, 5, 13, 34, 89, 233, 610)$ *which is superincreasing.*

Public Keys: $g = 99$ *and* $p = 1223$.

Private Keys: Alice's $a = 7$ *Bob's* $k = 3$.

1. *Alice computes* $A \equiv g^a \mod p \equiv 856$ *and sends this to Bob.*

2. *Bob has the plaintext message* $\vec{x} = (0, 0, 1, 1, 0, 0, 1, 0)$. *He computes* (c_1, c_2) *where* $c_1 = 460 \equiv g^k \mod p$, *and* $c_2 = 45 \equiv A^k(\vec{x} \cdot \vec{r}) \mod p$. *Bob sends* $(460, 45)$ *to Alice.*

3. *Alice computes* $C' \equiv (c_1)^{-a}(c_2) \mod p$. $c_1^{-a} \equiv 351^{-1} \mod p \equiv 233$. $C' = 251$. *She solves the Knapsack Problem for* $(\vec{r}, 251)$ *to recover the plaintext message* $\vec{x} = (0, 0, 1, 1, 0, 0, 1, 0)$.

The above cryptosystem is based on the fact that Alice and Bob already have a common superincreasing sequence. This is a fairly large assumption so we have created another similar cryptosystem that creates a common superincreasing sequence based on Fibonacci subsequences.

Cryptosystem Version 2: Secret Key Created

The following are public keys: a fixed $n \in \mathbb{Z}^+$ such that $n \geq 2$, a large prime $p >> \frac{2^{10n-7}}{\sqrt{5}}$, and $g \in \mathbb{Z}^+$ such that $1 < g \leq \log_2(\sqrt{5}p) - 10n + 9$, and $p \nmid g$.
Alice has a secret key $a \in \mathbb{Z}^+$ such that $gcd(a, p-1) = 1$ and Bob has a secret key $k \in \mathbb{Z}^+$ such that $gcd(k, p-1) = 1$.

1. Alice computes $A = g^a \mod p$ and sends A to Bob.

2. In order to encrypt his plaintext message $\vec{x} \in \mathbb{Z}_2^n$, he needs to create a superincreasing

vector $\vec{r}$. Bob computes $K \equiv A^k \mod p$. He then computes

$$u = \left\lfloor \frac{log_2(\sqrt{5}p) - g - 1}{n-1} \right\rfloor.$$

If $K < u$,

$$\vec{r} = \{F_g, F_{g+K}, F_{g+2K}, \ldots, F_{g+(n-1)K}\}.$$

If $K \geq u$,

$$\vec{r} = \{F_g, F_{g+v}, F_{g+2v}, \ldots, F_{g+(n-1)v}\}$$

where $v = \lfloor \frac{K}{w} \rfloor$ and $w = \lfloor \frac{K}{u} \rfloor + 1$.

Bob can now encrypt $\vec{x}$ by sending (c_1, c_2) to Alice where $c_1 = g^k \mod p$ and $c_2 = A^k(\vec{x} \cdot \vec{r}) \mod p$.

3. Alice computes $K = c_1^a \equiv g^{ka} \mod p$. She then creates a superincreasing vector $\vec{r}$ in the same manner as Bob. They now have a shared, secret, superincreasing sequence $\vec{r}$.

4. Alice decrypts the messages by computing $C' \equiv (c_1)^{-a}(c_2) \mod p$. She then uses the special proposition with C' and $\vec{r}$ to get back to the plaintext message $\vec{x}$. This result occurs because $(c_1)^{-a}(c_2) \mod p \equiv (g^{ka})^{-1} g^{ka} \vec{x} \cdot \vec{r} \equiv \vec{x} \cdot \vec{r} \mod p$.

Proof. Because $p > \frac{2^{10n-7}}{\sqrt{5}}$, $\sqrt{5}p > 2^{10n-7}$. This implies $log_2(\sqrt{5}p) \geq 10n - 7$ so $log_2(\sqrt{5}p) - 10n + 9 \geq 2$. As $g \leq log_2(\sqrt{5}p) - 10n + 9$, we can conclude that $g \geq 2$.

1. Case 1: $K < u$, $\vec{r} = \{F_g, F_{g+K}, F_{g+2K}, \ldots, F_{g+(n-1)K}\}$.

   We need to show that $K \geq 2$ so that $\vec{r}$ is superincreasing.

   Because $gcd(a, p-1) = 1$ and $gcd(k, p-1) = 1$, $K = g^{ak} \mod p > 1$. Thus $K \geq 2$. Then from Theorem 2.9, we know that $\vec{r}$ creates a superincreasing sequence. To prove $F_{g+(n-1)K} < p$:

$$\text{Because } K < \left\lfloor \frac{log_2(\sqrt{5}p) - g - 1}{n-1} \right\rfloor$$

we can use Lemma 2.6 to show that $F_{g+(n-1)K} < p$. Because the last number in our sequence is less than p, Proposition 2.2 can now be used to uncover the message.

2. Case 2: $K \geq u$, $\vec{r} = \{F_g, F_{g+v}, F_{g+2v}, \ldots, F_{g+(n-1)v}\}$.

   We need to prove $v \geq 2$:

   $p > \frac{2^{10n-7}}{\sqrt{5}}$ so $\sqrt{5}p > 2^{10n-7} > 2^{10n-9} \Rightarrow log_2(\sqrt{5}p) - 10n + 9 > 0$

   Since $g \leq log_2(\sqrt{5}p) - 10n + 9$, then $g + 10n - 9 \leq log_2(\sqrt{5}p) \Rightarrow g + n + 9n - 9 \leq log_2(\sqrt{5}p)$

   Thus $9(n-1) \leq log_2(\sqrt{5}p) - g - n \Rightarrow 9 \leq \frac{log_2(\sqrt{5}p)-g-n}{n-1} = \frac{log_2(\sqrt{5}p)-g-1}{n-1} - 1$

   From here, we know that $9 \leq \frac{log_2(\sqrt{5}p)-g-1}{n-1} - 1 \leq u$. Thus $6 \leq u - 3$. Then $\frac{6}{u-3} \leq 1 \Rightarrow \frac{6u}{u-3} \leq u \leq K$ in this case.

   Therefore, $K \geq \frac{6u}{u-3} \Rightarrow Ku - 3K \geq 6u \Rightarrow K \geq 6 + \frac{3K}{u} = 3(2 + \frac{K}{u})$.

   This implies $K \geq 3(1 + \lfloor \frac{K}{u} \rfloor)$ so $K \geq 3w$ or in other words $\frac{K}{w} \geq 3$.

   Lastly, $v = \lfloor \frac{K}{w} \rfloor \geq \frac{K}{w} - 1 \geq 2$ Because $v \geq 2$, from Theorem 2.9, we know that $\vec{r}$ creates a superincreasing vector.

   To prove $F_{g+(n-1)v} < p$:

$$v = \left\lfloor \frac{K}{u} \right\rfloor = \left\lfloor \frac{K}{\lfloor \frac{K}{u} \rfloor + 1} \right\rfloor < \frac{K}{\frac{K}{u}} = u$$

$$v < \left\lfloor \frac{log_2(\sqrt{5}p) - g - 1}{n-1} \right\rfloor$$

   Now using Lemma 2.6, we can show that $F_{g+(n-1)v} < p$. Because the last number in our sequence is less than p, Proposition 2.2 can now be used to uncover the message.

□

Example 5. *Public Keys:* $n = 4, g = 2, p = 12431470127$

Private Keys: Alice's $a = 7$, *Bob's* $k = 11$

1. *Alice computes* $A \equiv g^a \mod p$, $A = 128$.

2. *Bob has the plaintext message* $\vec{x} = (1, 0, 1, 1)$. *He computes* $K \equiv A^k \mod p$, $K = 8362875137$ *and* $u = 10$. *Because* $K \geq u$, *Bob finds* $\vec{r} = (1, 89, 6765, 514229)$ *which is superincreasing. He then sends Alice* $(c_1, c_2) = (2048, 9618950101)$.

3. *Alice computes* $K \equiv c_1^a \mod p$. *She similarly finds* $\vec{r} = (1, 89, 6765, 514229)$.

4. *Alice decrypts the message by computing* $C' \equiv (c_1)^{-a}(c_2) \mod p$. *She finds* $C' = 520995$ *and uses Proposition 2.2 to solve the Knapsack Problem for* $(\vec{r}, C')$ *to get back to the plaintext message* $\vec{x} = (1, 0, 1, 1)$.

Version 2 of the cryptosystem has quite a few intricate steps. To increase the feasibility of the computations, an algorithm for the cryptosystem has been written using the software SAGE and can be found in the Appendix. The next part of this paper will consider another piece of cryptography that uses many applications in Number Theory.

4 A Special Case of Elliptic Curves and the Points on the Y-Axis

Elliptic curves are becoming increasingly important in the world of cryptography. Elliptic Curve Cryptography, or *ECC*, represents one of the most modern methods used today. In this chapter, we will examine a special class of elliptic curves and establish when this set of curves will have a y-intercept. An elliptic curve E over a field $\mathbb{F}$ is defined by an equation of the form $y^2 = x^3 + Ax + B$, where A, B $\in \mathbb{F}$ satisfy $4A^3 + 27B^2 \neq 0$. A pair (x, y) where

$x, y \in \mathbb{F}$, is a point on the curve if (x, y) satisfies the above equation [4]. Elliptic curves have their own binary addition defined in a specific way. ECC uses the algebraic structure of the curve $y^2 = x^3 + Ax + B$ over a field $\mathbb{F}$ to encrypt and decrypt messages. Precisely, E is defined as follows:

Definition 4. *$E(\mathbb{F}) = \{(x, y) \mid x, y \in \mathbb{F}, y^2 = x^3 + Ax + B\} \bigcup \{\mathcal{O}\}$, where $\mathcal{O}$ represents the identity of this closed algebraic group. The operation of the group is represented as $\oplus$, defined below:[4]*
Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E.

1. *For every $P \in E(\mathbb{F}), P \oplus \mathcal{O} = P = \mathcal{O} \oplus P$*
2. *If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = \mathcal{O}$.*
3. *If $x_1 \neq x_2, P_1 \oplus P_2 = (x_3, y_3)$ where*

$$x_3 = \lambda^2 - x_1 - x_2 \quad and \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

for

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & if P_1 \neq P_2 \\ (3x_1^2 + A)(2y_1)^{-1} & if P_1 = P_2 \end{cases}$$

Example 6. *For example, if E is an elliptic curve $\in \mathbb{F}_7$, then the curve $y^2 = x^3 + 10x - 2$ consists of the following points:*

$$\{\mathcal{O}, (1,3), (1,10), (2,0), (3,4), (3,9), (5,2), (5,11), (6,1), (6,12), (11,3), (11,10), (12,0)\}.$$

Elliptic curves, as previously mentioned, are curves of the form $y^2 = x^3 + Ax + B$. It is important to notice that the left hand side must be a perfect square. In a finite field, perfect squares are called quadratic residues.

Definition 5. *[11] If m is a positive integer, we say that an integer a is a quadratic residue of m if $(a, m) = 1$ and the congruence $x^2 \equiv a \mod m$ has a solution. If the congruence $x^2 \equiv a \mod m$ has no solution, we say that a is a quadratic nonresidue of m.*

Example 7. *3 is a quadratic residue modulo 13 because $4^2 \equiv 3$ mod 13. On the contrary, 8 is a quadratic nonresidue because there is no integer which, when squared, will give 8 modulo 13.*

It will be shown in a later section why quadratic residues play an especially important role in elliptic curve cryptography. Because of their importance, it is valuable to know some key properties of quadratic residues. These properties can also be found in any number theory book.

Proposition 4.1. *Let p be an odd prime number.*

1. *The product of two quadratic residues modulo p is a quadratic residue modulo p.*
2. *The product of a quadratic residue and a quadratic nonresidue modulo p is a quadratic nonresidue modulo p.*
3. *The product of two quadratic nonresidues modulo p is a quadratic residue modulo p.*

Definition 6. *[4] Let p be an odd prime and a be an integer not divisible by p. The Legendre Symbol $\left(\frac{a}{p}\right)$ is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Using this definition, a is a quadratic residue of p if and only if $\left(\frac{a}{p}\right) = 1$. The next theorem states some of the basic properties of the Legendre Symbol.

Theorem 4.2. *Let p be any odd prime and a and b be integers not divisible by p. Then*

1. *if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3. $\left(\frac{a^2}{p}\right) = 1$.

Theorem 4.3. *[4] Let p be an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8, \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12}, \end{cases} \quad \text{and}$$

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 4 \pmod 5 \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod 5. \end{cases}$$

Theorem 4.4 (The Law of Quadratic Reciprocity)**.** *[4] Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Theorem 4.5.

$$\left(\frac{p}{q}\right) = \begin{cases} \frac{q}{p} & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\frac{q}{p} & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Some equations of the form $x^3 + Ax + B$ can be factored as $(x - a)(x - a^2)(x + a + a^2)$ where $a \in \mathbb{Z}$. We consider this factorization of an elliptic curve a special case of interest.

Recall Example 6. Notice that this curve does not have a y-intercept. A question naturally asked is: using the previous factorization, can we predict the number of a values that will result in curve with a y-intercept?

Methodology

Let's assume we work with a finite field, $\mathbb{Z}_p$ where p is an odd prime. As mentioned earlier, there is one condition that must hold for elliptic curves, that is, $4A^3 + 27B^2 \neq 0$. This requires that the curve not have any double roots. In other words, all factors are distinct. This restricts the possible a values in our factored form. For any prime p, $a \neq 0, 1, -2, (-2)^{-1}$ in order to guarantee that $(x-a)(x-a^2)(x+a+a^2)$ does not have any double roots in $\mathbb{Z}_p$.

In order to explore the y-intercepts of the curve, we set $x = 0$. The equation becomes $y^2 = a^4(a+1)$. For a solution to exist, $a + 1 = b^2$ for some $b \in \mathbb{Z}_p$. Thus $y^2 = a^4b^2 = (a^2b)^2 \Rightarrow y = \pm a^2b$.

In this case, two solutions exist: $(0, a^2b)$ and $(0, -(a^2b))$. However, if $a^2b = -(a^2b)$ then $2a^2b = 0$.

With the condition that $a \neq 0, 1, -2, (-2)^{-1}$ in $\mathbb{Z}_p$, this implies that $p|(a+1)$ or $p|b$ which implies that $a = -1$. Thus, the curve has y-intercepts if and only if $a + 1$ is a quadratic residue of p. When $a + 1$ is a quadratic residue, there exists two y-intercepts if and only if $a \neq -1$.

Definition 7. *For an odd prime p, define* $S_p = \{E_a(\mathbb{Z}_p) | y^2 = (x-a)(x-a^2)(x+a+a^2) \mod p$ *where* $a \in \mathbb{Z}, a \neq 0, 1, -2, (-2)^{-1} \mod p\}$

Now the question is: for a fixed prime p, how many $E_a(\mathbb{Z}_p) \in S_p$ intersect with the y-axis? We know that $a \neq 0, 1, -2, (-2)^{-1}$ thus $a+1 \neq 1, 2, -1, (-2)^{-1}+1$. To know how many a's, for a set p, will have a solution, we need to remove the values listed above that are quadratic

residues. One should note that if 2 is a quadratic residue then 2^{-1} is a quadratic residue. However, $(-2)^{-1}+1 = 2^{-1}$ so $(-2)^{-1}+1$ is a quadratic residue which can also be proven using Legendre symbols.

Theorem 4.6. *Consider $E_a \in S_p$. Assume $p \equiv r \mod 8$ $(0 \leq r < 8)$. There are m_r many a's $\in \mathbb{Z}_p$ such that the elliptic curve E_a has a y-intercept.*

$$m_r = \begin{cases} \dfrac{p+r-8}{2} & \text{if } r = 1, 5 \\ \dfrac{p+r-4}{2} & \text{if } r = 3 \\ \dfrac{p+r-12}{2} & \text{if } r = 7 \end{cases} \tag{3}$$

Proof. It is known that for a given p, there are exactly $\frac{p+1}{2}$ quadratic residues. We investigate how many values of $a+1$ can be quadratic residues. Since $a \neq 0, a+1 \neq 1$ so $\frac{p-1}{2}$ can be quadratic residues. With the added condition that $a+1 \neq 2, -1, 2^{-1}$, we can count how many a's such that $a+1$ is a quadratic residue. This all depends on how many amont the three values: $2, -1, 2^{-1}$ are quadratic residues of p. We will subtract the values from $\frac{p-1}{2}$.

1. If $p \equiv 1 \mod 8 \Rightarrow -1, 2, (-2)^{-1}+1$ are quadratic residues so there are $(p-7)/2$ quadratic residues.

2. If $p \equiv 3 \mod 8 \Rightarrow -1, 2, (-2)^{-1}+1$ are not quadratic residues so there are $(p-1)/2$ quadratic residues.

3. If $p \equiv 5 \mod 8 \Rightarrow -1$ is a quadratic residue but 2 and $(-2)^{-1}$ are quadratic residues so there are $(p-3)/2$ quadratic residues.

4. If $p \equiv 7 \mod 8 \Rightarrow 2, (-2)^{-1}$ are quadratic residues but -1 is not so there are $(p-5)/2$ quadratic residues.

□

Example 8. *Consider the special elliptic curve with* $p = 11$. *Since* $11 \equiv 3 \mod 8, r = 3$. *Therefore,* $\frac{p+r-4}{2} = \frac{11+3-4}{2} = 5$. *There are 5 values for a which, when* $x = 0$, *will provide a y-intercept on the curves. These a values are the following: 2, 3, 4, 8, 10. For example, when* $x = 0$ *and* $a = 2, y^2 = 4$. *Therefore, the points* $(0, 2)$ *and* $(0, 9)$ *are y-intercepts on the curve* $y^2 = (x - 2)(x - 4)(x + 6)$.

5 Applications in Education

This research was funded by the National Science Foundation through a program called "GK-12: Fellows in the Middle" at Montclair State University. Through this program, math and science graduate students are paired up with a team of middle school science and math teachers, and their research advisors. The graduate students, or fellows, attend the middle school once a week to teach integrated math and science lessons. The author of this paper, the math fellow, was paired with Jessica Evans, the science fellow. Our team worked in cooperation with Noreen Wiggins and Catherine Sickinger, the 6th grade math and science teachers, respectively, at the Franklin School in Kearny, New Jersey. There are several goals for the GK-12 program. At the very least, the program aims for the middle school students to experience math and science in a whole new light. The middle school students have the opportunity to observe the graduate fellows in fields of which the young students may have never heard. The integrated lessons are refreshing and the students are often sparked with new interest in math and science. Another important goal of the GK-12 program is to provide the teachers with sample integrated lessons and general ideas on how to increase students' interest in STEM fields. Teachers are often overwhelmed with the amount of curriculum they are required to teach. By integrating math with science, previous concepts can be reinforced while teaching a new idea. An additional important goal of the GK-12 Program is to allow the graduate students to enhance their own communication skills. Consequently,

the fellows are asked to create middle school lessons based on their research topics. As cryptography is often unheard of in a middle school classroom, the author of this thesis took the opportunity to show the students a brand new side of math. Displayed below is a lesson titled "Shift Cipher Shenanigans." The lesson introduces the concept of Cryptography to the students. They then learn the most basic cryptosystem, the Shift Cipher. Two additional lesson plans can be found in the appendix. The first, titled "How to Sound Like a Secret Agent" reviews more vocabulary and introduces the Substitution Cipher. The second is a lesson plan that explores the basics of modular arithmetic. It is titled "Modeling Modular Arithmetic." Through these lessons, key middle school concepts are reinforced. For example, dividing with a remainder is relevant to modular arithmetic.

Lesson: Shift Cipher Shenanigans

Grade: 6

Time: One 45 Minute Class Period

Materials:

- Jumble Warm-Up
- Wheel Worksheet printed on Cardstock (20)-precut to save time
- Practice Sheet
- Paper Fasteners (25)

Goal: The students will be introduced to cryptography and specifically, the shift or Caesar cipher.

Objective: Students will code and decode various messages using the shift cipher cryptosystem.

Standards Addressed:

-Math Common Core: 6.EE.2, 6.EE.4

-NJCCCS Science: 5.1.4.A..2, 5.1.4.A.3, 5.1.4.B.2 .

Procedure/ Lesson:

- Warm-Up: Find the daily jumble @ http://jumble.com/games/info/13
- Tell the students that we are going to start with a game today. The object is to jumble the letters around to find the right word. Make it a class effort. If necessary, click hint. Note: This may be necessary as some words may be above their vocabulary. **Dont let the warm-up go beyond 7-8 minutes.
- Ask the students if they liked that activity. Some may love the activity and some may not. Explain that puzzle solving can be very similar to Mathematics is several ways. One major way that puzzle solving is related to Mathematics is through Cryptography.
- Write the word "cryptography" on the board so the students can see it. Describe cryptography to the students in the following way.
  - Cryptography is a whole area of mathematics dedicated to sending and receiving secret messages. There are mathematicians that spend quite a bit of time studying— different ways of sending and receiving these messages in a secretive way. Today, we are going to learn just one of those ways.
- Let us take a moment to think of why we need to send messages in a secret way.
- If I wanted to send a message to Ms. Wiggins without anyone else (student OR teacher) reading it, how can I do that?

  - Students may respond in the following ways and the following responses should be given:
  - Text Message - What if someone sees her phone and reads her messages?
  - Email - If it is accidentally left open, someone could read it!
  - Note - What if it is left somewhere and someone gets a hold of it?

- Here is an idea! What if we wrote the message in such a way that even if someone saw it, they simply would not understand it. That is the general idea of cryptography.
- Now, let's think. How many letters are there in our alphabet? (26)
- Write the alphabet in large letters on the board. (To save time - this can be done prior to the beginning of class.) Label the alphabet original.
- Today we are going to learn what is called a "shift cipher". Here's the trick - we will take the alphabet and shift every letter a certain number of places to the left or right. For example, if we shifted the alphabet two places to the right, an "a" would be in the "c" spot, a "b" would be in the "d" spot ***Write the new (shifted) alphabet underneath while doing this- explain that when we get to the end of the alphabet, we must wrap around back to the beginning. Label the new alphabet as "new".
- Now if we wanted to write the word "APPLE" with our new alphabet, we would have to use a "C" instead of an "A", an "R" instead of a "P" . (By now the kids will have caught on). What would "APPLE" look like in the final product? (CRRNG)
  - CRRNG = APPLE
- If I wanted to tell Mrs. Wiggins that "I would like an apple." I might send her a message that says "I would like a crrng." This way if someone saw the message, they

would not understand. It would be even better if we translated the whole sentence. At your seats, please translate the sentence: "I would like an apple."

- The original and new alphabets we have created are often seen in circular form. Today, you will each create your own wheel so that you can easily shift the alphabet however many places you'd like in whatever direction you would like. Pass out cardstock and assist students with making shift cipher wheels. The attached cipher wheel model was taken from the following website: http://tutorialsoneverything.blogspot.com/2011/05/cryptology-substitution-and-shift.html.

- When the students finish their wheels, ask them to come up and receive the following worksheets.

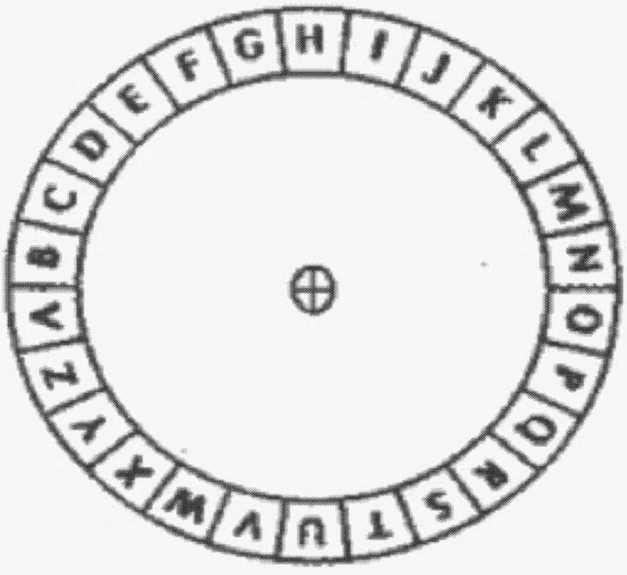
- For homework: The shift cipher has another name. Find out the other name for a shift cipher and where this name comes from.

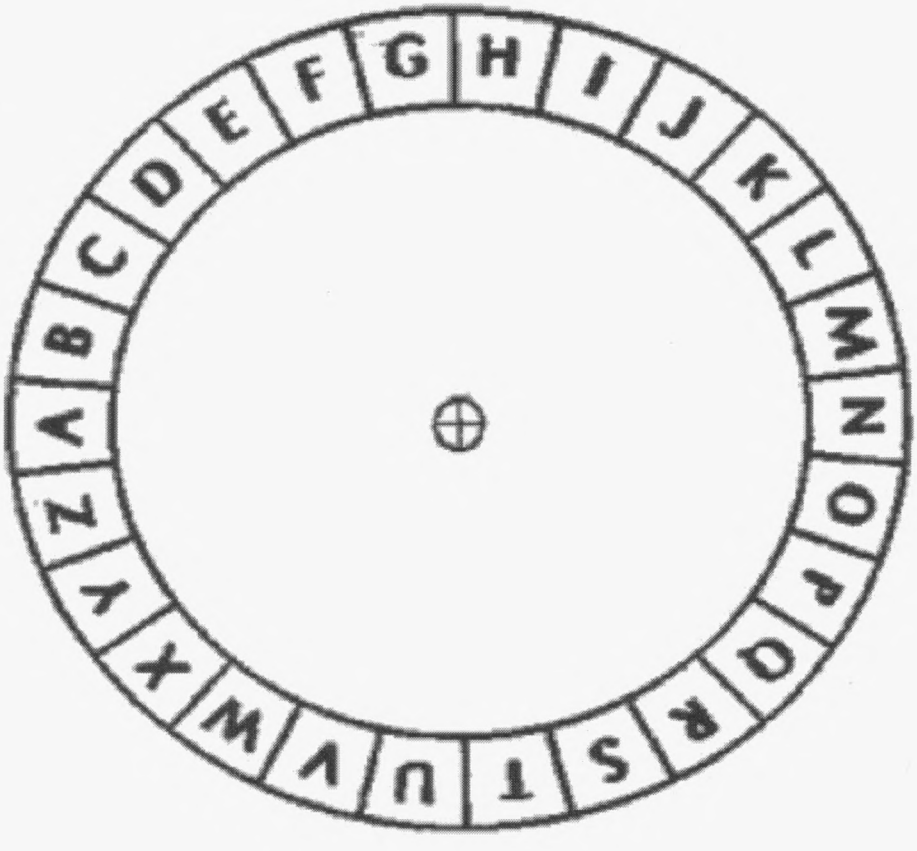
Extension:

For the more advanced students, here are some possible follow-up questions:

a) What is the total number of ciphers that can be created with shift cipher wheels?

b) What is the total number of ciphers that can be created with the letters of the English alphabet?


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name _____ Date_____

Shift Cipher Worksheet

1. After shifting your alphabet 5 spaces to the right, rewrite the phrase:

FRANKLIN SCHOOL IS THE BEST

2. Shift your alphabet 22 spaces to the right. Rewrite the phrase:

LETS GO YANKEES

3. If you were to shift the alphabet 22 spaces to the right, how can we arrive at the same letters by moving to the left?

4. The following message was created by shifting the alphabet 21 places to the right, or five places to the left. Find the original message. (Hint: Start from the inside of your wheel.)

ADIY EVHZN WJIY

5. The following message was created by shifting the alphabet 4 places to the right. How many left could it also be shifted? Find the original message.

XS KIX XS XLI SXLIV WMHI

6 Concluding Remarks

The two cryptosystems found in this thesis use simple applications of number theory including the Knapsack Problem and superincreasing sequences. Both cryptosystems require that the message be of binary nature but by our concept of generalized superincreasing sequences, these systems can be adapted to messages of a non-binary system. The security of the second version of our cryptosystem lies in the hidden, shared key. The key is made in a unique way so that even if a third party intercepted one number in the sequence, they would not know how to find the others as it is hidden in the Fibonacci subsequence. However, future research could be done to further examine the security and complexity of the system. This project also found several interesting properties of the Fibonacci sequence which are used in the development in the cryptosystem. It is natural to consider similar sequences for the same purpose. In fact, a sequence that is defined with the same recursive pattern as the Fibonacci sequence can be created using any random pair of starting numbers. Any nonconsecutive subsequence of this new sequence may also be superincreasing. Future work can elaborate on this idea and explore the nature of Lucas sequence in order to incorporate it into the cryptosystem.

References

[1] Anshel, Iris., Michael Anshel, Dorian Goldfeld. "An Algebraic Method for Public-Key Cryptography," Mathematical Research Letters. 6. 1999.

[2] Bartholdi, John J., "The Knapsack Problem," Georgia Institute of Technology. 2008.

[3] Dudley, Underwood. "A Guide to Elementary Number Theory," Mathematical Association of America. 2009.

[4] Hoffstein, J., Pipher, J., Silverman, J.H.. "An Introduction to Mathematical Cryptography," Springer. 2010.

[5] Koblitz, Neal. "A Course in Number Theory and Cryptography," Springer-Verlag, 1987.

[6] Luma, A., Raufi, B. "Relationship between Fibonacci and Lucas Sequences and Their Application in Symmetric Cryptosystems," Latest Trends on Circuits, Systems and Signals, 2010.

[7] Matousesk, Radomil. "Knapsack Cipher and Cryptanalyst Using Heuristic Methods," Institute of Automation and Computer Science, Brno University of Technology, —.

[8] Menezes, A., Vanstone, S., "Elliptic Curve Cryptosystems and Their Implementation," Journal of Cryptology, 1993.

[9] Paterson, Kenneth G. "Cryptography from Pairings: A Snapshot of Current Research," Information Security Group, University of London. November, 2002.

[10] Raphael, A. Joseph, Sundaram, Dr. V., "Secured Communication through Fibonacci Numbers and Unicode Symbols," International Journal of Scientific and Engineering Research, Vol. 3, Iss.4, April, 2012.

[11] Rosen, Kenneth H. "Elementary Number Theory ans its applications," Pearson. 2005.

[12] Singh, Thokchom Chhatrajit. "Lucas Numbers and Cryptography," Master's Thesis, National Institute of Technology Rourkela. 2012

[13] Weiss, Edwin. "Algebraic Number Theory," McGraw Hill. 1963.

7 Appendix

A A Cryptosystem Algorithm Using Sage

```
print 'Enter "n" (the message space). The following will check the necessary conditions
n=4
p1= int(2^(10*n-7)/sqrt(5))
#print p1
p2=p1+2^33 #Makes p sufficiently large
p = next_prime(p2)
print 'Our prime is', p
h=int(log (sqrt(5)*p,2)-10*n+9)
print 'Enter a g value greater than 1 but less than or equal to', h
g=2.0
a=7
k=11
print 'Check to see if p divides g: p/g = ',(p/g)
print 'Check to see if a and p-1 are relatively prime: gcd(a,p-1)=', gcd(a,p-1)
print 'Check to see if k and p-1 are relatively prime: gcd(k,p-1)=', gcd(k,p-1)
A=mod(g^a,p)
print 'Alice sends to Bob A=g^a mod p, A=', A
print 'Bob: Enter plaintext message x in the next box and hit "evaluate" '
#######################################################
x=vector([1,0,1,1])
print 'Encryption Process:'
K=mod(A^k,p)
print 'K=', K
u=int((log(sqrt(5)*p,2)-g-1)/(n-1))
```

```
print 'u=',u
if K < u:
        print 'Case 1: K < u'
        K=int(K)
        r=vector([])
        for i in range(0,n):
            r=vector(list(r) + list(vector([fibonacci(g+i*K)])))
        print r
        print 'Dot product of r and x', r.dot_product(x)
        c1=mod(g^k,p)
        c2=mod(A^k*(x*r),p)
        print c1
        print c2
        C =mod((c1^(a))^-1*c2,p)
        print C
else:
    print 'Case 2: K >= u'
    K=int(K)
    w=int(K/u)+1
    v=int(K/w)
    r=vector([])
    for i in range(0,n):
        r=vector(list(r) + list(vector([fibonacci(g+i*K)])))
    print 'The superincreasing sequence r is', r
    m=r.dot_product(x)
    c1=mod(g^k,p)
```

```
c2=mod(A^k*m,p)
print 'c_1=',c1
print 'c_2=',c2
C =mod((c1^(a))^-1*c2,p)
print 'Alice now needs to solve the Knapsack Problem with (r, C)'
print 'r=',r
print 'C=', C
```

B Lesson Plan 2: How to Sound Like a Secret Agent

Grade: 6

Time: One 45 Minute Class Period

Materials:

- Paper
- Pencil
- Attached Substitution Keys

Goal:

• Students will be introduced to the important terminology often used in cryptography.

•They will understand the difference between a substitution cipher and a shift cipher.

Objectives:

• Students will use correct vocabulary when working with cryptography.

• Students will encrypt and decrypt messages using a substitution cipher.

Standards Addressed:

-Math Common Core: 5.OA.3, 4.OA.5

-NJCCCS Science: 5.1.4.A..2, 5.1.4.A.3, 5.1.4.B.2 .

Procedure/ Lesson:

- As a warm-up, ask the students to report on what they found as the alternate name for a shift cipher and why. They should respond with the name "Caesar Cipher" as Julius Caesar used the method to communicate with his troops.
- Ask one student to stand and give just a summary of what went on in the "Shift Cipher Shenanigans" lesson. This will be helpful for any student that was absent but it is also important for the students to be able to reflect back on that lesson.
- Important ideas to be sure are covered:
  - Wheel
  - "original alphabet" and "new alphabet"
  - Apple = crrng
- We are going to learn the technical terms used in cryptology. We will sound like complete secret agents after today! (as a new word is introduced, write it on the board)
- Let's start with the term plaintext message. Last week, when we took "apple" and turned it into "crrng", "apple" was the word we were trying to secretly send. The plaintext message is the original word that you want to send.
  - The "crrng" is what we call the ciphertext. It is the message after it has been hidden.
  - What is another example of a plaintext message and a ciphertext that we worked with last week?

- The process that took "apple" and made it "crrng" is what we call encryption. It is the process of encoding or hiding a message.
- If we were to take the ciphertext, and decode it or unjumble it, that is what we call decryption.
  - Summary: APPLE $\rightarrow$ CRRNG = ENCRYPTION
  - CRRNG $\rightarrow$ APPLE = DECRYPTION
- The wheel that we used to encrypt and decrypt certain words and messages is called a key. If the key is known by many others, it is considered to be a public key. If the key is a secret, it is called a private key.
- At this point, ask the students to recap and name the terms just discussed.
  - What do you call the process of hiding a message? (encryption)
  - What do you call the message after it is hidden? (ciphertext)
  - What do you call the tool used to code or decode a message? (key)
  - What do you call the process of uncovering a message after it has been hidden? (decryption)
  - What do you call a message that you would like send in a secret manner? (plaintext message)
- Tell the students that from now on, we will use these terms in the classroom when working on cryptography related work.
- Display a summary of the vocabulary words on the smart board for the students to reference throughout the rest of the lesson.

- OKAY! Let's go back to sending secret messages. Last week, we encrypted messages by shifting the alphabet a certain number of spaces. Those keys that we created are great but they could be predictable. Once someone realizes the pattern, they can uncover the entire message!

- There is another method that is even safer than the shift cipher. This cipher is called the substitution cipher. The substitution cipher is used in the same way but there is no pattern to the key. Let's look at the following example:
  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
  Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

- What you will notice is that the bottom row, the row used for decryption, does not have any particular pattern to it. Therefore, using a substitution cipher is secure because if someone discovers one letter, they do not necessarily know any others.

- Use this key to decrypt the following message:
  DOLL H. SGCTL ZXKZSTL (MISS P. LOVES TURTLES)

- Now we are going to play a game and act like secret agents.

  - Group the students into heterogeneous teams of 3. They should sit (or stand) in a row and they will need a pencil. Every Player 1 will receive a copy of the public key. Players 2 and 3 will each get their own copy of another substitution key.

  - Each Player 1 will receive an encrypted message. They should decrypt the message and pass it on to Player 2. This should be done quietly, as every Player 1 will receive the same message. All Player 2's will have different substitution keys. It is their job to then encrypt the message again after receiving it from Player 1. Once encrypted, they are to pass the ciphertext to Player 3 (who's keys will match Player 2's) to decrypt it. The team of three to get passed through all three

steps correctly wins! Note: it will be easy to tell if the message is correct as it will be the same message that was originally given to Player 1. It will simply be encrypted and decrypted again using a different key.

- Attached is the original message for Player1, and 7 different substitution keys. Each key should have two copies, one for Player 2 and one for Player 3.
- At the end of the game, each Player 2 will have a different encryption of the same message! The students will see that any message can be encrypted and many different ways.

Original Encrypted Message to be given to Player 1 for decryption: They are to use the substitution key above which will be displayed on the board. ZIT JXOEA WKGVF YGB PXDHTR GCTK ZIT SQMN RGU

(THE QUICK BROWN FOX JUMPED OVER THE LAZY DOG)

Below are Keys to be copied and given to Players 2 and 3:

Key 1:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

H I Y T U R P O E W Q A S L K J G D F B N V M C Z X

Key 2:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

P O I U Y T R E W Q L K J H G F D S A Z M N B V C X

Key 3:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

M A Q W S Z X D E R F V B G T Y H N J U I K O L P C

Key 4:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

P I Z G O N F R A C E S J V W Y T Q U L K H D M X B

Key 5:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Z X C V B N M L K J H G F D S A Q W E R T Y U I O P

Key 6:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

N B K M L J H G V C S X Z A D F P U O Y I T R E W Q

Key 7:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A L S M D K F J G H Q P W O E I R U T Y Z X C V B N

C Lesson Plan 3: Modeling Modular Arithmetic

Grade: 6

Time: One 45 Minute Class Period

Materials:

- Pencil
- Paper

- Attached Sheets: Warm Up, Classwork 1 and Classwork 2

Goals:

-Students will be exposed to modular arithmetic.

-They will see a whole new exciting way to add, subtract, multiply, etc.

Objectives:

-Students will complete exercises similar to those that I work with in my own research experience.

-They will solve various modular problems with varying levels of difficulty.

Standards Addressed:

-Math Common Core: 6.NS.2, 6.EE.3, 6.EE.4

-NJCCCS Science: 5.1.4.A.3, 5.1.8.A.2, 5.1.4.B.3, 5.1.4.B.3 .

Procedure/ Lesson:

- Begin with the attached warm-up. They should take their time as this activity will get them thinking outside the box. It will cause them to get into thinking in a cyclic manner. Be sure to work slowly through this lesson. It can feel overwhelming to them if it is not done in an understandable manner.

- Explain today's goal: We will learn modular arithmetic which you have all been doing for years without even realizing it. Let's go back to that warm-up.

  - We use a clock to tell time and yet it only involves 12 numbersdoes that mean we can only have maximum 12 hours in a day? What do we do 13,14,15 hours later? Well sure - we wrap around the clock. This type of wrap around idea is what we call modular arithmetic.

  - That being said, what would we do if our clock only had six hours on it, or the numbers 1-6? (Draw the clock.) What would 10:00 look like on this clock? (4:00)
  - What about a 9 hour clock? (Try and see if they know it without drawing it) What would 20 hours later look like if we are starting at the top which would be "9:00"? (2:00)

- Let's ditch the clocks. If it is helpful, we can think of a number line but instead of a straight line let's think of it in the shape of a circle. The number of digits on our clock, or the number of numbers on our new number line is what we call the "modulus". The modulus tells us what to go up to before we begin to wrap around.
  - What would the modulus be on our usual clock? (12)
  - What is the modulus for the days of the week? (In other words, what number of days do we have before we start the week over again?)
  - What is the modulus for the number of seconds in a minute? At what number do we start over?

- Now, let's put our mathematician faces on. (Make a fun face! Try to get the students to do it too!)

- Earlier I asked what 10:00 would look like on a clock with only six digits and we all agreed it would be 4:00. To say this mathematically, we would say "10 mod 6 is congruent to 4" written as

- What about the 9 digit clock? We know it would be modulus 9. How would we say 20 hours later? (20 modulus 9 is congruent to 2 or .)

- One important idea with modular arithmetic is that when we reach our modulus, we consider it to be a 0 since we begin again with 1 after that. In other words, think of

the clock with a 0 in the 12 spot. Something with modulus 14 would have the numbers 0,1,2,3,4,5,6,7,8,9,10,11,12,13. There are still 14 numbers but instead of numbers 1-14 we use 0-13.

- Now have the students try the attached Classwork 1 problems.

- Let's take things up a notch. Modular Arithmetic is sometimes called Remainder Arithmetic. Can you think of any reason why? (More advanced students may arrive at this answer quickly. If they do, ask them to explain.)

- Let's look at some larger numbers. What would 29 mod 3 be? (2) How do we know this?

- Explain that you can certainly make a clock and wrap around a number of times. The other way to think of it is that 27 is a multiple of 3 which means we will work around the clock how many times? (9) Nine times around brings us back to 0. What is left? 29-27= 2. Therefore, the answer is 2. In other words, The remainder is your real answer!

- The normal operations can be performed with modular arithmetic as well. Remember when 2+2=4 back in first grade? Well now youre in 6th and 2+2 can be something else!

- Now try the Classwork 2 Assignment. The numbers are larger but if you get confused just divide and find the remainder!

Warm-Up (May take up to 10-12 minutes) Think through and solve the following problems:

1. The clock strikes midnight. In the extended version of the story, Cinderella must be back home in 36 hours. What time will the clock say when she gets home if she just meets curfew?

2. It is 1:00 in the afternoon. The detective determines that the crime was committed 13 hours ago. What time was it when the bank was robbed?

3. Miss P's turtle named "Yurtle" began a journey across her room. He began at one end of her room at 11:00 am and it took him 7 hours. What time did he reach the other side?

4. The movie began at 3:00 pm. Movie reviews said the movie was 110 minutes long. What time will the movie end?

Classwork Assignment 1

1. If you made a clock with 4 numbers on it, where does 17 hours bring you to? Draw a picture if necessary. What modular expression can you write for this?

2. Can you think of a real life modulus example? Examples would be the 12 hours of a clock or 60 minutes to an hour. We mentioned a few others earlier. Can you come up with any new ones?

3. What would 15 modulus 6 be? Write the modular expression.

4. 23 mod 9 = _____

5. 34 mod 17 = _____ *This one is tricky!

6. 18 mod 5 = _____

7. 19 mod 3 = _____

Classwork Assignment 2 Try these problems on your own! It may help to think about the remainder method!

1. 65 mod 8 = _____ 2. 100 mod 3= _____

3. 97 mod 4 = _____ 4. 38 mod 5 = _____

5. 99 mod 30 = _____ 6. 56 mod 6 =_____

7. In ordinary arithmetic, 8 7 = _____ which is _____ modulus 5.

8. In ordinary arithmetic, 9 10 = _____ which is _____ modulus 3.

9. In ordinary arithmetic, 8 + 73 = _____ which is_____ modulus 4.

10. In ordinary arithmetic, 14 + 30 = _____ which is _____ modulus 16.