Using Classical Ciphers in Secondary Mathematics

THESIS

Presented to the Honors Committee of

McMurry University

In partial fulfillment of the requirements for

Undergraduate Departmental Honors

in Mathematics

By

Rigoberto G. Castaneda

Abilene, Texas

May 2009

Using Classical Ciphers in Secondary Mathematics

APPROVED:

Dr. Kelly McCoun
Thesis Director

_____
Dr. Kelly McCoun (Mathematics)

_____
Dr. Kathryn Flores (Mathematics)

_____
Melody Roper (Education)

Honors Committee Members

_____
Dr. Gary Wilson, **Dean of SNCS**

_____
Dr. Beverly Lenoir, **VPAA**

ACKNOWLEDGEMENTS

I would like to gratefully acknowledge the enthusiastic supervision of Dr. Kelly McCoun during this project and throughout my undergraduate work. Because of his persistence and dedication to all students, I was able to develop a passion and deep understanding of mathematics. I thank my committee members, Dr. Kathryn Flores and Ms. Melody Roper, for all their help throughout my undergraduate work and their keen eye when reviewing my thesis. To the entire McMurry mathematics faculty and School of Education, thank you for your willingness and commitment to help all students. I also want thank my family for all their support and encouragement. Without their love, support, and encouragement I would not have been able to accomplish all my academic successes. Finally, I am forever indebted to my wife, Lacey, for keeping me motivated and giving me so much love and support throughout my academic career, especially during my final semester at McMurry University.

ABSTRACT

The purpose of this thesis is to give a brief history of cryptology and to show how to incorporate cryptology into secondary mathematics by introducing some of the mathematics used in the making and breaking of codes, with applications to classical ciphers, specifically, the Caesar Cipher, Affine Cipher, and Hill Cipher.

Including cryptology into secondary mathematics encourages the use of problem solving skills, reinforces the concept of a function, function notation, inverse functions, modular arithmetic, and matrix operations. Since everybody is naturally curious about encrypted secret messages and deciphering secret messages, it would be ideal to use cryptology to help enforce and utilize some of the core topics in secondary mathematics. So brace yourself while we explore the world of secrets, deceit, espionage … cryptology.

Table of Contents

1. A Brief History of Classical Ciphers 1

2. Shift Cipher 13

3. Affine Cipher 17

4. Hill Cipher 31

APPENDIX A 35

APPENDIX B 40

BIBLIOGRAPHY 45

CURRICULUM VITAE 46

Chapter 1

A Brief History of Classical Ciphers

What is the first thing that comes to mind when you hear the word cryptology? If your answer is along the lines of secret messages and code breaking then you are on the right track. To begin, let us first define and look at the word *cryptology* in detail. Derived from the Greek word *kryptós*, meaning "secret or hidden" and either the word *logós*, meaning "word," or *ology*, meaning "science" [Wrixon], cryptology is the science of secret writing, covering both cryptography and cryptanalysis [Singh].

With the general knowledge of what cryptology is, let us take a look at a brief history of cryptology and some of the outcomes in history resulting from this fascinating science and how it is used today.

It can be argued that the use of cryptology can be dated back thousands of years to the ancient Egyptians. Although not a true form of cryptography, Egyptian priests and scribes would use modified hieroglyphs, instead of the standard symbols, to transcribe religious text and to mark the tombs of pharaohs. Doing this added a sense of mystique and secrecy to the text which they were transcribing. The common Egyptian population was therefore dependent upon the priest and scribes for translation and interpretation of the modified hieroglyphs. As previously stated, the Egyptian use of modified hieroglyphs was not a true form of cryptography for what they did was merely transform (modify) their writing style without the intention of hiding the text [Barr, Wrixon]. As time went by, the transformations of the hieroglyphs became more and more complicated and the interest of their meaning soon died out.

One of the earliest recorded uses of cryptography, during war-time, was around the fifth century B.C. by the Spartans. Using a cryptosystem called a *scytale* (pronounced sí-ta-lee); the Spartan military would encipher and decipher military plans. The scytale consisted of a wooden cylinder or an officer's baton around which a strip of cloth, leather, or papyrus was tightly wrapped. The plaintext was then written on the strip down the length of the staff [Wrixon]. The strip was then removed from the cylinder and being a strip of leather with a jumble of letters; a messenger would wear it as a belt and carry it to the intended recipient. The recipient would then wrap the strip around his scytale, which was similar in diameter to the senders, and could therefore decipher the message.

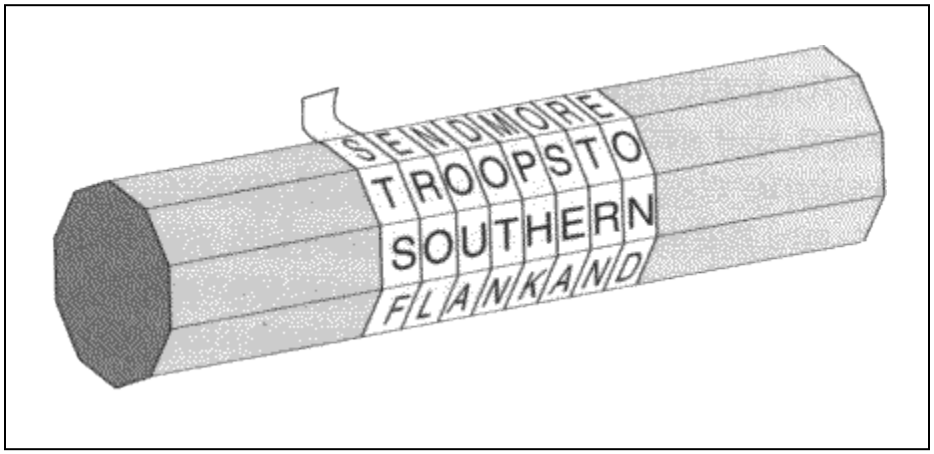
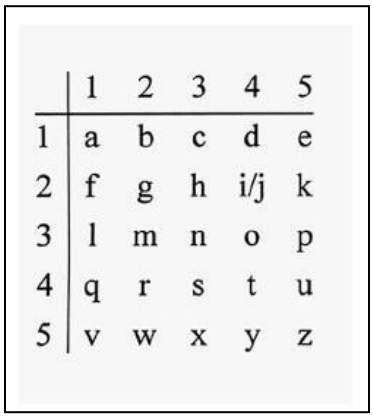


Figure 1.1 Spartan Scytale

Two centuries after the introduction of the scytale, a Greek historian Polybius introduced a cryptosystem known today as the *Polybius cipher* or *Polybius checkerboard*. This was a form of substitution cipher that substituted two digits for every plaintext letter. The Polybius cipher consisted of a 5x5 grid that was filled in with the twenty-four letter Greek alphabet. A commonly used adaptation of the Polybius cipher uses the Roman alphabet and combines the letters I and J into the same cell. The alphabet is prearranged within the twenty-five cells and the rows and columns are numbered from one through five.



	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Figure 1.2 Polybius Checkerboard

The first digit is the row in which the letter appears, and the second digit is the column in which it appears [Barr 5]. For example, using figure 1.2, 33 substitutes for the letter *n*, and *Polybius* is represented by 3534315412244543. As simple as this cryptosystem may seem, the Germans used the principle behind the Polybius cipher, during World War I, to develop a more complex cryptosystem, the *ADFGX cipher*, which will be discussed later.

During his successful military campaigns in the first century B.C., Julius Caesar documented, in his text *Gallic Wars*, a method of encipherment which is known today as the *Caesar cipher*. The Caesar cipher is a very simple shift-cipher achieved by shifting the alphabet forward three letters so that the letter A is enciphered as D, B as E, and so on. The last three letters X, Y, and Z would wrap around and encipher as A, B, and C respectively [Flannery 79]. While the three-shift Caesar cipher is very common, it is possible to use any shift between one and twenty-five generating twenty-five distinct ciphers.

Plaintext	A	B	C	D	…	W	X	Y	Z
Cipher text	D	E	F	G	…	Z	A	B	C

Figure 1.3 Caesar Cipher

After the fall of the Roman Empire, third century A.D., and before the rise of Islam, seventh century A.D., the study and progress of cryptology seemed to stop. Following this drought in cytological development and starting from eighth century onward, Arab scholars began to experiment with solving ciphers without the aid of a key. This practice of code breaking pioneered by the Arabs is known as *cryptanalysis*. In 1412, al-Kalka-shandi published a treatise in which he introduced a technique for solving a substitution cipher based on the relative frequency of letters in the language. The technique is to write down all the cipher text letters and to count the frequency of each symbol. By using the relative frequency of each letter and by trial and error, the plaintext can be written out. Frequency analysis exploits the fact that certain letters and combinations of letters occur with varying frequencies. For example, in most English books, the letter *E* tends to be very common, accounting for roughly 13% of the letters. Likewise, the letters *Q* and *Z* occur very rarely and account for less than 1% of the letters in most texts.

During the Middle Ages, the interest and use of cryptography began to progress. The first major advances following the resurrection of cryptography were made in Italy. In the fifteenth century, Italian Renaissance artist/scholar Leon Battista Alberti, known as "The Father of Western Cryptology," developed and used the first polyalphabetic substitution cipher, known as *Alberti's Disc*. His original design consisted of two copper discs, one smaller and inside a larger outer disc. The smaller inner disc, which becomes the ciphertext, was movable and was inscribed with randomly placed capitalized letters. The larger outer disc, the plaintext, was inscribed with twenty lower case letters (omitting h, j, k, u, w, and y) and numerals one to four [Wrixon]. To start enciphering, a predetermined letter on the inner disk is lined up with any letter on the outer disk, which is written as the first character of the ciphertext. After a few words of ciphertext, the disks are rotated so that the index letter on the inner disk is aligned with a new letter on the outer

disk, and in this manner, the message is enciphered. By rotating the disk every few words, the cipher changed enough to limit the effectiveness of frequency analysis [Cohen]. Unfortunately, Alberti failed to develop his concept in a fully formed cryptosystem.

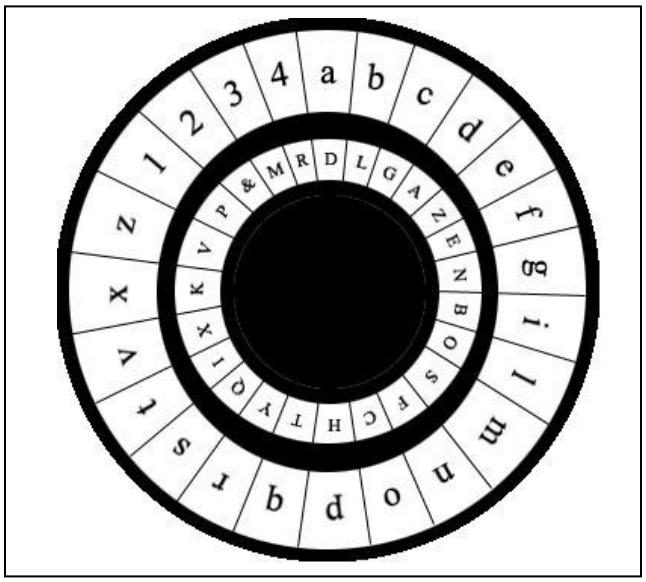


Figure 1.5 Alberti's Disc

In 1452, the Italians created an organization with the sole purpose of dealing with cryptology. This organization known as a *black chamber* consisted of three secretaries that solved and created various cryptosystems and gathered intelligence. As time progressed, cryptanalysis was becoming more widespread and by the 1700's each European power had its own black chamber [Singh]. One of the most celebrated and recognized black chamber's was the Geheime Kabinets-Kanzlei in Vienna. This Austrian organization was very disciplined and efficient and operated a very rigorous schedule. They would read through all the mail coming to foreign embassies, copy the letters, reseal them, and return them to the post-office the same morning as to not interrupt the postal service. Any encrypted letters that were copied were passed to cryptanalyst for decryption. Each day the Viennese Black Chamber would filter through hundreds of letters to include any other political or military interceptions they may come across.

Although not as efficient or rigorous, the process used by the Viennese Black Chamber was the standard for the various European black chambers.

Before letter frequency analysis and the formation of the black chambers, the basic monoalphabetic substitution ciphers were practically unbreakable and sufficient for common use. But as encryption became used more widely, the need to break these cryptosystems became inevitable. With the development of letter frequency analysis and advancement of black chambers, each message encrypted with a type of monoalphabetic substitution was easily broken. As soon as a commonly used monoalphabetic substitution cipher was broken, the word spread and that particular cryptosystem was useless. Cryptographers would then attempt to make a stronger cryptosystem but again would fail at keeping it secure and unbreakable. And so the war between cryptographers and cryptanalyst had begun. What cryptographers failed to realize was that their newly invented cryptosystems were mere variations of the simple monoalphabetic substitution ciphers which are easily broken by cryptanalysis using letter frequencies.

Although hitting upon a very significant breakthrough in encryption (as mentioned earlier), Alberti failed to form his polyalphabetic cryptosystem into a fully functional system. Instead, Alberti's idea was expanded on by a diverse group of intellectuals [Singh]. First by the German abbot, Johannes Trithemius, who proposed the *tabula recta* in 1518, in his fifth volume of *Polygraphiae Libri Sex (Six Books of Polygraphy),* which is a square table of alphabets where each row is made by shifting the previous row to the left one position [Wrixon]. Next to experiment with Alberti's work was an Italian scientist Giovanni Porta who developed a disc system similar to Alberti's where the difference was using special characters, instead of the alphabet, for the ciphertext. Porta also developed a system known as *Porta's Digraphic Cipher* which was a table that used special non-repeated symbols to represent pairs of letters.

Finally, a French diplomat, Blaise de Vigenère, examined and used the works of Alberti, Trithemius, and Porta to develop a coherent and very powerful new cryptosystem which came to be known as *le chiffre indéchiffrable* (the indecipherable cipher).

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

Fig 1.6 Vigenère Square

In 1586, Vigenère published his treatise *Traicté des Chiffres* which discussed his polyalphabetic cipher system that used twenty-six distinct cipher alphabets and a keyword or phrase to encrypt a message [Singh, Wrixon]. In the 1500's, the *Vigenère cipher* was invulnerable to letter frequency analysis and had an enormous number of keys since the key could be any word, combination of words, or a string of letters. Having such an astronomical number of keys made it impossible for cryptanalyst to crack the message by searching all possible keys. Being such a powerful and secure system, it would appear that the Vigenère cipher would become the premiere form of encryption used by European powerhouses. Unfortunately it was not used since it consisted of several alphabets which made it difficult, for some, and complicated to use [Singh].

As a result, the Vigenère cipher was ignored for a few decades and remained unbreakable until the eighteen hundreds where it was broken by Charles Babbage in 1854 and a published attack strategy by Friedrich Kasiski in 1863.

Although most of the major contributions to cryptology were made in the European continent, there were some cryptographic advances in United States of America. In the 1790's Thomas Jefferson developed a mechanical device known as a wheel cipher. Jefferson's design was a wooden cylinder two inches in diameter and six inches long. It held thirty-six removable wheels each one-sixth of an inch thick with twenty-six randomly inscribed letters on the outside edge of each wheel. Each wheel was numbered and the order in which the wheels were assembled was agreed upon by the correspondents. Each message had to be encrypted thirty-six letters at a time since there were only thirty-six wheels on the device. After the sequence of the wheels was determined the message would be aligned one letter at a time. Once the massage was completely aligned the sender would select one of the twenty-five remaining parallel rows of letters as the ciphertext. In essence, the message was encrypted twenty-five times and the sender selected any encrypted row [Barr, Wrixon]. To decipher the message, the receiver aligned the cipher text, considering the recipient had the correct wheel order, and searched the remaining twenty-five rows of letters for the plaintext.

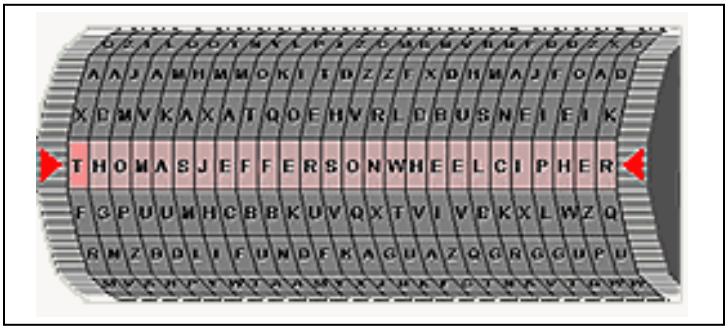


Figure 1.7 Jefferson Wheel Cipher

In 1854 Charles Wheatstone developed a system in which pairs of letters (digraphs) are encrypted in a 5x5 alphabet matrix with their arrangement set by a variable keyword. The keyword, containing no repeated letters, is written horizontally from left to right. The unused letters of the alphabet are entered in the remaining cells of the matrix in alphabetical order, with the letter 'I' and 'J' combined in the same cell. To encrypt, the plaintext is divided into two letter groups and if double letters occur in a pair, an 'X' is used to separate them. If there is an odd number of letters, an 'X' is also used to complete a pair of letters [Wrixon]. To encrypt the message one must follow a set of rules:

1. If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
2. If the letters appear on the same column of the table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
3. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter. [Wikipedia]

To decrypt the message all one needs to do is follow the given steps in reverse assuming the correct keyword is possessed. Although Wheatstone invented this system, it is commonly called the Playfair cipher because it was popularized and promoted by Baron Lyon Playfair, a friend of Wheatstone's. Because of its fairly easy use, the Playfair cipher was used and adopted by British forces in the Boer War and World War I [Barr].

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

Figure 1.8 Playfair Cipher w/ Keyword: CRYPTOLOGY

In 1918, during World War I, the Germans adopted the *ADFGVX cipher*. They believed that this system was very secure and unbreakable. But a few months after its introduction to WWI the ADFGVX cipher was broken by French cryptanalyst Georges Painvin. This cipher system, invented by German Colonel Fritz Nebel, was a combination of substitution and transposition ciphers [Barr]. It was built on the principles of the Polybius checkerboard, as previously stated, and the Spartan Scytale. The ADFGVX cipher is a 6x6 table with the letters ADFGVX as the vertical and horizontal coordinates and contains twenty-six letters and ten numerals inside the table. The first step of encryption is locating each plaintext letter within the table and replacing it with the coordinate pair with the vertical ADFGVX coordinate as the first letter and the horizontal ADFGVX as the second letter of the encrypted pair. The encrypted letters are then written from left to right in successive rows according to a keyword which indicates the number of columns. The next step involves transposition of the ciphertext from the first step. Finally, the columns are taken in blocks of five according to the alphabetic order of the letters in the keyword [Wrixon].

Throughout the duration of World War I there was a large increase of new cipher systems being developed, but the weakness of these new ciphers was that they were variations or combinations of previously broken ciphers. Although these systems provided some security initially, they were soon cracked by cryptanalyst. The need for secrecy of military plans and government communications was extremely desired if any war was to be won. As a result, governments needed and employed cryptographers to develop unbreakable cryptosystems. The previously discussed systems were sufficient for their time, but as we have seen, they were soon broken and became obsolete. For modern times, the "classical ciphers" are not adequate. The development of technology and the dire need for secrecy made the modern advancement of cryptology inevitable. Cryptosystems were now being integrated into modern technology making the cryptanalysis of these modern cryptosystems near if not impossible to impenetrate.

One of the first technological breakthroughs was the development of the *Enigma* by a German engineer Arthur Scherbius. This machine was initially used by commercial vendors but was soon adopted by the German military and used during World War II. The Enigma was extremely secure using rotors, scramblers, and plugboards to make it near impossible to crack. It had an astronomical amount of keys making it harder for cryptanalyst to use a "brute force method." Eventually the Enigma was cracked due to espionage, carelessness of the Enigma operators, and the genius of Alan Turing. Large devices such as *Bombes* and *The Colossus* were developed to assist in breaking the developing Enigma. If not for the work of the Bletchley Park in cracking the Enigma, it can be argued the Allies would have not been able to win World War II.

Figure 1.9 German Enigma

Today cryptography is still used to conceal military and government plans. It is also used to secure purchases made online and bank transactions that are made every day. The advent of computers made it possible to secure information efficiently. The security of the *RSA cipher* relies on the fact that it is currently very time consuming, using known factoring algorithms to factor a large composite number (200 digits or more) into primes. As time continues and technology increases, computer based cryptosystems will become stronger and cryptanalyst will have the obligation of cracking the code, keeping the long time battle between cryptographers and cryptanalyst alive and well.

Cryptology has definitely evolved from its primitive form from centuries ago. Every developed cryptosystem was a temporary secure means of communication but was subject to cryptanalysis which eventually made it obsolete. Cryptographers have fought to preserve secrecy while their counterpart, cryptanalyst, fought to reveal it. The battle between cryptographers and cryptanalyst will continue as new systems are developed. The need for secrecy of information is like humans needing air. It is essential for governments to protect the security of its people by keeping certain information encrypted and secure from foreign governments and terrorists looking for a weakness to strike. Even the most seemingly secure cryptosystems may have their weakness. When will the "ultimate" unbreakable cryptosystem be developed?

Chapter 2

Shift Cipher

In cryptography, a shift cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3 (commonly known as the Caesar Cipher), A would be replaced by D, B would become E, and so on. This transformation can be represented by aligning the plaintext alphabet on top of the ciphertext alphabet as shown in figure 2.1.

Plain-text	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
Cipher-text	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

Figure 2.1 Caesar Cipher

The ciphertext alphabet is simply the plaintext alphabet shifted left or right by some number of units. To encipher a message, simply look up each letter of the message in the "plaintext" alphabet and write down the corresponding letter from the "ciphertext" alphabet. To decipher, do the reverse. For instance, using the Caesar Cipher from figure 2.1, the word, *CAESAR*, enciphers to *FDHVDU*.

The shift cipher can be implemented mathematically, specifically, using modular arithmetic. The first step is to assign an integer to each letter of the plaintext alphabet, beginning with 0 and ending with 25.

The integers corresponding to the twenty-six letter plaintext alphabet are

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2.1

Every cipher in cryptography has a *key* which gives the ability to encipher and decipher a message. For the Shift Cipher, the key, *k*, is an integer between 1 and 25, with zero being excluded since no shift in the plaintext will occur with a key of zero.

After assigning the appropriate integer, *x*, to a particular plaintext letter of the message, per table 2.1, the Shift Cipher is implemented mathematically by adding the key, *k*, to *x* modulo 26, effectively shifting the plaintext letter *k* units to the right. Therefore, the aforementioned process can be represented mathematically by

$$y = (x + k) \bmod 26$$

and using function notation, we have,

$$f(x) = (x + k) \bmod 26.$$

Finally, after applying our encryption function to each plaintext letters' corresponding integer, per table 2.1, we simply look up the resulting integers in table 2.1 to get our ciphertext.

Using the previous example, the Caesar Cipher is a Shift Cipher that uses a key of three, $k = 3$. Applying our encryption function to encrypt *CAESAR* we obtain,

Plaintext	C	A	E	S	A	R
x	2	0	4	18	0	17
f(x) =(x+3) mod 26	5	3	7	21	3	20
Ciphertext	F	D	H	V	D	U

Table 2.2 Encryption

Naturally, we do not have to shift by 3, exclusively, as Caesar did. As mentioned earlier, we can choose our key to be a number between 1 and 25, thus giving us 25 distinct ciphers.

Decryption of the ciphertext obtained by using the Shift Cipher encryption function can be accomplished similar to the encryption process. But first we must find a way of reversing our steps. Since our encryption algorithm is in the form of a function, we can use the steps, learned in algebra, to find the inverse function.

1. Replace $f(x)$ with y.

$$y = (x + k) \bmod 26$$

2. Interchange the x and y.

$$x = (y + k) \bmod 26$$

3. Solve the equation for y.

$$y = (x - k) \bmod 26$$

4. Replace y with $f^{-1}(x)$.

$$f^{-1}(x) = (x - k) \bmod 26$$

Therefore, the Shift Cipher decryption function is

$$f^{-1}(x) = (x - k) \bmod 26$$

Using the derived decryption function for the Shift Cipher, let us decipher the ciphertext, FDHVDU, from the previous example to ensure we get the correct plaintext. Since our plaintext was encrypted using the Caesar Cipher, we know the key is 3. To decrypt the ciphertext we use the same steps used to find the integer equivalent of each ciphertext letter per table 2.1, apply the decryption function to each resulting integer, and find the corresponding letter to each resulting integer. This decryption process is shown in table 2.3.

Ciphertext	F	D	H	V	D	U
x	5	3	7	21	3	20
$f(x) = (x-3) \bmod 26$	2	0	4	18	0	17
Plaintext	C	A	E	S	A	R

Table 2.3 Decryption

As you may have noticed, Shift Ciphers offer very little security since there are only twenty-five options for the key thus requiring at most twenty-five attempts to crack the code. Due to the small number of keys the Shift Cipher is not used today when trying to secure valuable information. However, the use of Shifts Ciphers in the secondary math classroom is ideal since it gives students the opportunity to use functions and inverse functions in an entertaining and useful way.

Chapter 3

Affine Cipher

As we have seen, Shift Ciphers offer very little security. The problem is that the letter substitutions, or shifts, are not mixed up enough. The idea of an Affine Cipher is to use multiplication combined with addition, modulo *m,* where *m* is an integer, to create a more mixed-up substitution [Barr]. The Affine cipher is simply a special case of the more general monoalphabetic substitution cipher.

The key for the Affine Cipher consists of an ordered pair, say *(a, b).* In selecting the key, it is important to note the following restrictions; $a \neq 0$ and *b* must be chosen from among the integers 0, 1, 2, 3, …, *m*-1 and $a \neq 0$ must be relatively prime to *m* (i.e. *a* should have no factors in common with *m*). For example, assuming we use a 26 character alphabet (i.e. $m = 26$), 15 and 26 have no factors in common and therefore 15 is an acceptable value for *a.* On the other hand, if we chose 12 for the value of *a* it is obvious that 12 would be an unacceptable value since 12 and 26 have common factors, specifically 2.

In General, an Affine Cipher is a cipher system in which plaintext letters are enciphered mathematically by the function,

$$y = (ax + b) \bmod m$$

and using function notation, we have,

$$f(x) = (ax + b) \bmod m$$

where *x* is the numerical equivalent of the plaintext letter and *m* is the number of letters in the alphabet.

Suppose we want to set up correspondence where a message is encrypted with the key (7, 11) and using a twenty-six letter alphabet (i.e. $m = 26$). Substituting our given key and modulus into the Affine Cipher encryption function, we have

$$f(x) = (7x + 11) \bmod 26.$$

Then, using table 2.1, the message, ATTACK, has numerical equivalent

$$0, 19, 19, 0, 2, 10,$$

and to encrypt the plaintext we substitute the integer values into the Affine Cipher encryption function as follows

$$(7*0 + 11) \bmod 26 = 11 \bmod 26 = 11$$

$$(7*19 +11) \bmod 26 = 144 \bmod 26 = 14$$

$$(7*19 +11) \bmod 26 = 144 \bmod 26 = 14$$

$$(7*0 +11) \bmod 26 = 11 \bmod 26 = 11$$

$$(7*2 +11) \bmod 26 = 25 \bmod 26 = 25$$

$$(7*10 +11) \bmod 26 = 81 \bmod 26 = 3,$$

hence, the numerical equivalents of the ciphertext are

$$11, 14, 14, 11, 25, 3.$$

Finally, we translate the encrypted integers back into letters using table 2.1 and get

LOOLZD.

All of the examples presented thus far have been calculated modulo 26, with the numbers 0 thru 25 corresponding to letters A thru Z respectively. When we take into consideration using lower case, upper case, punctuation, and other symbols, more numbers are required. To help us define alphabets other than the standard twenty-six letter upper case alphabet, we will employ shifted ASCII codes, which are numerical values assigned to every character on a computer keyboard, to generate three additional alphabets, specifically, the Mod 29 alphabet, which is formed from the mod 26 alphabet by adding a space, period, and question mark, the Mod 89 alphabet, which are the ASCII codes of a certain 89 characters shifted left 34 units, and the Mod 95 alphabet, which are the ASCII codes shifted left 32 units, (McCoun).

Note: *Each of these additional alphabets are located in Appendix A.*

Decryption of the ciphertext obtained by applying the Affine Cipher encryption function can be accomplished similar to the encryption process. However, as we seen with the Shift Cipher, we must first perform the steps, learned in algebra, to find the inverse function. As we previously stated, the Affine Cipher consists of both multiplication and addition and unlike the Shift Cipher, it is necessary to define the *multiplicative inverse* of an integer *a* modulo *m*.

Definition 3.1 A multiplicative inverse of an integer *a* modulo *m* is an integer *b*, in the range *1* to *m-1*, such that $ab \equiv 1 \bmod m$. When *a* and *m* are relatively prime, such a *b* will exist and we call *b* the multiplicative inverse of *a* and label it a^{-1}(Barr).

Note: *For the purposes of this project, the multiplicative inverses of invertible elements in the alphabets modulo 26, 29, 89, and 95 will be supplied in Appendix B. However, there is a process that can be used to calculate the multiplicative inverse, generally seen in Discrete Mathematics and Number Theory, known as the Euclidean Algorithm.*

With the knowledge of multiplicative inverses, we can now derive the decryption formula for the Affine Cipher.

1. Replace $f(x)$ with y.

$$y = (ax + b) \bmod m$$

2. Interchange the x and y.

$$x = (ay + b) \bmod m$$

3. Solve the equation for y.

$$x - b = ay \bmod m$$

$$a^{-1}(x - b) = a^{-1}ay \bmod m$$

$$a^{-1}(x - b) = y \bmod m$$

$$y = a^{-1}(x - b) \bmod m$$

4. Replace y with $f^{-1}(x)$.

$$f^{-1}(x) = a^{-1}(x - b) \bmod m$$

Therefore, the Affine Cipher decryption function is

$$f^{-1}(x) = a^{-1}(x - b) \bmod m.$$

Using the derived decryption function for the Affine Cipher, let us decipher the ciphertext, LOOLZD, from the previous example to ensure we get the correct plaintext.

Our plaintext was encrypted using a key of *(7, 11,)*, where $a = 7$ and $b = 11$, and therefore we must first find 7^{-1} modulo *26*.

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1} mod 26	1	9	21	15	3	19	7	23	11	5	17	25

Table 3.1 Multiplicative Inverses modulo 26

By table 3.1, $7^{-1} = 15$, so our decryption formula will be

$$f^{-1}(x) = 15(x – 11) \bmod 26.$$

The numerical equivalents of the encrypted message are

11, 14, 14, 11, 25, 3.

Substituting these values for *x* in the derived decryption function we get

$$15(11 – 11) \bmod 26 = 0 \bmod 26 = 0$$

$$15(14 – 11) \bmod 26 = 45 \bmod 26 = 19$$

$$15(14 – 11) \bmod 26 = 45 \bmod 26 = 19$$

$$15(11 – 11) \bmod 26 = 0 \bmod 26 = 0$$

$$15(25 – 11) \bmod 26 = 210 \bmod 26 = 2$$

$$15(3 – 11) \bmod 26 = -120 \bmod 26 = 10$$

Therefore, the numerical equivalents of our calculated plaintext are

0, 19, 19, 0, 2, 10.

Finally, the last step is to translate the decrypted integers back into letters using table 2.1, and get

ATTACK.

Now suppose we want to encrypt a message twice. Suppose we use the mod 95 alphabet in Appendix A, we would then need to select two separate keys, say *(17, 62)* and *(9, 24)*. Substituting our two keys and the selected modulus into the Affine Cipher encryption function, we get two functions *g* and *h* as follows

$$g(x) = 17x + 62 \bmod 95, \text{ and } h(x) = 9x + 24 \bmod 95.$$

Using the same process as the previous example, let us encrypt the message, *Retreat NOW!*, first using function *g* and then *h*. Do note, since we are using a 95 character alphabet, we must take into account using lower and upper case letters, punctuation, and empty spaces. Using Mod 95 Alphabet, in Appendix A, the numerical equivalents of *Retreat NOW!* are

50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1

and encrypting the message by first using *g* we get

$$17*50 + 62 \bmod 95 = 912 \bmod 95 = 57$$

$$17*69 + 62 \bmod 95 = 1235 \bmod 95 = 0$$

$$17*84 + 62 \bmod 95 = 1490 \bmod 95 = 65$$

$$17*82 + 62 \bmod 95 = 1456 \bmod 95 = 31$$

$$17*69 + 62 \bmod 95 = 1235 \bmod 95 = 0$$

$$17*65 + 62 \bmod 95 = 1167 \bmod 95 = 27$$

$$17*84 + 62 \bmod 95 = 1490 \bmod 95 = 65$$

$$17*0 + 62 \bmod 95 = 62 \bmod 95 = 62$$

$$17*46 + 62 \bmod 95 = 844 \bmod 95 = 84$$

$$17*47 + 62 \bmod 95 = 861 \bmod 95 = 6$$

$$17*55 + 62 \bmod 95 = 997 \bmod 95 = 47$$

$$17*1 + 62 \bmod 95 = 79 \bmod 95 = 79$$

hence, the integer values of the encrypted plaintext using *g* are

$$57, 0, 65, 31, 0, 27, 65, 62, 84, 6, 47, 79.$$

For the second encryption, we will use the integer values found using *g* and plug them into *h* as follows

$$9*57 + 24 \bmod 95 = 537 \bmod 95 = 62$$

$$9*0 + 24 \bmod 95 = 24 \bmod 95 = 24$$

$$9*65 + 24 \bmod 95 = 609 \bmod 95 = 39$$

$$9*31 + 24 \bmod 95 = 303 \bmod 95 = 18$$

$$9*0 + 24 \bmod 95 = 24 \bmod 95 = 24$$

$$9*27 + 24 \bmod 95 = 267 \bmod 95 = 77$$

$$9*65 + 24 \bmod 95 = 609 \bmod 95 = 39$$

$$9*62 + 24 \bmod 95 = 582 \bmod 95 = 12$$

$$9*84 + 24 \bmod 95 = 780 \bmod 95 = 20$$

$$9*6 + 24 \bmod 95 = 78 \bmod 95 = 78$$

$$9*47 + 24 \bmod 95 = 447 \bmod 95 = 67$$

$$9*79 + 24 \bmod 95 = 735 \bmod 95 = 70$$

After twice encrypting the plaintext with a key of *(17, 62)* and then with *(9, 24)* we get the integers

62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70.

Finally, we translate the encrypted integers back into letters using the Mod 95 Alphabet in Appendix A and get the following ciphertext

^ 8 G 2 8 m G , 4 n c f

The process of encrypting plaintext multiple times can be lengthy and time consuming. To shorten the process we can use function composition to create one function for encryption. However, before we begin it is important to note that $f(k(x)) \neq k(f(x))$, except for special cases, therefore, we must take caution when performing function composition. As a general rule, take the first encryption function and insert into the second encryption function. In our case take *g* and insert it into *h,* specifically $f(x) = h(g(x))$, as follows

$$9(17x + 62) +24 \bmod 95$$

$$153x +558 + 24 \bmod 95$$

$$153x + 582 \bmod 95$$

Since we are calculating modulo 95, all integer values must be reduced modulo 95.

Hence, our new function composition is

$$f(x) = 58x + 12 \bmod 95.$$

Using our function composition, let us encrypt the same message, *Retreat NOW!*, to show we get the same ciphertext as the process of double encrypting. First, using Mod 95 Alphabet, in Appendix A, the numerical equivalents of *Retreat NOW!* are

50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1

and encrypting using *f* we get

$$58*50 + 12 \bmod 95 = 2912 \bmod 95 = 62$$

$$58*69 + 12 \bmod 95 = 4014 \bmod 95 = 24$$

$$58*84 + 12 \bmod 95 = 4884 \bmod 95 = 39$$

$$58*82 + 12 \bmod 95 = 4768 \bmod 95 = 18$$

$$58*69 + 12 \bmod 95 = 4014 \bmod 95 = 24$$

$$58*65 + 12 \bmod 95 = 3782 \bmod 95 = 77$$

$$58*84 + 12 \bmod 95 = 4884 \bmod 95 = 39$$

$$58*0 + 12 \bmod 95 = 12 \bmod 95 = 12$$

$$58*46 + 12 \bmod 95 = 2680 \bmod 95 = 20$$

$$58*47 + 12 \bmod 95 = 2738 \bmod 95 = 78$$

$$58*55 + 12 \bmod 95 = 3202 \bmod 95 = 67$$

$$58*1 + 12 \bmod 95 = 70 \bmod 95 = 70$$

The resulting integers after applying our composition function are

62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70,

and using Mod 95 Alphabet in Appendix A we can look up the ciphertext, which is

^ 8 G 2 8 m G , 4 n c f

Finally, we can see that we can use function composition in place of using multiple encryption functions which will save time and tedious computations.

Decrypting the previous example can be accomplished by finding and applying $f^{-1}(x)$ to the ciphertext or by finding and applying $h^{-1}(x)$ then $g^{-1}(x)$ to the ciphertext. We will show both processes.

First, we will apply $f^{-1}(x)$ to the ciphertext. Since our plaintext was encrypted using the key $(58, 12)$, where $a = 58$ and $b = 12$, we must find 58^{-1} modulo 95. Using the Multiplicative Inverses modulo 95 table in Appendix B, $58^{-1} = 77$. Substituting 58^{-1} and $b = 12$ into the Affine Cipher decryption function, we get

$$f^{-1}(x) = 77(x – 12) \bmod 95.$$

Now, using the Mod 95 Alphabet in Appendix A, the numerical equivalents of the encrypted message are

$$62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70.$$

Substituting these values for x in the derived decryption function we get

$$77(62 -12) \bmod 95 = 3850 \bmod 95 = 50$$

$$77(24 -12) \bmod 95 = 924 \bmod 95 = 69$$

$$77(39 -12) \bmod 95 = 2079 \bmod 95 = 84$$

$$77(18 -12) \bmod 95 = 462 \bmod 95 = 82$$

$$77(24 -12) \bmod 95 = 924 \bmod 95 = 69$$

$$77(77 -12) \bmod 95 = 5005 \bmod 95 = 65$$

$$77(39 -12) \bmod 95 = 2079 \bmod 95 = 84$$

$$77(12 -12) \bmod 95 = 0 \bmod 95 = 0$$

$$77(20 -12) \bmod 95 = 616 \bmod 95 = 46$$

$$77(78 -12) \bmod 95 = 5082 \bmod 95 = 47$$

$$77(67 -12) \bmod 95 = 4235 \bmod 95 = 55$$

$$77(70 -12) \bmod 95 = 4466 \bmod 95 = 1$$

Therefore, the numerical equivalents of our calculated plaintext are

$$50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1.$$

Finally, the last step is to translate the decrypted integers back into characters using the Mod 95 Alphabet in Appendix A, and get

Retreat NOW!

For our second option, we need to find and apply $h^{-1}(x)$ then $g^{-1}(x)$. For h, our key was $(9, 24)$, where $a = 9$ and $b = 24$, and we must therefore find 9^{-1} modulo 95. Using the Multiplicative Inverses modulo 95 table in Appendix B, $9^{-1} = 74$. Substituting 9^{-1} and $b = 24$ into the Affine Cipher decryption function we get

$$h^{-1}(x) = 74(x – 24) \bmod 95.$$

For *g*, our key was *(17, 62)*, where $a = 17$ and $b = 62$, and we must therefore find 17^{-1} modulo *95*. Using the Multiplicative Inverses modulo 95 table in Appendix B, $17^{-1} = 28$. Substituting 17^{-1} and $b = 62$ into the Affine Cipher decryption function we get

$$g^{-1}(x) = 28(x – 62) \bmod 95$$

Now, using the Mod 95 Alphabet in Appendix A, the numerical equivalents of the encrypted message, *^ 8 G 2 8 m G , 4 n c f* ,are

62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70.

Substituting these values for *x* into h^{-1} first we get

$$74(62 – 24) \bmod 95 = 2812 \bmod 95 = 57$$

$$74(24 – 24) \bmod 95 = 0 \bmod 95 = 0$$

$$74(39 – 24) \bmod 95 = 1110 \bmod 95 = 65$$

$$74(18 – 24) \bmod 95 = -444 \bmod 95 = 31$$

$$74(24 – 24) \bmod 95 = 0 \bmod 95 = 0$$

$$74(77 – 24) \bmod 95 = 3922 \bmod 95 = 27$$

$$74(39 – 24) \bmod 95 = 1110 \bmod 95 = 65$$

$$74(12 – 24) \bmod 95 = -888 \bmod 95 = 62$$

$$74(20 – 24) \bmod 95 = -296 \bmod 95 = 84$$

$$74(78 – 24) \bmod 95 = 3996 \bmod 95 = 6$$

$$74(67 – 24) \bmod 95 = 3182 \bmod 95 = 47$$

$$74(70 – 24) \bmod 95 = 3404 \bmod 95 = 79$$

hence, the integer values from first applying h^{-1} to the ciphertext are

57, 0, 65, 31, 0, 27 65, 62, 84, 6, 47, 79.

Next, we will use the integer values found using h^{-1} and substitute them into g^{-1} as follows

$$28(57 – 62) \bmod 95 = -140 \bmod 95 = 50$$

$$28(0 – 62) \bmod 95 = -1736 \bmod 95 = 69$$

$$28(65 – 62) \bmod 95 = 84 \bmod 95 = 84$$

$$28(31 – 62) \bmod 95 = -868 \bmod 95 = 82$$

$$28(0 – 62) \bmod 95 = -1736 \bmod 95 = 69$$

$$28(27 – 62) \bmod 95 = -980 \bmod 95 = 65$$

$$28(65 – 62) \bmod 95 = 84 \bmod 95 = 84$$

$$28(62 – 62) \bmod 95 = 0 \bmod 95 = 0$$

$$28(84 – 62) \bmod 95 = 616 \bmod 95 = 46$$

$$28(6 – 62) \bmod 95 = -1568 \bmod 95 = 47$$

$$28(47 – 62) \bmod 95 = -420 \bmod 95 = 55$$

$$28(79 – 62) \bmod 95 = 476 \bmod 95 = 1$$

Therefore, the numerical equivalents, after apply h^{-1} and g^{-1}, of our calculated plaintext are

50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1.

Finally, the last step is to translate the decrypted integers back into characters using the Mod 95 Alphabet in Appendix A, and get

Retreat NOW!

We have shown that text encrypted by the composition, $f = h \circ g$, can be decrypted in two ways: first, by finding f^{-1} and applying it to the ciphertext or second, by applying h^{-1} to the ciphertext and then applying g^{-1} to the result. Thus illustrating

$$f^{-1} = (h \circ g)^{-1} = (g^{-1} \circ h^{-1}).$$

As you may have noticed, the Affine Cipher allows for a lot of practice in using functions, finding inverses functions, and composing functions. Using the Affine Cipher in the secondary mathematics classroom will help to enforce function operations.

Chapter 4

Hill Cipher

Introduced in 1929 by Lester Hill, the Hill Cipher is a poly-alphabetic cipher that uses matrices to encode plaintext messages. The key for this cipher system consist of an *n x n* square invertible matrix A, where the larger the dimensions the more secure the encryption will be. To ensure the key matrix A is invertible it is important to note that the determinant of A, *det(A)* , must be relatively prime to the modulus *m*.

The basic idea of the Hill Cipher is to put the letters of the plaintext into blocks of length *n*, assuming an *n x n* key matrix, and then each block of plaintext letters is then converted into a column matrix of integers according to the alphabet chosen and then pre-multiplied by the *n x n* key matrix. The results are then converted back to letters and the ciphertext message is produced. Due to the complexity of working with large matrices, we will stick with using a *2 x 2* matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ that is invertible modulo *26* and where *det(A) =(ad – bc)* mod *26*.

Suppose we want to encrypt the message TROJAN using the key matrix $A = \begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix}$ modulo *26*. The first step is to assign each letter of the plaintext its numerical equivalent, using table 2.1, which are

19, 17, 14, 9, 0, 13.

In the event that the length of the plaintext is not a multiple of the size of the key matrix, random letters can be added to the end of the plaintext.

We then perform matrix multiplication as follows

$$\begin{bmatrix}3 & 7\\ 9 & 10\end{bmatrix}\begin{bmatrix}19\\ 17\end{bmatrix} = \begin{bmatrix}176\\ 341\end{bmatrix} = \begin{bmatrix}20\\ 3\end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix}3 & 7\\ 9 & 10\end{bmatrix}\begin{bmatrix}14\\ 9\end{bmatrix} = \begin{bmatrix}105\\ 216\end{bmatrix} = \begin{bmatrix}1\\ 8\end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix}3 & 7\\ 9 & 10\end{bmatrix}\begin{bmatrix}0\\ 13\end{bmatrix} = \begin{bmatrix}91\\ 130\end{bmatrix} = \begin{bmatrix}13\\ 0\end{bmatrix} \ mod\ 26$$

So the numerical equivalents of the ciphertext are

20, 3, 1, 8, 13, 0.

This corresponds to the letter sequence

UDBINA.

As previously stated, when selecting a key matrix A it is imperative that it be invertible. To determine if the key matrix A is invertible, the *det(A)* must be relatively prime to the modulus *m*. By definition of an inverse matrix, the inverse of a matrix must be a matrix such that when multiplied by the original matrix, or key matrix in our case, the product yields the identity matrix $I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$.

There are at least a couple techniques for finding the inverse of an invertible matrix, whose entries come from a ring $\langle \mathbb{Z}, +, \cdot \rangle$, where + denotes addition modulo *m* and • denotes multiplication modulo *m*. It is possible to use a modified Gauss-Jordan method, but to keep it simple for secondary mathematics students, the method described below works well for finding inverses of *2 x 2* invertible matrices.

For a *2 x 2* invertible matrix, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we will use the following rule

$A^{-1} = [det(A)]^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \bmod m$, where *[det(A)] $^{-1}$* is the multiplicative inverse of *det(A)* modulo *m*, provided it exists.

To decipher the previous encrypted message, UDBINA, which was encrypted with the key matrix $A = \begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix}$, we need to find *A $^{-1}$*. First, since the *det(A) = 30 – 63 = -33 = 19 mod 26,* we have

$$A^{-1} = 19^{-1} \begin{bmatrix} 10 & -7 \\ -9 & 3 \end{bmatrix} \bmod 26.$$

Using the multiplicative inverse modulo *26* table in Appendix C, *19 $^{-1}$ = 11*. Hence we have

$$A^{-1} = 11 \begin{bmatrix} 10 & -7 \\ -9 & 3 \end{bmatrix} = \begin{bmatrix} 110 & -77 \\ -99 & 33 \end{bmatrix} = \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \bmod 26.$$

Now, the numerical equivalents of the ciphertext are

20, 3, 1, 8, 13, 0,

and we calculate

$$\begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 3 \end{bmatrix} = \begin{bmatrix} 123 \\ 121 \end{bmatrix} = \begin{bmatrix} 19 \\ 17 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 8 \end{bmatrix} = \begin{bmatrix} 14 \\ 61 \end{bmatrix} = \begin{bmatrix} 14 \\ 9 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 78 \\ 65 \end{bmatrix} = \begin{bmatrix} 0 \\ 13 \end{bmatrix} \bmod 26$$

The numerical equivalents of the calculated plaintext is

$$19, 17, 14, 9, 0, 13,$$

and converting each calculated integer to its respective letter using table 2.1 we obtain

TROJAN.

The Hill Cipher is an excellent application that enables students to practice matrix operations in an interesting and exciting way. As with the previous examples of classical ciphers, it is assumed that the student is familiar with each classical cipher's respective mathematical process.

APPENDIX A

Mod *m* Alphabets

Table of 95 Printable Ascii Characters with a Mod 26 Alphabet ©KLM

Char	Mod26	Hex	Dec		Char	Mod26	Hex	Dec		Char	Mod26	Hex	Dec
space		20	32		@		40	64		`		60	96
!		21	33		A	0	41	65		a		61	97
“		22	34		B	1	42	66		b		62	98
#		23	35		C	2	43	67		c		63	99
$		24	36		D	3	44	68		d		64	100
%		25	37		E	4	45	69		e		65	101
&		26	38		F	5	46	70		f		66	102
‘		27	39		G	6	47	71		g		67	103
(		28	40		H	7	48	72		h		68	104
)		29	41		I	8	49	73		i		69	105
*		2A	42		J	9	4A	74		j		6A	106
+		2B	43		K	10	4B	75		k		6B	107
,		2C	44		L	11	4C	76		l		6C	108
-		2D	45		M	12	4D	77		m		6D	109
.		2E	46		N	13	4E	78		n		6E	110
/		2F	47		O	14	4F	79		o		6F	111
0		30	48		P	15	50	80		p		70	112
1		31	49		Q	16	51	81		q		71	113
2		32	50		R	17	52	82		r		72	114
3		33	51		S	18	53	83		s		73	115
4		34	52		T	19	54	84		t		74	116
5		35	53		U	20	55	85		u		75	117
6		36	54		V	21	56	86		v		76	118
7		37	55		W	22	57	87		w		77	119
8		38	56		X	23	58	88		x		78	120
9		39	57		Y	24	59	89		y		79	121
:		3A	58		Z	25	5A	90		z		7A	122
;		3B	59		[		5B	91		{		7B	123
<		3C	60		\		5C	92		|		7C	124
=		3D	61		]		5D	93		}		7D	125
>		3E	62		^		5E	94		~		7E	126
?		3F	63		_		5F	95					

Table of 95 Printable Ascii Characters with a Mod 29 Alphabet ©KLM

Char	Mod29	Hex	Dec		Char	Mod29	Hex	Dec		Char	Mod29	Hex	Dec
space	28	20	32		@		40	64		`		60	96
!		21	33		A	0	41	65		a		61	97
“		22	34		B	1	42	66		b		62	98
#		23	35		C	2	43	67		c		63	99
$		24	36		D	3	44	68		d		64	100
%		25	37		E	4	45	69		e		65	101
&		26	38		F	5	46	70		f		66	102
‘		27	39		G	6	47	71		g		67	103
(		28	40		H	7	48	72		h		68	104
)		29	41		I	8	49	73		i		69	105
*		2A	42		J	9	4A	74		j		6A	106
+		2B	43		K	10	4B	75		k		6B	107
,		2C	44		L	11	4C	76		l		6C	108
-		2D	45		M	12	4D	77		m		6D	109
.	26	2E	46		N	13	4E	78		n		6E	110
/		2F	47		O	14	4F	79		o		6F	111
0		30	48		P	15	50	80		p		70	112
1		31	49		Q	16	51	81		q		71	113
2		32	50		R	17	52	82		r		72	114
3		33	51		S	18	53	83		s		73	115
4		34	52		T	19	54	84		t		74	116
5		35	53		U	20	55	85		u		75	117
6		36	54		V	21	56	86		v		76	118
7		37	55		W	22	57	87		w		77	119
8		38	56		X	23	58	88		x		78	120
9		39	57		Y	24	59	89		y		79	121
:		3A	58		Z	25	5A	90		z		7A	122
;		3B	59		[		5B	91		{		7B	123
<		3C	60		\		5C	92		|		7C	124
=		3D	61		]		5D	93		}		7D	125
>		3E	62		^		5E	94		~		7E	126
?	27	3F	63		_		5F	95		Copyright. Kelly L. McCoun			

Table of 95 Printable Ascii Characters with a Mod 89 Alphabet ©KLM

Char	Mod89	Hex	Dec		Char	Mod89	Hex	Dec		Char	Mod89	Hex	Dec
space		20	32		@	30	40	64		`	62	60	96
!		21	33		A	31	41	65		a	63	61	97
“	0	22	34		B	32	42	66		b	64	62	98
#	1	23	35		C	33	43	67		c	65	63	99
$	2	24	36		D	34	44	68		d	66	64	100
%	3	25	37		E	35	45	69		e	67	65	101
&	4	26	38		F	36	46	70		f	68	66	102
‘	5	27	39		G	37	47	71		g	69	67	103
(	6	28	40		H	38	48	72		h	70	68	104
)	7	29	41		I	39	49	73		i	71	69	105
*	8	2A	42		J	40	4A	74		j	72	6A	106
+	9	2B	43		K	41	4B	75		k	73	6B	107
,	10	2C	44		L	42	4C	76		l	74	6C	108
-	11	2D	45		M	43	4D	77		m	75	6D	109
.	12	2E	46		N	44	4E	78		n	76	6E	110
/	13	2F	47		O	45	4F	79		o	77	6F	111
0	14	30	48		P	46	50	80		p	78	70	112
1	15	31	49		Q	47	51	81		q	79	71	113
2	16	32	50		R	48	52	82		r	80	72	114
3	17	33	51		S	49	53	83		s	81	73	115
4	18	34	52		T	50	54	84		t	82	74	116
5	19	35	53		U	51	55	85		u	83	75	117
6	20	36	54		V	52	56	86		v	84	76	118
7	21	37	55		W	53	57	87		w	85	77	119
8	22	38	56		X	54	58	88		x	86	78	120
9	23	39	57		Y	55	59	89		y	87	79	121
:	24	3A	58		Z	56	5A	90		z	88	7A	122
;	25	3B	59		[	57	5B	91		{		7B	123
<	26	3C	60		\	58	5C	92		|		7C	124
=	27	3D	61		]	59	5D	93		}		7D	125
>	28	3E	62		^	60	5E	94		~		7E	126
?	29	3F	63		_	61	5F	95					

Table of 95 Printable Ascii Characters with a Mod 95 Alphabet ©KLM

Char	Mod95	Hex	Dec		Char	Mod95	Hex	Dec		Char	Mod95	Hex	Dec
space	0	20	32		@	32	40	64		`	64	60	96
!	1	21	33		A	33	41	65		a	65	61	97
“	2	22	34		B	34	42	66		b	66	62	98
#	3	23	35		C	35	43	67		c	67	63	99
$	4	24	36		D	36	44	68		d	68	64	100
%	5	25	37		E	37	45	69		e	69	65	101
&	6	26	38		F	38	46	70		f	70	66	102
‘	7	27	39		G	39	47	71		g	71	67	103
(	8	28	40		H	40	48	72		h	72	68	104
)	9	29	41		I	41	49	73		i	73	69	105
*	10	2A	42		J	42	4A	74		j	74	6A	106
+	11	2B	43		K	43	4B	75		k	75	6B	107
,	12	2C	44		L	44	4C	76		l	76	6C	108
-	13	2D	45		M	45	4D	77		m	77	6D	109
.	14	2E	46		N	46	4E	78		n	78	6E	110
/	15	2F	47		O	47	4F	79		o	79	6F	111
0	16	30	48		P	48	50	80		p	80	70	112
1	17	31	49		Q	49	51	81		q	81	71	113
2	18	32	50		R	50	52	82		r	82	72	114
3	19	33	51		S	51	53	83		s	83	73	115
4	20	34	52		T	52	54	84		t	84	74	116
5	21	35	53		U	53	55	85		u	85	75	117
6	22	36	54		V	54	56	86		v	86	76	118
7	23	37	55		W	55	57	87		w	87	77	119
8	24	38	56		X	56	58	88		x	88	78	120
9	25	39	57		Y	57	59	89		y	89	79	121
:	26	3A	58		Z	58	5A	90		z	90	7A	122
;	27	3B	59		[	59	5B	91		{	91	7B	123
<	28	3C	60		\	60	5C	92		|	92	7C	124
=	29	3D	61		]	61	5D	93		}	93	7D	125
>	30	3E	62		^	62	5E	94		~	94	7E	126
?	31	3F	63		_	63	5F	95					

APPENDIX B

Multiplicative Inverses Modulo *m*

Multiplicative Inverses Modulo 26

x	x^{-1} mod 26
1	1
3	9
5	21
7	15
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25

Multiplicative Inverses Modulo 29

x	x^{-1} mod 29
1	1
2	15
3	10
4	22
5	6
6	5
7	25
8	11
9	13
10	3
11	8
12	17
13	9
14	27
15	2
16	20
17	12
18	21
19	26
20	16
21	18
22	4
23	24
24	23
25	7
26	19
27	14
28	28

Multiplicative Inverses Modulo 89

x	x^{-1} mod 89
1	1
2	45
3	30
4	67
5	18
6	15
7	51
8	78
9	10
10	9
11	81
12	52
13	48
14	70
15	6
16	39
17	21
18	5
19	75
20	49
21	17
22	85
23	31
24	26
25	57
26	24
27	33
28	35
29	43
30	3
31	23
32	64
33	27
34	55
35	28
36	47
37	77
38	82
39	16
40	69
41	76
42	53
43	29
44	87

x	x^{-1} mod 89
45	2
46	60
47	36
48	13
49	20
50	73
51	7
52	12
53	42
54	61
55	34
56	62
57	25
58	66
59	86
60	46
61	54
62	56
63	65
64	32
65	63
66	58
67	4
68	72
69	40
70	14
71	84
72	68
73	50
74	83
75	19
76	41
77	37
78	8
79	80
80	79
81	11
82	38
83	74
84	71
85	22
86	59
87	44
88	88

Multiplicative Inverses Modulo 95

x	$x^{-1} \bmod 95$
1	1
2	48
3	32
4	24
6	16
7	68
8	12
9	74
11	26
12	8
13	22
14	34
16	6
17	28
18	37
21	86
22	13
23	62
24	4
26	11
27	88
28	17
29	59
31	46
32	3
33	72
34	14
36	66
37	18
39	39
41	51
42	43
43	42
44	54
46	31
47	93

x	$x^{-1} \bmod 95$
48	2
49	64
51	41
52	53
53	52
54	44
56	56
58	77
59	29
61	81
62	23
63	92
64	49
66	36
67	78
68	7
69	84
71	91
72	33
73	82
74	9
77	58
78	67
79	89
81	61
82	73
83	87
84	69
86	21
87	83
88	27
89	79
91	71
92	63
93	47
94	94

BIBLIOGRAPHY

Works Cited

Barr, Thomas H. Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall, Inc., 2002.

Cohen, Fred. "A short History of Cryptology." (1995) 01 May 2008 <http://all.net/books/ip/Chap2-1.html>.

Flannery, Sarah. In Code: A Mathematical Journey. Chapel Hill, NC: Algonquin Books of Chapel Hill, 2001.

Knight, Judson. "Cryptology, History." (2007) 01 May 2008 <http://www.espionageinfo.com/Cou-De/Cryptology-History.html>.

Pell, Oliver. "Cryptology." 01 May 2008 <http://www.ridex.co.uk/cryptology/>.

Singh, Simon. The Code Book. New York: Anchor Books, 1999.

Wrixon, Fred B. Codes, Ciphers, Secrets and Cryptic Communication. New York: Black Dog & Leventhal Publishers, Inc., 1998.