Cryptography:
A History in Mathematics,
An Application in the Classroom

Brian Olmanson
Mathematics Major
Mathematics Education Major
Bemidji State University

Thesis Introduction

The following is an Honors Thesis conducted within the field of mathematics. Cryptography, the subject of this thesis, was chosen for its rich history and its mathematical significance. Today's world is deeply involved with cryptography, whether people realize this or not. The specific type of cryptography researched for this thesis is classical cryptography, namely ciphers that require only a pencil and paper. This restriction is in place to narrow the topic to ideas and concepts that predate computers and technology. Cryptography has reached levels at which attempting to decipher a message requires high-powered computers. The highest level of technology addressed will be the use of a cipher disk.

This thesis consists of two parts. The first part is the result of research into the history and the mathematics of cryptography. In the form of a paper, the results are presented in an order of increasing complexity and level of mathematical involvement. The goal of the research and paper is to provide the background support for the second part of the thesis.

The second part of this thesis is creative in nature. Using the information gathered through the research conducted, I created two units that are applicable to the classroom. The first unit is intended for students in the middle school level, and the second unit is intended to be used in a high school classroom. The nature of each unit is to engage students in mathematics by having them explore the world of cryptography. The units are also intended to address standards as identified by the National Council of Teachers of Mathematics including Problem Solving, Numbers and Operations, Communications and Connections.

Included within this thesis are the paper which presents the findings from the research, a middle school cryptography unit as well as a high school cryptography unit, both of which include an outline, lesson plans, activities and worksheets, and a conclusive statement about the thesis.

Cryptography is an area of mathematics that has been of deep interest to people throughout history, and it continues to this day to spark a sense of excitement and intrigue when it is encountered.

Cryptography: A History in Mathematics

The world is full of secrets. During times of war or political upheaval, as well as times of relative peace, there has been a great deal of secret communication. People throughout history have relied upon cryptography, or secret writing, to communicate. The earliest known use of cryptography dates back to the Babylonians. Researchers discovered an encrypted recipe on a tablet for making pottery glaze dating from about 1500 BC (Tattersall 210). Egyptians also used hieroglyphics in a cryptographic system. Many cultures are known to have utilized cryptography. As cultures become more advanced, so do their cryptographic systems and the devices they use for encryption and decryption. From the Greeks, who developed multiple cryptographic systems, to the present widespread accessibility and use of the internet, people have relied upon cryptography to ensure security and privacy.

Before engaging in the study of cryptography, it is important to understand the terminology. Cryptography is different than simply using a code. Cryptography takes the original message and transforms it into an enciphered message. This means the plaintext is turned into ciphertext using a cipher. A code, on the other hand, is a system that substitutes meanings for different words or symbols. It is often necessary to have a code book in order to decode a secret message (Callery 57). When using cryptography, a ciphertext may be sent with the letters of the message in groups of the same size as the words of the plaintext message. Depending on the message length, a ciphertext may be sent with the letters of the message in groups of four or five to increase the difficulty of deciphering the message by unwanted parties. An important note to make is that for some messages, a letter that appears less often in plaintext such as X or Z is added to the plaintext enough times to preserve the message's quadruplicate or quintuplicate nature (Tattersall 215).

One basic type of ciphers is transposition ciphers. A transposition cipher does not transform any of the letters of plaintext into ciphertext. Rather, the plaintext message itself is rearranged in order to hide its intended meaning. The Spartans are known to have used one of the earliest transposition ciphers and utilized the first known cryptographic device. To encrypt a message, a strip of papyrus was wrapped around a scytale, a cylindrical rod of set length and radius, and the message was written lengthwise down the

rod. Both sender and receiver had identical scytales, so when the strip of papyrus was delivered, the receiver needed only to wrap the papyrus around the scytale and read the deciphered message. The speed and ease of decryption was particularly useful to communicate during battles when time was of the essence (Callery 64).

Transposition ciphers do not rely upon devices to encrypt and decrypt. Anagrams are a simple example of a transposition cipher. These are commonly published in newspapers as a logic activity for readers. An anagram is simply a rearrangement of the plaintext letters to hide the original message. A simple example is the plaintext THOMAS JEFFERSON can be rearranged to JANE OFFERS MOTHS (Lambert 24). Sending an anagram message is not particularly easy or useful, but the anagramming technique is an excellent approach when attempting to decipher a ciphertext known to have been created using a transposition cipher (Pincock 19). Since all of the original plaintext letters are still in the message, arranging them in their intended order may be accomplished through anagramming. However, the results will not be achieved as quickly as knowing the type of transposition that was performed.

Most transposition ciphers follow a certain visual pattern to create ciphertext from plaintext. A simple transposition cipher example is the rail-fence cipher which got its name from the split-rail fences that were constructed across the United States in the 19th century that formed a zigzag pattern when viewed from above (Callery 65). Using this method for plaintext encryption, the sender writes the message in a zigzag pattern, and then writes the letters in horizontal order to obtain the ciphertext. See Figure 1 for an example of this cipher.

Figure 1: The rail-fence cipher.

To decipher the ciphertext, the receiver would first divide the letters into two equal groups. Then they would write down the first letter from the first group, write the first letter from the second group, continue with the second letter of the first group, and so on,

thus recreating the plaintext. A more complex rail-fence cipher is to use more than two rows, but continue the zigzag pattern. See Figure 2 for an example of a three row rail-fence cipher.

Figure 2: Three row rail-fence cipher.

Deciphering a three row rail-fence cipher requires care on the receiver's part. The process is easy if the number of rows being used is known. To break a rail-fence cipher, reorganizing the message into different numbers of rows may result in decipherment (Callery 67).

Complex transposition ciphers include geometric ciphers, or box ciphers, which provide a number of ways plaintext may be enciphered. These require the plaintext be written in a matrix of predetermined dimensions and enciphered using a certain pattern or method (Lambert 30). Generally, the number of columns is the dimension that will be set for a certain cipher. Below, in Figure 3, are two examples of geometric ciphers. The first example is a two-column matrix and the second uses a four-column matrix. The message is identical with the different resulting ciphertexts shown. As stated earlier, many messages have a certain letter (say X or Z) added to the end to help the plaintext reach a certain length to make the message quadruplicate or quintuplicate (divisible by four or five, respectively).

Plaintext: ciphers have been used for centuries x

Two-column ciphertext: CSIE PDHF EORR SCHE
ANVT EUBR EIEE NSUX

Four-column ciphertext: CASN IVET PEDU HBFR
EEOI RERE SNCS HUEX

C	S
I	E
P	D
H	F
E	O
R	R
S	C
H	E
A	N
V	T
E	U
B	R
E	I
E	E
N	S
U	X

C	A	S	N
I	V	E	T
P	E	D	U
H	B	F	R
E	E	O	I
R	E	R	E
S	N	C	S
H	U	E	X

Figure 3: A two-column and four-column geometric cipher.

As shown above, the receiver should know the number of columns being used to decipher these messages. While not crucial, it aids in speeding up the process. When given the number of columns, the receiver writes the message in the number of columns and is able to quickly read the plaintext message vertically.

To increase the integrity of geometric ciphers, the encrypted pattern can be modified to deter unwanted decryption. Using a four-by-six matrix array, multiple path options are possible. The plaintext can be written in consecutive columns and then encrypted in a spiral starting from the center. Another possible path is to write the plaintext across a row and back the next. The message could also be written in the rows and the encryption path follows the columns (Lambert 34). Another method to increase a cipher's security is to assign a key word to the pattern. This allows writing the plaintext then encrypting the message using the columns in alphabetical order from the letters of the key word. In Figure 4, there are a few examples adapted from Lambert pp.36-37 that

show multiple pathways along with key words that may be used for encryption. In the lower part of the figure is an example using the key word SHADOW and its corresponding pathway to encipher a plaintext message.

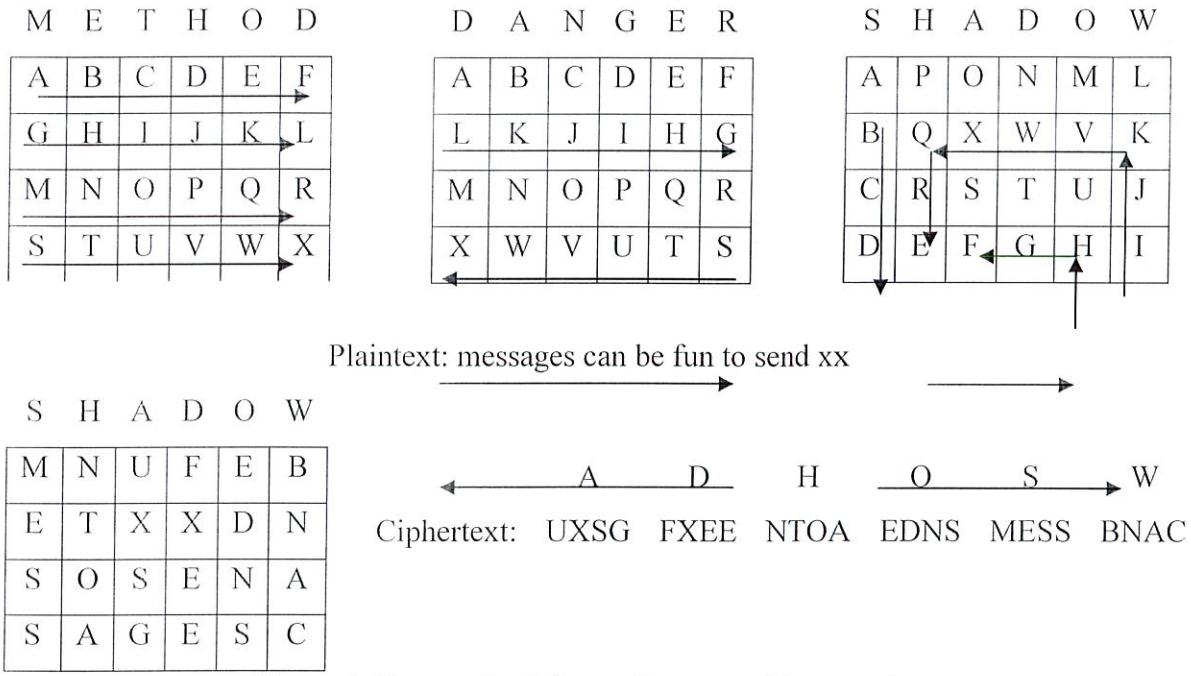


Figure 4: Geometric cipher pathways and key words.

Providing the key word and identified pattern expedites the process of deciphering the message. It is advantageous to be able to change the encryption method from message to message to hinder the progress of deciphering by anyone intercepting the message. Transposition ciphers combined with other ciphers create a ciphertext that is much less likely to be deciphered by anyone for whom it was not intended.

A basic monoalphabetic cipher utilizing matrices was devised by Polybius in Greece during the second century BC. His method was to create a matrix, or grid, and place the letters of the alphabet within them (Berloquin 6). To create the ciphertext, he replaced the letters of his message with two-digit numbers. The first digit corresponded with the row in which the plaintext letter was located and the second digit corresponded with the respective column. For a 26 letter alphabet, a five-by-five matrix is made, but two letters must share a space. In the English language, this cipher usually has I and J share the same location. The table below shows the structure of the grid used for Polybius' method, with the rows and columns labeled 1 through 5.

	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

Table 1: Polybius' method.

To demonstrate Polybius' method, take the plaintext message: be as you wish to seem. Using the table above, the ciphertext message sent would be:

12 15 11 43 54 34 45 52 24 43 23 44 34 43 15 15 32

Making the cipher more difficult to crack by unwanted parties is easily accomplished by using a key word to change the order of the letters within the table. When using a key word, the letters of the word are placed in the spaces on the table from left to right, top to bottom. Letters are not repeated, so if a letter again appears in the word, it is then skipped. Once the word is written out, the remaining letters of the alphabet are placed in order in the table, skipping the letters used in the key word. Two examples may be viewed in the table below.

	1	2	3	4	5
1	C	I/J	P	H	E
2	R	A	B	D	F
3	G	K	L	M	N
4	O	Q	S	T	U
5	V	W	X	Y	Z

	1	2	3	4	5
1	A	X	E	M	N
2	B	C	D	F	G
3	H	I/J	K	L	O
4	P	Q	R	S	T
5	U	V	W	Y	Z

Table 2: Polybius' method. Key words CIPHER and AXEMAN.

Using key words can aid in keeping messages secret. To enhance the usefulness of this practice, changing key words regularly can keep messages from being deciphered easily by outside parties. This can be accomplished by hiding the key word within certain parts of the overall message and using it to encipher vital, secret information. Deciphering these types of messages is best done through frequency analysis.

Ciphers that appear in different problem-solving activities are substitution ciphers where letters are substituted for one another at random, such as B represents X in the enciphered message. These ciphers are subject to deciphering through logical approach and frequency analysis. The relative frequency, in percentages, of letters as observed in the English language can be seen in the table below.

A	B	C	D	E	F	G	H	I	J	K	L	M
8.0	1.5	3.0	3.9	12.5	2.3	1.9	5.5	7.2	0.1	0.7	4.1	2.5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.1	7.6	2.0	0.1	6.1	6.5	9.2	2.7	1.0	1.9	0.2	1.7	0.1

Table 4: Frequency of letters in the English language, in percentages (Pincock p.24).

Cryptanalysts rely heavily upon frequency distributions in breaking various ciphers. By analyzing the characters or numbers that appear in a cipher, the person attempting to decipher a message can use the information to make conjectures as to which ciphertext characters represent which plaintext characters. This approach is often used for monoalphabetic ciphers. If more steps are utilized during the message enciphering process, frequency analysis becomes less viable.

Shift ciphers have a more organized approach to their methods than substitution ciphers. Julius Caesar devised a shift cipher to send confidential messages to his military officers and political allies. To create a ciphertext using the Caesar cipher, the sender substitutes the plaintext letters with the letters in the alphabet that are three to the right (Kahn 84). For example, *X*, *Y*, and *Z*, are enciphered as *A*, *B*, and *C*, respectively. The table below shows the Caesar cipher with the top row representing the plaintext letters and the bottom row representing the corresponding ciphertext.

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
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

Table 3: Caesar cipher (Tattersall 212).

Caesar had created a cipher which allowed him to send secret messages that were more difficult to decipher than simple transposition ciphers. Messages fairly short in length are not as vulnerable to frequency analysis. Also at this time, language analysis was not

developed to the point to which letter frequency was studied. Caesar's monoalphabetic shift cipher created a strong advantage over his foes.

Encryption and decryption of a shift cipher may be done mathematically using modular arithmetic. To begin, the letters of the alphabet are assigned numerical values with A being 0 through Z being 25. For the Caesar cipher, to encipher a message, the original message must be translated into its numerical equivalent, then each value is entered into the congruence $C \equiv P + 3 \pmod{26}$, where P is the plaintext value and C is the ciphertext value (Tattersall 213). In this expression, the 3 represents the size of the shift that is used for this cipher. For example, consider the plaintext message: the fox jumped over the lazy dog. Translated into its numerical equivalent, the plaintext message now reads:

19 7 4 5 14 23 9 20 12 15 4 3 14 20 4 17 19 7 4 11 0 25 24 3 14 6.

After being entered into the congruence equation given above, the ciphertext message now reads:

22 10 7 8 17 0 12 23 15 18 7 6 17 23 7 20 22 10 7 14 3 2 1 6 17 9.

Replacing the numerical values with their letter representations gives the ciphertext: WKHIR AMXPS HGRXH UWKHO DCBGRJ. To decipher the message, the congruence $P \equiv C - 3 \pmod{26}$ is used on the ciphertext. This will produce the plaintext message.

The Caesar cipher is the most common example of a simple shift transformation. For any shift transformation, the size of the shift, say k, can range from $0 \leq k \leq 25$. To encipher with a shift of k, the congruence $C \equiv P + k \pmod{26}$ is used. The congruence $P \equiv C - k \pmod{26}$ is used for decipherment of messages (Young 27). Simple shift ciphers may easily be deciphered using frequency analysis if enough messages are sent using the same cipher, thus causing vulnerability. By computing the frequency of each letter in ciphertexts, a decipherer may easily determine which letters represent the letters of the plaintext messages and also find the shift size to recreate the original message.

To increase the difficulty in deciphering messages, an affine cipher may be utilized. Affine ciphers use modular arithmetic similar to shift ciphers, however, the congruence equation is $C \equiv aP + b \pmod{26}$, with $0 \leq a,b \leq 25$ and a and 26 are relatively prime, that is $\gcd(a, 26) = 1$. Shift ciphers are affine ciphers with $a = 1$. In

order to decipher an affine cipher, the congruence $P \equiv a^{-1}(C - b) \pmod{26}$ is used where $0 \leq P \leq 25$ and $aa^{-1} \equiv 1 \pmod{26}$ (Tattersall 214). While affine ciphers are more difficult to crack than shift ciphers, they are still vulnerable to frequency analysis. A shift cipher follows the same frequency pattern as the English alphabet whereas the frequency pattern is changed when using an affine cipher, making deciphering more challenging.

In reaction to the decipherment through frequency analysis, polyalphabetic ciphers using multiple substitutions were introduced. An Italian named Leon Battista Alberti, artist and author of the first printed book on architecture, developed the idea for constructing a cipher disk in a treatise on ciphers in 1467 (Tattersall 220). Alberti's cipher disk is the first appearance of a polyalphabetic cipher. The disk was constructed from two copper disks of different sizes held together with a pin through their centers. These disks were divided into 24 equal parts. Alberti's original design used the 20 letters of the Italian alphabet along with the first four natural numbers for his plaintext on the outer disk (Boone 16). When using a cipher disk, the outer disk represents the plaintext, and the inner disk represents the ciphertext. Below are two examples of the cipher disk: the one on the left is the original design as created by Alberti, the disk on the right uses modern English letters and is divided into 26 parts accordingly.

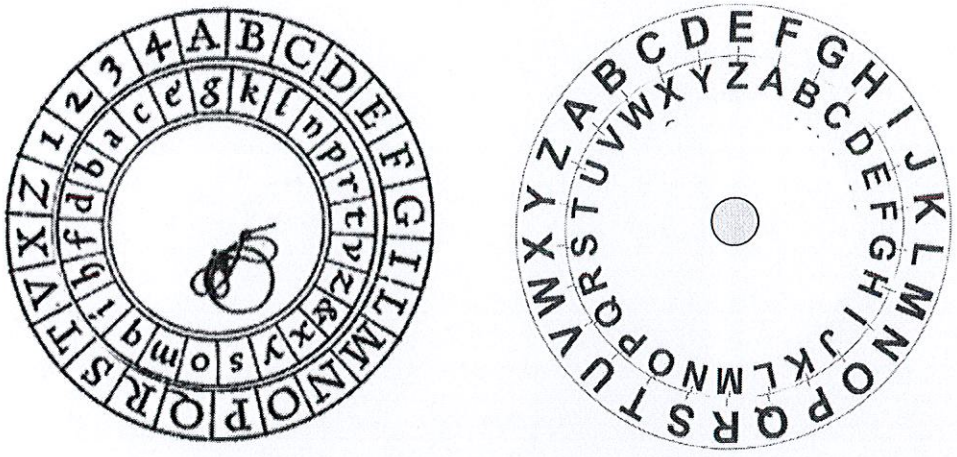


Figure 5: Alberti's original cipher disk design (http://starbase.trincoll.edu), and modern English design (http://www.kidsmakestuff.com).

To increase the difficulty of decipherment with a cipher disk, one can randomize the order of the letters on the inner disk. There are numerous ways one can use a cipher disk to encipher a message. If the inner disk is not turned during encipherment, then a simple

substitution or shift cipher results. One method to utilize the advantage a cipher disk presents is to encipher the first few words under one setting, then rotate the inner disk a set distance and encipher the rest of the message (Tattersall 220). Consider the plaintext message: no sacrifice no victory x. Enciphering the first two words using the setting of the modern English cipher disk in Figure 5, the first part of the ciphertext reads: IJNVX MDADX Z. Now, by rotating the inner disk seven positions clockwise so that F is now enciphered as T, the rest of the ciphertext is: BCJW HLFML. So the complete resulting ciphertext is: IJNVX MDADX ZBCJW HLFML. By introducing multiple shifts in the cipher, frequency analysis is not as useful in decipherment (Callery 94). To accurately decipher the message, the receiver will need an identical cipher disk, and needs to know the initial settings for the message and how far and in which direction shifts occur. Once this information is relayed, the receiver locates the letters of the enciphered message on the inner disk and translates the plaintext off the outer disk.

In 1518, the first book on cryptography, *Polygraphia*, was printed. The author, a German monk named Johannes Trithemius, had previously published works on various subjects that were written containing various writings in ciphers. The most important innovation that Trithemius made in *Polygraphia* was the transformation of the cipher disk into an alphabetic square to encode plaintext (Tattersall 221). As seen below, the plaintext alphabet table was recreated into a table where the alphabet shifted one place to the left each step down.

	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

Table 7: The Trithemius table (http://www.braingle.com).

Using Trithemius' cipher, a message is enciphered by finding the corresponding plaintext letter in the top row. The first letter of the ciphertext is then the letter below the plaintext

letter in the first row below the topmost row. Each successive ciphertext letter is found in the next row down below its corresponding plaintext letter (Kippenhahn 110). For example, through this method the plaintext word "secret" would result in the ciphertext word SFEUIY.

Giovan Batista Belaso introduced a polyalphabetic cipher in 1553 similar to Trithemius' cipher. The cipher used the table developed by Trithemius, but has a more involved method for encoding: a key phrase has its letters aligned with the letters of the plaintext message. The letter in the key phrase above a plaintext letter is located in the topmost row above which column the ciphertext letter comes from, and the plaintext letter itself is located in the leftmost column of the table. The letter which is in that row and column is the ciphertext letter used (Kahn 137). For example, the key phrase "thy kingdom come" is placed above the plaintext. Using Table 7, the plaintext message "they come at dawn" is enciphered as seen below.

Key phrase:	T	H	Y	K	I	N	G	D	O	M	C	O	M	E
Plaintext:	t	h	e	y	c	o	m	e	a	t	d	a	w	n
Ciphertext:	M	O	C	I	K	B	S	H	O	F	F	O	I	R

Table 8: Belaso cipher.

To decipher the message, the receiver knows the key phrase and finds the ciphertext letter in the column with the letter of the key phrase in the top row and identifies the plaintext letter at the leftmost position of the row. This cipher is quite useful in avoiding unwanted decipherment. From the above enciphered message, frequency analysis would have little affect because the ciphertext F represents both T and D, I represents Y and W, and O represents E and A. The communication difficulty for the sender and receiver with this cipher is sharing the key phrase to use for the message and keeping this information from being intercepted.

Blaise de Vigenére, a cryptanalyst for Charles IX of France, developed a number of cipher systems. His work with the Trithemius table resulting in it becoming known as the Vigenére tableau. Similar to Belaso's method, Vigenére created a cipher where a key word was repeated instead of using a key phrase (Kippenhahn 185). For example, using the key word "safe", the plaintext message "please send help" is enciphered using the same process as Belaso.

Key word:	S	A	F	E	S	A	F	E	S	A	F	E	S	A
Plaintext:	p	l	e	a	s	e	s	e	n	d	h	e	l	p
Ciphertext:	H	L	J	E	K	E	X	I	F	D	M	I	D	P

Table 9: Vigenére key word cipher.

Similar to Belaso's cipher, frequency analysis has little use, because the letter E is enciphered as J, E, and I. Also, the ciphertext letter D represents both plaintext letters D and L. A weakness in this cipher is that if the length of the key word is found by a cryptanalyst, say six letters, then frequency analysis can be applied to successive sets containing every sixth word (Tattersall 225). This method may be used if the key word is used for either long or multiple messages. Vigenére worked to develop more rigorous ciphers.

Two of Vigenére's most notable ciphers are both autokey ciphers. In these ciphers, both the sender and receiver know the first letter of the key, then the rest of the letters of the key are either the letters of the plaintext or the ciphertext themselves (Pincock 72). If the person who is deciphering received the ciphertext "IKLML GBCBR" and knew the first letter of the key was P, then by using the same method of decipherment as before, the plaintext is revealed, and each successive letter of the plaintext is then used as the key for the cipher as seen in the table below.

Key:	P	T	R	U	S	T	N	O	O	N
Plaintext:	t	r	u	s	t	n	o	o	n	e
Ciphertext:	I	K	L	M	L	G	B	C	B	R

Table 10: Vigenére plaintext autokey cipher.

Through decryption, the plaintext message is revealed to be "trust no one". Now consider if the message received is CGKDD WJXLY, and the first letter of the key is known to be Q. Using the ciphertext as the autokey, the plaintext may then be deciphered as follows.

Key:	Q	C	G	K	D	D	W	J	X	L
Plaintext:	m	e	e	t	a	t	n	o	o	n
Ciphertext:	C	G	K	D	D	W	J	X	L	Y

Table 11: Vigenére ciphertext autokey cipher.

Again, using Table 7 as before, the plaintext message is found to be "meet at noon". The autokey ciphers are even less susceptible to frequency analysis than the Vigenére's key word cipher (Tattersall 225).

As time goes on, cryptographers challenge themselves by developing ciphers that are difficult to break. One such cipher is the block cipher, or Hill cipher, as devised by Lester Hill (Tattersall 231). The Hill cipher takes certain size blocks of letters from the plaintext and substitutes a block of ciphertext of the same size. Vulnerability to frequency analysis is decreased greatly due to the cipher's polygraphic nature. To encipher using a Hill cipher, a plaintext message must have its letters replaced with their numerical values. Then the ciphertext is formed using the relationship $C \equiv AP \pmod{26}$, where A is an n-by-n matrix with determinant co-prime to 26, and C and P are 1-by-n column matrices with entries corresponding to the ciphertext and plaintext numerical values, respectively, and n is the length of the blocks of letters.

Encipher the message "Euler was quite bright x" with the "x" added to preserve the quintuplicate nature of the message, using a Hill cipher with

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} \qquad \det(A) = -5,\ \gcd(-5, 26) = 1$$

First, partition the plaintext into blocks of length 2 and translate the blocks into their numerical equivalents:

E	U	L	E	R	W	A	S	Q	U	I	T	E	B	R	I	G	H	T	X
4	20	11	4	17	22	0	18	16	20	8	19	4	1	17	8	6	7	19	23

The matrix calculations performed on the first four blocks are shown below:

$$\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 4 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 44 \\ 76 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 24 \end{pmatrix} \pmod{26} \qquad \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 56 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 4 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 17 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 61 \\ 134 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 4 \end{pmatrix} \pmod{26} \qquad \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 0 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 36 \\ 54 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 2 \end{pmatrix} \pmod{26}$$

These calculations are continued and result in the following blocks of ciphertext:

18	24	19	4	9	4	10	2	4	20	20	11	6	19	7	14	20	19	13	15
S	Y	T	E	J	E	K	C	E	U	U	L	G	T	H	O	U	T	N	P

Thus the resulting ciphertext reads: SYTEJ EKCEU ULGTH OUTNP

For decipherment of a Hill cipher, the inverse of matrix A, A^{-1} (mod 26), must be used. The following expression shows why through substitution on matrix operations. $A^{-1}C \equiv A^{-1}(AP) \equiv (A^{-1}A)P \equiv P$ (mod 26). A digraphic Hill cipher has $n = 2$, a trigraphic has $n = 3$, and if $n > 3$ it is called polygraphic.

As communication technology improves, the need for high-level security increases. Innovative ciphers were developed by Martin Hellman at Stanford in 1978. These ciphers were exponential ciphers. To encipher with an exponential cipher, a prime p such that $2525 < p < 252525$ and an enciphering key, e being a positive integer such that $\gcd(e, p - 1) = 1$ are needed. The exponential congruence $C \equiv P^e$ (mod p), where C is the ciphertext block and P is the plaintext block, and $0 \leq C \leq p$, is used to create the ciphertext. From the method of enciphering, the level of complexity involved with this cipher is clear. These ciphers are the basis on which internet security relies upon. "Exponential ciphers discourage cryptanalysis since the cryptanalyst needs to determine the prime and exponent involved in enciphering the message, a formidable task even with a high-speed computer" (Tattersall 235). Technology has created ways for increasingly rigorous ciphers to be developed.

The world of cryptography is a vast, never-ending adventure. Secret communication throughout history has been important. Many cryptographers have made it their goal to create an unbreakable cipher. While many have created ciphers that challenge even the best cryptanalysts, mathematics most often provides a clue or answer as to how to break the cipher. Cryptography is an area where history, mathematics and imagination meet to form exciting and interesting puzzles.

Cryptography Units Introduction

Using the findings from the paper, two units were constructed for use in a classroom setting. The first unit is designed for the middle school level, and the second for the high school level. Each of these units addresses the standards identified by the National Council of Teachers of Mathematics. These standards include Problem Solving, Numbers and Operations, Communication and Connections.

The two units have similar structures. Each has an outline that provides basic information about the topics that are addressed during the lesson. The overall lesson plan structure is of the design Launch, Explore, Share and Summarize as adapted from the Core-Plus Mathematics Project (Hirsch xiii). This method fosters student learning and involvement through the classroom. Deviating from traditional lectures, the activities within each unit encourage students to use their prior knowledge to aid them in answering questions and formulating ideas. Lesson plans and black-line masters are provided for each unit.

Middle School Cryptography Outline

Days: 10

Lesson plan format: Launch, Explore, Share, Summarize

Day 1:
- Introduction to cryptography
- Transposition ciphers, namely rail-fence ciphers
- Students create and decipher transposition ciphers

Day 2:
- Review transposition ciphers
- Show an example of a geometric cipher
- Students work in pairs to develop a geometric cipher
- Work in pairs to attempt to break a geometric cipher
- Share different methods of enciphering and deciphering

Day 3:
- Introduce substitution ciphers
- Students receive worksheet with messages on them, work in pairs to solve
- As class, share different methods for solutions

Day 4:
- Review solutions to substitution ciphers
- Develop a mathematical approach to solving: frequency analysis
- Students receive plaintext writing, make graphs of letter frequency
- Students receive enciphered messages, using letter frequency, make conjectures as to what ciphertext letters represent which plaintext letters

Day 5:
- Continue looking at frequency analysis
- Introduce shift ciphers
- Students analyze shift ciphers
- Identify the pattern of letter frequency of shift ciphers verse substitution ciphers

Day 6:
- Introduce cipher disk
- Each student receives a sheet with two disks to cut out and a brass fastener
- Students get to decide how to organize inner disk
- Students encipher messages using disks, and create methods to hinder frequency analysis
- Students share how they constructed their cipher disks, and as class discuss different levels of difficulty in deciphering

Day 7:

- Introduce the Trithemius table
- Work with key phrase and key word methods

Day 8:

- Continue working with Trithemius table
- Introduce autokey cipher
- Discuss frequency analysis for key word method

Day 9:

- Review and potential overflow day if lessons go beyond their allotted times
- Possible extra credit: have one or two messages students must solve without knowing the method used for enciphering

Day 10:

- Test: Students must: decipher a rail-fence cipher; using frequency analysis identify a substitution cipher, shift cipher, and a cipher that cannot be determined; decipher an autokey cipher using the Trithemius table; use their cipher disk to encipher a message utilizing and identifying a method with which they can deter frequency analysis
- For the final test, either provide each student with the Trithemius table or display one on the board in front of the class
- Test: "Cryptography Quest"

Day 1 Lesson Plan

Objective:

To introduce students to cryptography, develop communication between students through collaboration, make connections between mathematics and history, and develop students' problem-solving skills.

Materials Needed:

None.

Launch: (Approximately 10 minutes)

Give a brief background on cryptography. Ask the students how long they believe people have been writing in secret. They have been doing so for over 3000 years! Share with them how the Greeks used the scytale and how today cryptography is seen in news papers with jumbled words. Show how THOMAS JEFFERSON can be rearranged as JANE OFFERS MOTHS. Demonstrate a two row rail-fence cipher (See example below). Explain how transposition ciphers change the order of the letters of a message, but leaves them unaltered.

Plaintext: cryptography is neat

C Y T G A H I N A

R P O R P Y S E T

Ciphertext: CYTGA HINAR PORPY SET

Explore: (Approximately 25 minutes)

Have students divide up into pairs. Instruct the pairs to come up with a three or four word message they would like to send. Then as a pair, have them devise a transposition cipher to encipher their message. Inform them that they will have approximately 10 minutes to encipher their message. When groups are doing this, circulate the room and provide ideas or ask questions to motivate student thinking. After the 10 minutes have passed, have students trade with another pair, and then give them time to attempt to decipher the message they have received.

Share: (Approximately 10 minutes)

Once the groups have had their 15 minutes to decipher, ask for a few groups to share the message they received and how the did, or tried, to decipher it. Then have the group that wrote the message share how they enciphered the message. Ideally a few successful groups will be able to share how they deciphered their message.

Summarize: (Approximately 5 minutes)

Ask the students what the most important assets are when trying to decipher a message. Put their answers on the board. Stress that the two most valuable tools when attempting to decipher a message are time and patience.

Day 2 Lesson Plan

Objective:

Develop problem-solving and communication amongst students through the exploration of geometric ciphers.

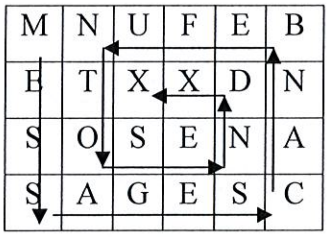
Materials Needed:

None.

Launch: (Approximately 10 minutes)

Begin the class by reviewing the outcomes of the previous day. Remind students that transposition ciphers change only the order of the letters, not the letters themselves. Introduce the class to geometric ciphers. Share with them an example of a possible path and key word, and how to encipher with it. (See example below.)

S H A D O W



	A	D	H	O	S	W
Ciphertext:	UXSG	FXEE	NTOA	EDNS	MESS	BNAC

This message also demonstrates how null letters (letters that do not have meaning in context with the message) are inserted to help messages reach a prescribed length. Tell students that X will be the letter used in the class as a null letter.

Explore: (Approximately 25 minutes)

Have students divide into pairs. With their partner, have them create a geometric cipher and then encipher a message using it. Make sure that students use a four-by-six grid for their cipher so that the class is uniform. Allow students approximately 10 minutes to encipher their message. Next, have each pair trade messages with another group, and then have them attempt to decipher the message. Give

students about 15 minutes to work on their messages. During both the enciphering and deciphering of messages, monitor pairs to keep them on task, and provide encouragement and insight where necessary.

Share: (Approximately 10 minutes)

Have a few groups share the message they received and how they attempted to decipher it. When a group presents how they attempted to decipher the message, have the group who enciphered it share how they did so. As a class, examine the different methods of enciphering and identify which ones created difficulties when attempting to decipher.

Summarize: (Approximately 5 minutes)

Discuss the usefulness of a geometric cipher over other transposition ciphers, in the fact that they can provide more complex transpositions while being fairly easy to decipher when the method for enciphering is known. Ask students how key words can be shared secretly without being within the cipher itself. Share how it is possible to include a plaintext message with little meaning in which a certain word, say the fourth, is the key word to which type of geometric cipher was used.

Day 3 Lesson Plan

Objective:

To encourage problem solving and communication by having students solve substitution ciphers with partners.

Materials Needed:

One "Intercepted Messages!" sheet per student.

Launch: (Approximately 5 minutes)

Inform the students that you have just received two messages that the National Security Agency, one of the top cryptological organizations, needs help deciphering. Let them know that the two messages were enciphered using substitution ciphers. This means that each letter has been replaced by a different letter in the alphabet, such as X is now written as A. Also, let them know that the order of the letters and size of the words have not been altered.

Explore: (Approximately 35 minutes)

For this lesson, the Explore and Share portions are intermixed. Have the students work on the first message. Walk around the room to monitor progress, and provide minimal assistance. If a pair is having difficulties, ask them what certain words may be, such as two letter words, or words that occur more than once in the message. Allow approximately 15 minutes for the first message then have groups share what they found the answer to be, and how they went about deciphering the message. Encourage groups to use refined methods to decipher the second message. Allow about 10 minutes for this then have groups share what they found the message to say as well as how they deciphered it.

Share: (Approximately 0 minutes)

Combined with Explore portion of lesson.

Summarize: (Approximately 10 minutes)

Discuss with students different methods for deciphering substitution ciphers, such as making logical guesses based on word size or letter placement. For example, if the message as a word such as KWWO, it is a reasonable assumption to make that the WW represents EE or OO like in the words seen or took. Using logical approaches to these types of ciphers produce good results. Ask the students what they could do if the ciphertext letters were grouped differently than the sizes of the original words. This will be addressed the next day.

Name_____

INTERCEPTED MESSAGES!!!

Message 1:

X-Z-T-V Z-A E-Y-Z V-L-Y-C-S-C-E-X I-E E-Y-V K-I-E-C-Z-K-I-B

F-G-O-J-E-Z-B-Z-M-C-F T-H-X-V-R-T K-V-I-G S-I-B-E-C-T-Z-G-V

F-I-K S-V X-V-V-K Z-K E-Y-V D-Z-G-B-Q D-C-Q-V D-V-S.

Wait until instructed to continue on to the second message.

Message 2:

H-R-K-N-D J-D-N-K G-R D-N-O-K D-B-G-N-I-I-Z-G-N

U-Z-H-G-J-A-N-D E-B-H-F G-R N-B-A-G-W B-O-K G-R U-I-B-V

E-B-H-F H-R-L-U-B-H-G K-Z-D-F-D B-A-N B-H-G-J-B-I-I-B B-E-I-N

G-R H-R-A-A-N-H-G N-A-A-R-A-D.

Name **Key**

INTERCEPTED MESSAGES!!!

Message 1:

X-Z-T-V Z-A E-Y-Z V-L-Y-C-S-C-E-X I-E E-Y-V K-I-E-C-Z-K-I-B
F-G-O-J-E-Z-B-Z-M-C-F T-H-X-V-R-T K-V-I-G S-I-B-E-C-T-Z-G-V
F-I-K S-V X-V-V-K Z-K E-Y-V D-Z-G-B-Q D-C-Q-V D-V-S.

Some of the exhibits at the national cryptological museum near Baltimore can be seen on the world wide web.

Message 2:

H-R-K-N-D J-D-N-K G-R D-N-O-K D-B-G-N-I-I-Z-G-N
U-Z-H-G-J-A-N-D E-B-H-F G-R N-B-A-G-W B-O-K G-R U-I-B-V
E-B-H-F H-R-L-U-B-H-G K-Z-D-F-D B-A-N B-H-G-J-B-I-I-B B-E-I-N
G-R H-R-A-A-N-H-G N-A-A-R-A-D.

Codes used to send satellite pictures back to Earth and to play back compact disks are actually able to correct errors.

Source: COMAP, Inc. Mathematics: Modeling our World. W. H. Freeman and Company. New York: 1998, p. 56.

Day 4 Lesson Plan

Objective:

Utilize graphing skills and understanding of percentages to aid in the deciphering of a message. Students will use number sense when both calculating and comparing percentages. Identify connections between language and mathematics.

Materials Needed:

One "The Letters Count" worksheet per student.

Launch: (Approximately 5 minutes)

Review the findings of the previous day on substitution ciphers. Share with the students that many ciphers are sent with the ciphertext in groups of letters, rather than in their original words. Today they will analyze the English language, and use this knowledge to decipher a message.

Explore: (Approximately 40 minutes)

After each student has received a "The Letters Count" worksheet, they should find a partner to work with. The worksheet involves counting the letters of a passage, and then analyzing their frequency. Next, students analyzed an enciphered message using the same method, and use their findings to aid in deciphering the message. Allow them the class period to work on these findings. During this time, circulate through the room providing insight and encouragement where necessary.

Share: (Approximately 5 minutes)

Once the pairs seem to have all completed the first page of the worksheet, have one pair draw their dot plot on the board. Have another pair fill in a table with the percentages up on the board.

Summarize: (Approximately 0 minutes)

Students will continue the worksheet the next day.

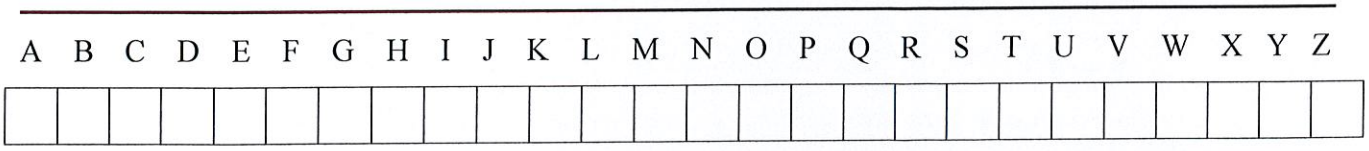
Name_____

The Letters Count

Read the passage below from Codes and Ciphers by Sean Callery.

"The scytale is the earliest known piece of cryptographic equipment, dating from fifth-century BC Greece. Probably first used by the Spartans to carry messages around the battlefield, it is a simple transposition machine. A piece of parchment similar to a ribbon was wrapped around a cylinder, such as a wooden staff. The message was then written unencrypted onto the coiled paper" (Callery 64).

Once you have read through it once, work with a partner to count how many times each letter of the alphabet appears in the text. Record your findings on the dot plot below. Record the number of times each letter occurs in the space in the table below it.



Add up the numbers from the table to find the total number of letters in the passage. Find the frequency that each letter occurs as a percentage of the passage. Record these calculations in the table below.

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

The Letters Still Count

The following message is enciphered text from Codes and Ciphers by Sean Callery. Can you decipher the message?

RQFHU HPRYH GIURP WKHUR GWKHZ ULWLQ JZDVM XVWDM XPEOH RIOHW
WHUVW KDWZR XOGEH PHDQL QJOHV VLIWK HHQHP BFDSW XUHGL
WLWLV SRVVL EOHWK DWPHV VHQJH UVZRU HWKHI DEULF DVDEH OWZLW
KWKHZ ULWLQ JRQWK HLQVL GHZKH QWKHP HVVDJ HZDVG HOLYH
UHGLW ZDVZU DSSHG DURXQ GDFBO LQGHU LGHQW LFDOL QGLDP HWHUW
RWKHI LUVWR QHDQG FRXOG EHUHDG.

The letters are in groups of five! Word size was not maintained through this cipher! Again with your partner, count and record the number of times each letter occurs in both the dot plot and table below.

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

Use the data you have found to answer the following questions.

1. By comparing the two dot plots, can you make any educated guesses as to which ciphertext letters represent which plaintext letters? Justify your answer.

2. The passage and the message are of different lengths. Now compute the frequency of the ciphertext letters in the message in percentages and record them in the table below.

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

3. Using the table you just completed, what do you notice about this table and the one from the passage? Are they the same? Different? How?

4. In the following table, fill in the ciphertext letter below the plaintext letter it represents.

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

Congratulations! You just discovered the Caesar shift cipher!

Day 5 Lesson Plan

Objective:

Utilize graphing skills and understanding of percentages to aid in the deciphering of a message. Applying number sense to percentages. Identify connections between language and mathematics.

Materials Needed:

From the day before: one "The Letters Count" worksheet per student.

Launch: (Approximately 5 minutes)

Begin by reviewing the findings from the first part of the worksheet by having a pair draw their dot plot on the board, and have another pair complete a letter frequency table on the board.

Explore: (Approximately 15 minutes)

Allow students the time to complete their worksheet. Monitor each group's progress and have some identify the characteristics they discovered between the data they analyzed.

Share: (Approximately 20 minutes)

Once each pair has answered all of the questions on the worksheet, go over them as a class. A key characteristic to identify is that the two dot plots have similar distributions, but the enciphered message plot is shifted three spots to the right. Display the table below, which has the frequency of the letters of the English language as it has been calculated through lengthy studies, from Pincock p.24.

A	B	C	D	E	F	G	H	I	J	K	L	M
8.0	1.5	3.0	3.9	12.5	2.3	1.9	5.5	7.2	0.1	0.7	4.1	2.5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.1	7.6	2.0	0.1	6.1	6.5	9.2	2.7	1.0	1.9	0.2	1.7	0.1

Students should be able to recognize that most shift ciphers can be deciphered using this method if messages are long or if a number of messages are collected. However, frequency analysis will not always work because a person enciphering a message may ensure that the plaintext message does not

reflect the frequency of the English alphabet. An interesting fact is that even though E is the most frequently used letter in English, there is a book that was written entirely without any E's.

Summarize: (Approximately 10 minutes)

Now that students have an understanding of how frequency analysis works, have them describe what the relative frequency of a substitution would most likely look like. Help them to understand that a shift cipher maintains the frequency distribution, only shifted left or right, whereas a substitution cipher will likely have matching frequencies, but the pattern will be random, allowing for only narrowing down the options of plaintext letters that ciphertext letters represent.

Day 6 Lesson Plan

Objective:

Develop student problem-solving through seeking enciphering methods that deter frequency analysis. Provide a basic connection between technology and mathematics through construction of a cipher disk.

Materials Needed:

One cipher disk cutout sheet per student. If classroom is safe for scissors, have students cut out the disks, otherwise have the disks already cut from sheet.

One brass fastener per student.

Launch: (Approximately 5 minutes)

Remind students that devices have been involved with cryptography since ancient Greece. In the 15th century, an innovative enciphering tool was developed by an Italian named Leon Battista Alberti. Today, they will be creating their own version of that tool: the cipher disk. Have an example to show students. With the example, explain that the letters on the outside represent the plaintext letters, and the letters on the inside represent the ciphertext letters. Demonstrate to them how to place the brass fastener through the centers so that the two disks spin around each other.

Explore: (Approximately 25 minutes)

Encourage students to label the spots on the inner disk how they wish, and tell them that the goal of this activity is to create a cipher that is less vulnerable to frequency analysis than substitution or shift ciphers. Also make it clear to students that they should record what settings there cipher disks are at the start of their enciphering, as well as recording any changes that are made and when they occur.

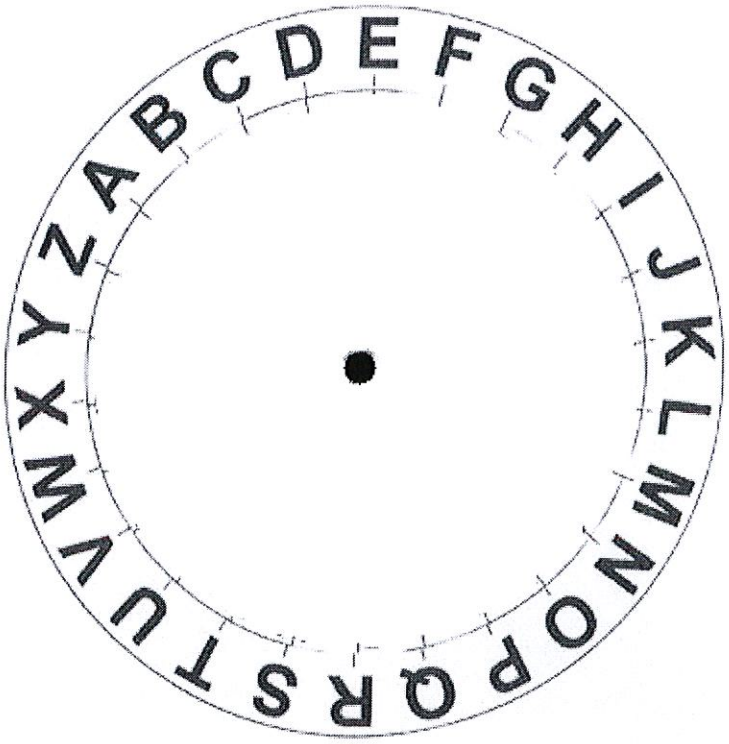
Share: (Approximately 15 minutes)

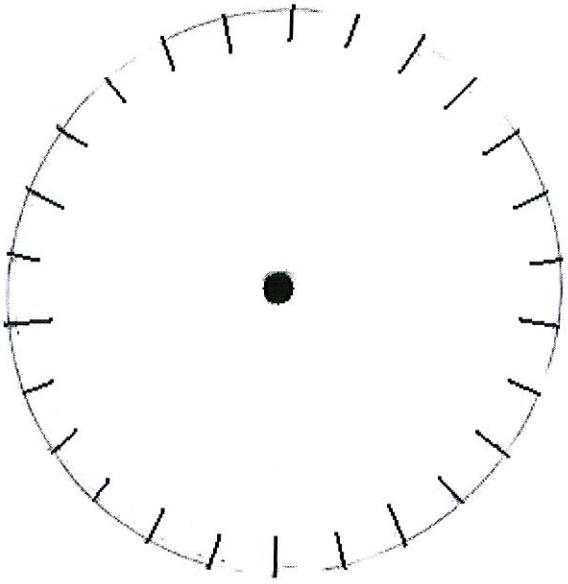
Have students share the different ways they enciphered their messages as well as explain why they believe that frequency analysis will be less useful with their cipher. If students did not spin the inner disk during the enciphering process, they created either a substitution or shift cipher, depending on the

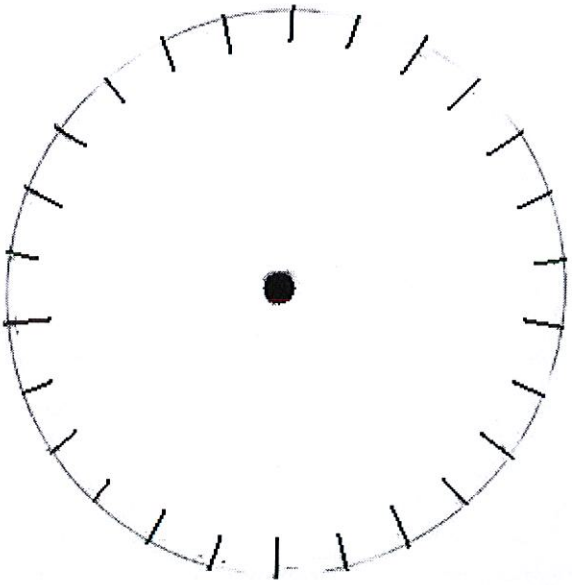
way they constructed their inner disk. Also, if students did not keep track of when they rotated the inner disk and by how far in which direction, then deciphering becomes quite difficult.

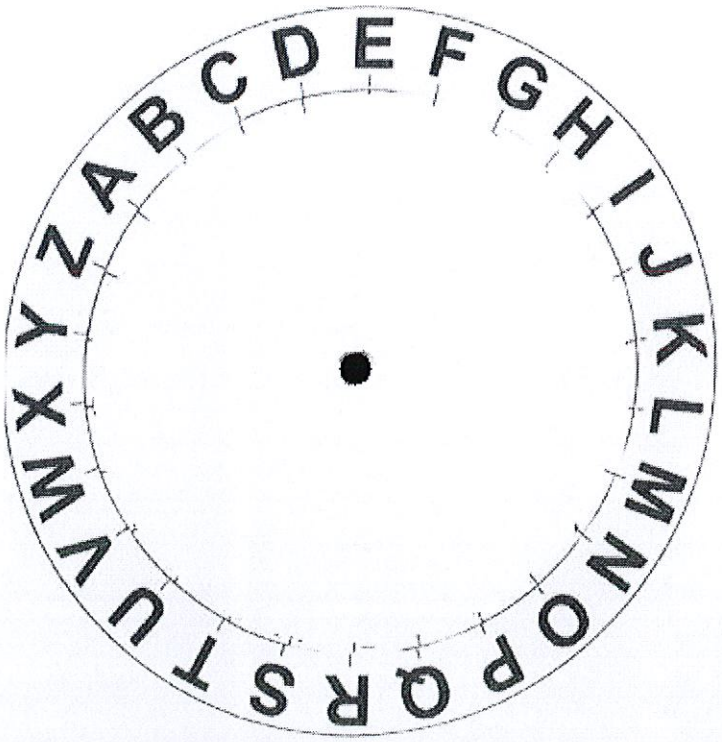
Summarize: (Approximately 5 minutes)

Students should be able to recognize that it is important to have some way of communicating with the receiver when shifts occur, and by how much in which direction. They should also recognize that in order for this method to work, both parties involved with the message will need identical cipher disks.


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

Day 7 Lesson Plan

Objective:

Work with a different representation of the cipher disk. Continue developing communication by having students work in pairs so they can learn how to express their ideas and methods of enciphering.

Materials Needed:

One "Trithemius' or Vigenére's Table" per student.

An overhead of the "Trithemius' or Vigenére's Table".

Launch: (Approximately 15 minutes)

Ask the students about their cipher disks and what is interesting or neat about them. Display the "Trithemius' or Vigenére's Table" to the class and explain that if a cipher disk is created where the inner disk is in alphabetical order, the table represents each possible shift cipher that results. Demonstrate to students how Trithemius used this table to encipher by going down a row for each successive plaintext letter. Next, show the students how Giovan Batista Belaso used a phrase as a key to encipher using the table.

Explore: (Approximately 20 minutes)

For the activity, students should work in pairs. Students should practice with another phrase as a key to encipher a different message. Inform the students that to have an agreed upon phrase between sender and receiver is difficult to keep hidden, especially if it changes regularly. Using the table, they should come up with a key word and use it as a key to encipher another message. Since a word is much shorter than a phrase, it would be easier to communicate discretely, however students must now figure out how to use a key that is shorter than the message itself.

Share: (Approximately 10 minutes)

After students have enciphered a message using a key word, have a few pairs show how they used the key word and the effect that it had on the ciphertext. Try to have groups that used keys of different lengths present their ciphers.

Summarize: (Approximately 5 minutes)

A few key ideas to make sure the students see are that the longer the key word, the more plaintext letters a ciphertext letter may represent. Frequency analysis is less viable against a cipher using the table, which provides an advantage over shift or substitution ciphers.

Trithemius' or Vigenére's Table

	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

Day 8 Lesson Plan

Objective:

Continue developing problem-solving skills as well as communication through collaboration.

Materials Needed:

From the day before: one "Trithemius' or Vigenére's Table" per student.

Note-card sized slip with two autokey ciphers and the first letter of the key.

Launch: (Approximately 15 minutes)

Review the methods used by Trithemius and Belaso. Tell the students that the work they did with key words was first developed by Blaise de Vigenére in the 16th century. A cipher that he developed that is even less susceptible to frequency analysis is his autokey cipher. Explain that an autokey cipher is a cipher that uses the Vigenére table where the key is actually the plaintext or the ciphertext itself. Work with the class to decipher a message sent where the first letter of the key is an agreed upon letter between the sender and receiver and the rest of the key is the ciphertext.

Explore: (Approximately 20 minutes)

Have students divide into pairs. Pass out the slips for students to begin deciphering the messages where the first is an autokey cipher using the ciphertext for the key, and the second is an autokey cipher using the plaintext as the key. Once students have completed this, they should create two messages using autokey ciphers: one using the plaintext for the key, the other using the ciphertext.

Share: (Approximately 5 minutes)

A few pairs should show the class the autokey ciphers that they created. Be sure to have at least one autokey using the plaintext as the key shown to the class.

Summarize: (Approximately 10 minutes)

Discuss with students why the autokey is more difficult to crack using frequency analysis. A main point to bring up is that when using a key word, if the length of a key is determined, say it is found to be six

letters long, then someone who has intercepted messages can look at the groups of every sixth letter, and can apply frequency analysis to each of these groups. This is because each letter of the key word represents a specific shift cipher, and therefore the groups containing every sixth letter are all enciphered using the same shift cipher.

Name _____

Cryptography Quest

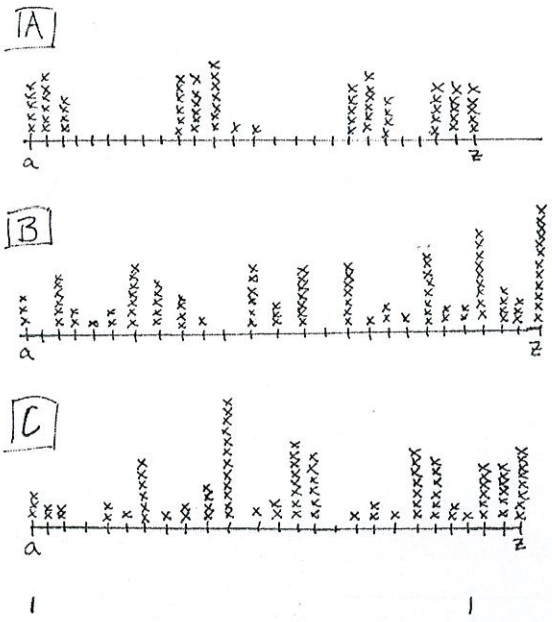
Be sure to answer all questions fully. Provide brief explanations of how you performed the necessary operations where appropriate. Make sure you show your work!

1. Decipher the following message. It was enciphered using a rail-fence cipher with an unknown number of rows.

KEUTE ODOKE PPHGO WR

Deciphered message: _____

2. Recall that frequency analysis is a key tool to use when identifying what type of cipher was used to encipher a message. Place the letter of the frequency distribution next to the type of cipher that it best fits.



___ Substitution cipher

___ Shift cipher

___ Type of cipher cannot be determined

Cryptography Quest page 2

3. The following cipher is an autokey cipher. Refer to the Trithemius table handout to aid in deciphering the message. The key to this message begins with the letter M, and the plaintext provides the rest of the key.

YMTAY LFPW

Deciphered message: _____

4. Use your cipher disk that you constructed to encipher the following message. Be sure to identify and utilize at least one method with which you can deter frequency analysis of your cipher. Be specific when describing how you enciphered the message.

"seek the treasure after midnight"

Method used to encipher message:

Final message sent: _____

Name KEY

Cryptography Quest

Be sure to answer all questions fully. Provide brief explanations of how you performed the necessary operations where appropriate. Make sure you show your work!

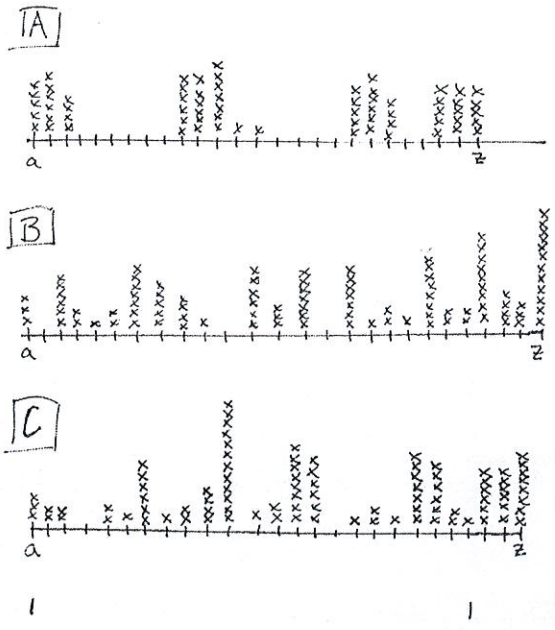
1. Decipher the following message. It was enciphered using a rail-fence cipher with an unknown number of rows.

KEUTE ODOKE PPHGO WR

Work may vary.
The cipher used was a two-row rail fence cipher.

Deciphered message: Keep up the good work

2. Recall that frequency analysis is a key tool to use when identifying what type of cipher was used to encipher a message. Place the letter of the frequency distribution next to the type of cipher that it best fits.



_B_ Substitution cipher

_C_ Shift cipher

_A_ Type of cipher cannot be determined

Cryptography Quest page 2

3. The following cipher is an autokey cipher. Refer to the Trithemius table handout to aid in deciphering the message. The key to this message begins with the letter M, and the plaintext provides the rest of the key.

YMTAY LFPW

Key:	M	M	A	T	H	R	U	L	E
Plaintext:	M	A	T	H	R	U	L	E	S
Ciphertext:	Y	M	T	A	Y	L	F	P	W

Deciphered message: Math Rules!!!

4. Use your cipher disk that you constructed to encipher the following message. Be sure to identify and utilize at least one method with which you can deter frequency analysis of your cipher. Be specific when describing how you enciphered the message.

"seek the treasure after midnight"

Method used to encipher message:

Answers may vary. The first part of their solution should be to identify the starting position of their cipher disk. Students should include at least one turn of their inner disk during the enciphering process. They should be specific about how far and in which direction the shift occurs, as well as when this happens.

If students have created their own cipher disks, have them attach their disks to their test before handing it in. If the disks are pre-made and identical, have a cipher disk on hand to check results.

Final message sent: (Answers will vary.)

High School Cryptography Outline

Days: 10

Lesson plan format: Launch, Explore, Share, Summarize

Day 1:
- Introduction to cryptography
- Students begin working with the Caesar cipher
- Worksheet: "Caesar's Cipher"

Day 2:
- Students begin analyzing the Caesar cipher using numerical values for letters
- Introduction to shift ciphers
- Begin working with modular arithmetic
- Worksheet: "Cipher Time"
- NOTE: This lesson may overflow to the next day depending on the speed of the class. Adjust schedule as necessary to accommodate if this happens. Ninth day is available as an outlet if the lessons extend beyond their allotted times.

Day 3:
- Deciphering shift ciphers
- Reversing enciphering operations in modular arithmetic
- Worksheet: "Let's Decipher"

Day 4:
- Deciphering substitution ciphers
- Students apply problem-solving strategies
- Begin to address differences and similarities between substitution and shift ciphers
- Worksheet: "Intercepted Messages!"

Day 5:
- Continue considering differences between the two types of ciphers
- Students will use frequency distributions to analyze a cipher
- Discovering characteristics about shift ciphers and the Caesar cipher specifically
- Worksheet: "The Letters Count"

Day 6:
- Work with affine ciphers which are more complex than shift ciphers
- Continue developing understanding of modular arithmetic
- Opportunities for students to share their understanding of operations and to be able to communicate mathematical ideas
- Worksheet: "An Affinity for Ciphers"

Day 7:

- Develop problem-solving skills through deciphering affine ciphers
- Continue working with modular arithmetic
- Worksheet: "Deciphering the Affine"

Day 8:

- Deciphering a message using the prior knowledge that students have
- Developing problem-skills through dealing with a situation
- Connections between mathematics and the English language
- Worksheet: "Calling All Cryptographers!"

Day 9:

- Day for overflow of lessons
- Review of ciphers and worksheets
- Possible extra-credit: Have a few enciphered messages that students can work on without knowing what cipher was used.

Day 10:

- Test: Students must: encipher a message using a shift cipher of a given shift size, ciphertext must be written using numerical values; given a ciphertext message, decipher the message and state both the enciphering congruence and the deciphering congruence; create an affine cipher and encipher a given message using it, also identify what characteristics their affine cipher has that makes it work
- Test: "Cryptography Quest"

Day 1 Lesson Plan

Objective:

Introduce students to cryptography. Use knowledge of numbers and operations to begin working with shift ciphers. Develop communication between students by working with partners and sharing ideas with the rest of class.

Materials Needed:

One "Caesar's Cipher" worksheet per student.

Launch: (Approximately 5 minutes)

Give a brief introduction of cryptography to students. Touch on points such as the fact that it has been used since 1500 BC, and its role in society is increasing everyday. To begin with, students will be working with the cipher developed by Emperor Julius Caesar to communicate secretly with his allies and officers. Hand out a "Caesar's Cipher" worksheet to each student. Have them work with a partner on the worksheet.

Explore: (Approximately 35 minutes)

Allow students to work with the cipher and develop an understanding of how the cipher works. The worksheet has them practice enciphering messages with the Caesar cipher. It also asks questions to provoke their thinking about how to increase the security of enciphered messages. Circulate through the room and provide insights and ask questions to help the students grasp the ideas being presented through the worksheet.

Share: (Approximately 10 minutes)

Once students have completed the worksheet, have the class discuss the cipher as a group. Ask questions about the difficulty of enciphering or deciphering with the Caesar cipher. Also ask what they found when using a shift cipher of a different size. Have a few groups write their enciphered message on the board that they chose the shift size for. As a class, analyze the messages and remark on any differences

or similarities used. Encourage students to share other ideas on how to increase the security of messages that are sent.

Summarize: (Approximately 0 minutes)

The summarization of the lesson should occur during the Share portion of this lesson. Key ideas are that all shift ciphers are similar in the fact that they do not change the order in which the letters of the alphabet appear, merely which letter begins the alphabet. Later they will explore ciphers that will change the order of the letters.

NOTE: This lesson is designed to take one day. Depending on the level of the class and their ability to stay on task, part of a second day may be needed to complete this lesson.

Name ____________________

Caesar's Cipher

Julius Caesar, the Emperor of Rome, devised a system to enable secret communication between himself, his military officers and political allies. Thus he created what has come to be known as the Caesar cipher.

To encipher his messages, Caesar would replace each letter of his message with the letter three places further in the alphabet. For example, A is replaced with D, B with E and so forth. X, Y, and Z are replaced with A, B and C respectively.

1. Using this system, what letter would H be replaced with? ______

2. Encipher the following message using Caesar's cipher:

"Do not give up hope. Reinforcements will arrive shortly."

_ _   _ _ _   _ _ _ _   _ _   _ _ _ _ .   _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _   _ _ _ _ _ _   _ _ _ _ _ _ _ .

3. What are some initial observations you can make about the enciphered message? If the enemy captured the messenger, what would they likely make of this message? ____________________

____

____

____

4. Are there any characteristics of the enciphered message that may give the enemy an idea of how to possibly crack the cipher? What are they? ____________________

____

____

5. Can you think of any method of sending messages that would make it harder for people who intercepted the message to figure out what it says? What would *you* do to make the message harder to crack? ____________________

____

____

____

Caesar's Cipher page 2

Now that you know how to encipher using Caesar's cipher, let's break it! Enciphering the message means to replace the original message, or plaintext, with the letters of the cipher, or ciphertext. Use your knowledge of the cipher used by Caesar to answer the following questions.

1. What plaintext letter does H replace in a message? _____ What letter does Y replace? ____

2. Decipher the word VHFUHW: _____

3. The following message has been intercepted from an expert on ciphers. Our sources say that this person was not very concerned about others reading it, so it was enciphered using the Caesar cipher. Please decipher the message to reveal its content.

WKH FDHVDU FLSKHU LV NQRZQ DV D VKLIW FLSKHU.

___ _____ _____ __ _____ __ _

_____ _____ .

Shift ciphers replace plaintext letters with ciphertext letters that are a certain number of places further in the alphabet. The Caesar cipher has a shift size of +3, since each letter is replaced with the letter three places later.

4. If a shift cipher with a shift size of +12 were used, what letter would replace S? ____

What letter would J replace? ____

5. Decide on a shift size that is greater than 4. Using a shift cipher with that shift size, encipher the message: Shift size: _____

"Civilizations will rise and fall, but cryptography will remain"

_____

_____

Be prepared to share your enciphered message with the class. Note any interesting observations you make when other shift sizes are used.

Name KEY

Caesar's Cipher

Julius Caesar, the Emperor of Rome, devised a system to enable secret communication between himself, his military officers and political allies. Thus he created what has come to be known as the Caesar cipher.

To encipher his messages, Caesar would replace each letter of his message with the letter three places further in the alphabet. For example, A is replaced with D, B with E and so forth. X, Y, and Z are replaced with A, B and C respectively.

1. Using this system, what letter would H be replaced with? K

2. Encipher the following message using Caesar's cipher:

"Do not give up hope. Reinforcements will arrive shortly."

G R Q R W J L Y H X S K R S H U H L Q I R U F H P H Q W V

Z L O O D U U L Y H V K L U W O B .

3. What are some initial observations you can make about the enciphered message? If the enemy captured the messenger, what would they likely make of this message? Answers may vary. Key observations are that the message itself does not make sense because none of the words are actual words. They would likely realize that it is a enciphered message because the word sizes are still intact.

4. Are there any characteristics of the enciphered message that may give the enemy an idea of how to possibly crack the cipher? What are they? A characteristic that is likely to give the enemy aid in cracking the message is that the word sizes are intact. They can make guesses as to what the smaller two-letter words are, and begin to decipher them in that manner.

5. Can you think of any method of sending messages that would make it harder for people who intercepted the message to figure out what it says? What would *you* do to make the message harder to crack? Answers may vary. One method would be to change the grouping of the letters, such as either putting them in random sized groups, or having one uniform size such as groups of five letters.

Caesar's Cipher page 2

Now that you know how to encipher using Caesar's cipher, let's break it! Enciphering the message means to replace the original message, or plaintext, with the letters of the cipher, or ciphertext. Use your knowledge of the cipher used by Caesar to answer the following questions.

1. What plaintext letter does H replace in a message? _E___ What letter does Y replace? __V__
2. Decipher the word VHFUHW: __secret____
3. The following message has been intercepted from an expert on ciphers. Our sources say that this person was not very concerned about others reading it, so it was enciphered using the Caesar cipher. Please decipher the message to reveal its content.

WKH FDHVDU FLSKHU LV NQRZQ DV D VKLIW FLSKHU.

THE CAESAR CIPHER IS KNOWN AS A SHIFT CIPHER.

Shift ciphers replace plaintext letters with ciphertext letters that are a certain number of places further in the alphabet. The Caesar cipher has a shift size of +3, since each letter is replaced with the letter three places later.

4. If a shift cipher with a shift size of +12 were used, what letter would replace S? __E__
   What letter would J replace? __X__
5. Decide on a shift size that is greater than 4. Using a shift cipher with that shift size, encipher the message: Shift size: _____

"Civilizations will rise and fall, but cryptography will remain"

Answers will vary.

Be prepared to share your enciphered message with the class. Note any interesting observations you make when other shift sizes are used.

Day 2 Lesson Plan

Objective:

Address the Numbers and Operations standard of NCTM by working with modular arithmetic. Develop communication through working with partners. Increase problem-solving and thinking skills by posing conjectures.

Materials Needed:

One "Cipher Time" worksheet per student.

Launch: (Approximately 5 minutes)

Briefly review the lesson from the previous day with the students. Review that the Caesar cipher is a shift cipher and those are the ciphers that are going to be worked with today. Hand out the worksheets to students and have them pair up with a partner.

Explore: (Approximately 35 minutes)

While students are working on their worksheets, circulate the room and provide assistance as necessary. Have students work up to question 9, completing the front page, and have the class gather together to go over their answers and to clear up and questions that they may have. Next, have students work through question 13, and have the class gather together again to go over the new concepts that have been introduced. Once this is done, have students complete their worksheet.

Share: (Approximately 8 minutes)

After students have finished, have them share what they created as the congruence for any shift cipher. Discuss the different solutions presented and have the students identify why they do or do not work. Help students to see that the shift size itself is important when considering developing a congruence to use for enciphering messages.

Summarize: (Approximately 2 minutes)

Share with students the correct expression $C \equiv P + k \pmod{26}$. Explain that all shift ciphers are enciphered using this equation, where k represents the size of the shift.

Note: Lesson may take more than one class time. Combined with the previous day's lesson, the two potentially could take three days to complete rather than 2.

Name _____

Cipher Time!

For many ciphers, numbers are sent as the ciphertext rather than letters. The most common numerical values for letters are A having value 0, B having value 1, up to Z having value 25. In the table below, the letters of the alphabet are listed out with their respective numerical values below them.

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

When using the numerical values of letters, spacing is important:1 4 can be read as BE whereas 14 is O.

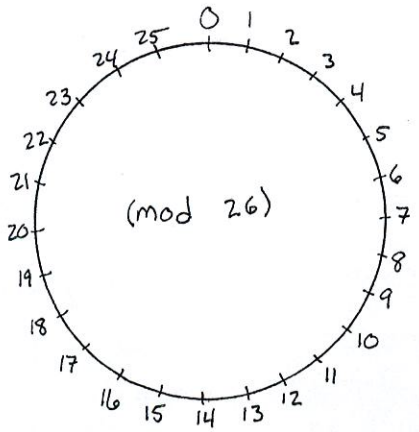
1. Using the Caesar cipher, encipher the word "Caesar" with letters for the ciphertext: _____

2. Now write out the word "Caesar" replacing the letters with their numerical values: _____

3. Add 3 to each number above to create a new ciphertext: _____

4. With the ciphertext created in the previous question, replace the numbers with their corresponding letters as shown in the table above: _____ Have you seen this message before? ____

Shift cipher messages can be enciphered and deciphered using their numerical values with a type of mathematics called *modular arithmetic*. For the ciphers we will be exploring, the modulus we will be working with is 26. This means that our messages will only have 0 through 25 as values. The circle below is a tool that can be used to aid in finding values of letter in modulo 26. Use the circle to answer the following questions. Be prepared to share your results with the class.



5. Addition can be simulated on the circle by moving in which direction? _____

6. What is the value of 3 + 4 in modulus 26? _____

7. What is the value of 18 – 5 in modulus 26? _____

Note: Another way of expressing these congruencies is to place (mod 26) on the right side of the expression to signify if the answer is or should be given in a certain modulo.

Example: $12 + 4 \equiv 16 \pmod{26}$ or $12 + 4 \pmod{26} \equiv ?$

8. a) $23 - 10 \pmod{26} \equiv$ _____ **b)** $5 + 20 \pmod{26} \equiv$ _____

9. a) $6 - 10 \pmod{26} \equiv$ _____ **c)** $23 + 7 \pmod{26} \equiv$ _____

10. What value does 30 have in modulo 26? ____ (Hint: Can you write 30 as an equation using addition or subtraction of two numbers less than 26?)

11. Solve: 37 (mod 26) ≡ ____

12. What value does -3 have in modulo 26? _____

13. Solve: -15 (mod 26) ≡ _____

Modular arithmetic is often called clock arithmetic. This is because the values of numbers in a certain modulus can be determined by finding its corresponding place on a circle like the one above, similar to a clock face.

In the congruence expressions we will see throughout our exploration of cryptography, the letter P will stand for the numerical value of a plaintext letter, and the letter C will stand for the numerical value of a ciphertext letter.

14. Using the congruence $C \equiv P + 5 \pmod{26}$, encipher the word "math": _____

15. Encipher the following message using the congruence $C \equiv P + 13 \pmod{26}$:

"Beware! The milk man is a spy!"

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

____ ____ ____ ____ ____ ____ ____ ____ ____

16. Given the information that you are to encipher a message using a shift size of 10, write a congruence expression to represent this: $C \equiv$

Shift ciphers use a key, k, where $0 \leq k \leq 25$. Can you write a congruence expression that could be applied to any shift cipher where the key, k, represents the size of the shift?

Name KEY

Cipher Time!

For many ciphers, numbers are sent as the ciphertext rather than letters. The most common numerical values for letters are A having value 0, B having value 1, up to Z having value 25. In the table below, the letters of the alphabet are listed out with their respective numerical values below them.

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

When using the numerical values of letters, spacing is important:1 4 can be read as BE whereas 14 is O.

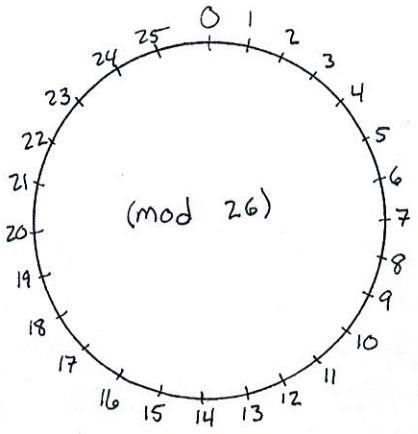
1. Using the Caesar cipher, encipher the word "Caesar" with letters for the ciphertext: FDHVDU

2. Now write out the word "Caesar" replacing the letters with their numerical values: 2 0 4 18 0 17

3. Add 3 to each number above to create a new ciphertext: 5 3 7 21 3 20

4. With the ciphertext created in the previous question, replace the numbers with their corresponding letters as shown in the table above: FDHVDU Have you seen this message before? Yes!

Shift cipher messages can be enciphered and deciphered using their numerical values with a type of mathematics called *modular arithmetic*. For the ciphers we will be exploring, the modulus we will be working with is 26. This means that our messages will only have 0 through 25 as values. The circle below is a tool that can be used to aid in finding values of letter in modulo 26. Use the circle to answer the following questions. Be prepared to share your results with the class.



1. Addition can be simulated on the circle by moving in which direction? To the right

1. What is the value of 3 + 4 in modulus 26? 7

2. What is the value of 18 – 5 in modulus 26? 13

Note: Another way of expressing these congruencies is to place (mod 26) on the right side of the expression to signify if the answer is or should be given in a certain modulo.

Example: $12 + 4 \equiv 16 \pmod{26}$ or $12 + 4 \pmod{26} \equiv ?$

3. a) $23 - 10 \pmod{26} \equiv$ 13 **b)** $5 + 20 \pmod{26} \equiv$ 25

4. a) $6 - 10 \pmod{26} \equiv$ 22 **c)** $23 + 7 \pmod{26} \equiv$ 4

5. What value does 31 have in modulo 26? __5__ (Hint: Can you write 30 as an equation using addition or subtraction of two numbers less than 26?)

6. Solve: 37 (mod 26) ≡ __11__

7. What value does -3 have in modulo 26? __23__

8. Solve: -15 (mod 26) ≡ __11__

Modular arithmetic is often called clock arithmetic. This is because the values of numbers in a certain modulus can be determined by finding its corresponding place on a circle like the one above, similar to a clock face.

In the congruence expressions we will see throughout our exploration of cryptography, the letter P will stand for the numerical value of a plaintext letter, and the letter C will stand for the numerical value of a ciphertext letter.

5. Using the congruence $C \equiv P + 5 \pmod{26}$, encipher the word "math": __17 5 24 12__

6. Encipher the following message using the congruence $C \equiv P + 13 \pmod{26}$ using numerical values:

"Beware! The milk man is a spy!"

__14__ __18__ __9__ __13__ __4__ __17__ __6__ __20__ __17__ __25__ __21__ __24__ __23__

__25__ __13__ __0__ __21__ __5__ __13__ __5__ __2__ __11__

7. Given the information that you are to encipher a message using a shift size of 10, write a congruence expression to represent this: $C \equiv P + 10 \pmod{26}$

Shift ciphers use a key, k, where $0 \leq k \leq 25$. Can you write a congruence expression that could be applied to any shift cipher where the key, k, represents the size of the shift?

$$C \equiv P + k \pmod{26}$$

Day 3 Lesson Plan

Objective:

Develop number sense through working with modular arithmetic. Increase problem-solving abilities through deciphering messages and developing congruence expressions to use to decipher.

Materials Needed:

One "Let's Decipher" worksheet per student.

Launch: (Approximately 5 minutes)

Review the information developed from the day before. Inform the students that now they need to find a way to decipher messages once they are enciphered. Through working with ciphers, they will create a way to reverse the enciphering process to reproduce the message in plaintext. Hand out the "Let's Decipher" worksheet and have students work in pairs.

Explore: (Approximately 30 minutes)

Allow students to complete the worksheet. Move throughout the room and ask prompting questions to students that are having difficulties. Make note of which students are doing quite well so that when it comes time to share their results, you can have a group or two present their findings that are the sought after outcome.

Share: (Approximately 10 minutes)

Have students share what they found while doing their worksheets. Go through each of the questions with them and address any problems that they encountered on the way. After the questions have been reviewed, have a few groups present the congruence they developed to decipher any shift cipher with key k. Have the groups explain how they came to this conclusion and work with the class to ensure that everyone saw how this was developed.

Summarize: (Approximately 5 minutes)

Point out to students that as long as k is between 0 and 25, the congruence $P \equiv C - k \pmod{26}$ can be used because k is less than 26. If time allows, ask student what would happen if you were to add 26 to the right side of the expression. Would you need to do this to both sides? Is this expression equivalent to the one before? Through this, students should see that adding or subtracting 26 to either side does not disrupt the balance since $26 \equiv 0 \pmod{26}$.

Name _____

Let's Decipher!

Now that you are getting better and better at enciphering using shift ciphers, let's figure out how to decipher messages that we receive. In the table below, write out the numerical value for each letter to help with the process.

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

1. First, using the Caesar cipher, decipher the word "PDWKHPDWLFV": _____

2. Rewrite the ciphertext word above by replacing the letters with their numerical values:

_____

3. Rewrite the deciphered word above by replacing the letters with their numerical values:

_____

4. Using the two words above, can you develop a congruence that can be used to decipher the ciphertext word above? If so, write the expression relating P to C below.

$P \equiv$ _____

(Remember: the Caesar cipher is a shift cipher with shift size _____)

5. With the expression above, adjust it so that it may be used to decipher a message that was sent using a shift cipher with shift size $k = 9$. Use it to decipher the message below.

2 16 13 0 13 9 0 13 1 23 21 13 11 17 24 16 13 0 1 2 16 9 2 16 9 4 13
22 13 4 13 0 10 13 13 22 10 0 23 19 13 22 10 7 13 6 24 13 0 2 1

Develop an expression to decipher a shift cipher with key k: $P \equiv$ _____

Name KEY

Let's Decipher!

Now that you are getting better and better at enciphering using shift ciphers, let's figure out how to decipher messages that we receive. In the table below, write out the numerical value for each letter to help with the process.

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

1. First, using the Caesar cipher, decipher the word "PDWKHPDWLFV": mathematics

2. Rewrite the ciphertext word above by replacing the letters with their numerical values:

15 3 22 10 7 15 3 22 11 5 21

3. Rewrite the deciphered word above by replacing the letters with their numerical values:

12 0 19 7 4 12 0 19 8 2 18

4. Using the two words above, can you develop a congruence that can be used to decipher the ciphertext word above? If so, write the expression relating P to C below in modulo 26.

$P \equiv C - 3 \pmod{26}$

(Remember: the Caesar cipher is a shift cipher with shift size 3)

5. With the expression above, adjust it so that it may be used to decipher a message that was sent using a shift cipher with shift size $k = 9$. Use it to decipher the message below.

2 16 13 0 13 9 0 13 1 23 21 13 11 17 24 16 13 0 1 2 16 9 2 16 9 4 13
22 13 4 13 0 10 13 13 22 10 0 23 19 13 22 10 7 13 6 24 13 0 2 1

"there are some ciphers that have never been broken by experts"

Develop an expression to decipher a shift cipher with key k: $P \equiv C - k \pmod{26}$

Day 4 Lesson Plan

Objective:

To encourage problem solving and communication by having students solve substitution ciphers with partners.

Materials Needed:

One "Intercepted Messages!" sheet per student.

Launch: (Approximately 5 minutes)

Inform the students that you have just received two messages that the National Security Agency, one of the top cryptological organizations, needs help deciphering. Let them know that the two messages were enciphered using substitution ciphers. This means that each letter has been replaced by a different letter in the alphabet, such as X is now written as A. Also, let them know that the order of the letters and size of the words have not been altered.

Explore: (Approximately 35 minutes)

For this lesson, the Explore and Share portions are intermixed. Have the students work on the first message. Walk around the room to monitor progress, and provide minimal assistance. If a pair is having difficulties, ask them what certain words may be, such as two letter words, or words that occur more than once in the message. Allow approximately 15 minutes for the first message then have groups share what they found the answer to be, and how they went about deciphering the message. Encourage groups to use refined methods to decipher the second message. Allow about 10 minutes for this then have groups share what they found the message to say as well as how they deciphered it.

Share: (Approximately 0 minutes)

Combined with Explore portion of lesson.

Summarize: (Approximately 10 minutes)

Discuss with students different methods for deciphering substitution ciphers, such as making logical guesses based on word size or letter placement. For example, if the message as a word such as KWWO, it is a reasonable assumption to make that the WW represents EE or OO like in the words seen or took. Using logical approaches to these types of ciphers produce good results. Ask the students what they could do if the ciphertext letters were grouped differently than the sizes of the original words. This will be addressed the next day.

Name_____

INTERCEPTED MESSAGES!!!

Message 1:

X-Z-T-V Z-A E-Y-Z V-L-Y-C-S-C-E-X I-E E-Y-V K-I-E-C-Z-K-I-B

F-G-O-J-E-Z-B-Z-M-C-F T-H-X-V-R-T K-V-I-G S-I-B-E-C-T-Z-G-V

F-I-K S-V X-V-V-K Z-K E-Y-V D-Z-G-B-Q D-C-Q-V D-V-S.

Wait until instructed to continue on to the second message.

Message 2:

H-R-K-N-D J-D-N-K G-R D-N-O-K D-B-G-N-I-I-Z-G-N

U-Z-H-G-J-A-N-D E-B-H-F G-R N-B-A-G-W B-O-K G-R U-I-B-V

E-B-H-F H-R-L-U-B-H-G K-Z-D-F-D B-A-N B-H-G-J-B-I-I-B B-E-I-N

G-R H-R-A-A-N-H-G N-A-A-R-A-D.

Name **Key**

INTERCEPTED MESSAGES!!!

Message 1:

X-Z-T-V Z-A E-Y-Z V-L-Y-C-S-C-E-X I-E E-Y-V K-I-E-C-Z-K-I-B
F-G-O-J-E-Z-B-Z-M-C-F T-H-X-V-R-T K-V-I-G S-I-B-E-C-T-Z-G-V
F-I-K S-V X-V-V-K Z-K E-Y-V D-Z-G-B-Q D-C-Q-V D-V-S.

Some of the exhibits at the national cryptological museum near Baltimore can be seen on the world wide web.

Message 2:

H-R-K-N-D J-D-N-K G-R D-N-O-K D-B-G-N-I-I-Z-G-N
U-Z-H-G-J-A-N-D E-B-H-F G-R N-B-A-G-W B-O-K G-R U-I-B-V
E-B-H-F H-R-L-U-B-H-G K-Z-D-F-D B-A-N B-H-G-J-B-I-I-B B-E-I-N
G-R H-R-A-A-N-H-G N-A-A-R-A-D.

Codes used to send satellite pictures back to Earth and to play back compact disks are actually able to correct errors.

Source: COMAP, Inc. Mathematics: Modeling our World. W. H. Freeman and Company. New York: 1998, p. 56.

Day 5 Lesson Plan

Objective:

Utilize graphing skills and understanding of percentages to aid in the deciphering of a message. Students will use number sense when both calculating and comparing percentages. Identify connections between language and mathematics.

Materials Needed:

One "The Letters Count" worksheet per student.

Launch: (Approximately 5 minutes)

Review the findings of the previous day on substitution ciphers. Share with the students that many ciphers are sent with the ciphertext in groups of letters, rather than in their original words. Today they will analyze the English language, and use this knowledge to decipher a message.

Explore: (Approximately 30 minutes)

After each student has received a "The Letters Count" worksheet, they should find a partner to work with. The worksheet involves counting the letters of a passage, and then analyzing their frequency. Next, students analyzed an enciphered message using the same method, and use their findings to aid in deciphering the message. Allow them the class period to work on these findings. During this time, circulate through the room providing insight and encouragement where necessary.

Share: (Approximately 5 minutes)

Once the pairs seem to have all completed the first page of the worksheet, have one pair draw their dot plot on the board. Have another pair fill in a table with the percentages up on the board.

Once each pair has answered all of the questions on the worksheet, go over them as a class. A key characteristic to identify is that the two dot plots have similar distributions, but the enciphered message plot is shifted three spots to the right. Display the table below, which has the frequency of the letters of the English language as it has been calculated through lengthy studies, from Pincock p.24.

A	B	C	D	E	F	G	H	I	J	K	L	M
8.0	1.5	3.0	3.9	12.5	2.3	1.9	5.5	7.2	0.1	0.7	4.1	2.5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.1	7.6	2.0	0.1	6.1	6.5	9.2	2.7	1.0	1.9	0.2	1.7	0.1

Students should be able to recognize that most shift ciphers can be deciphered using this method if messages are long or if a number of messages are collected. However, frequency analysis will not always work because a person enciphering a message may ensure that the plaintext message does not reflect the frequency of the English alphabet. An interesting fact is that even though E is the most frequently used letter in English, there is a book that was written entirely without any E's.

Summarize: (Approximately 10 minutes)

Now that students have an understanding of how frequency analysis works, have them describe what the relative frequency of a substitution would most likely look like. Help them to understand that a shift cipher maintains the frequency distribution, only shifted left or right, whereas a substitution cipher will likely have matching frequencies, but the pattern will be random, allowing for only narrowing down the options of plaintext letters that ciphertext letters represent.

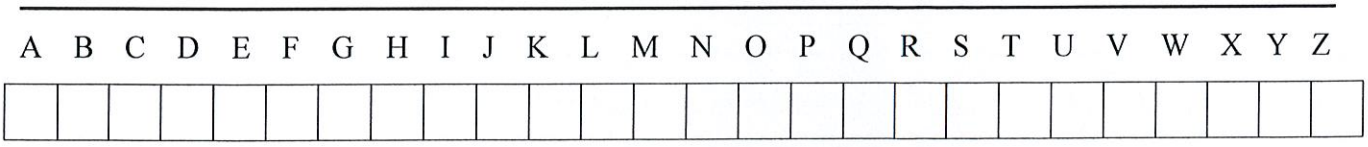
Name_____

The Letters Count

Read the passage below from Codes and Ciphers by Sean Callery.

"The scytale is the earliest known piece of cryptographic equipment, dating from fifth-century BC Greece. Probably first used by the Spartans to carry messages around the battlefield, it is a simple transposition machine. A piece of parchment similar to a ribbon was wrapped around a cylinder, such as a wooden staff. The message was then written unencrypted onto the coiled paper" (Callery 64).

Once you have read through it once, work with a partner to count how many times each letter of the alphabet appears in the text. Record your findings on the dot plot below. Record the number of times each letter occurs in the space in the table below it.



Add up the numbers from the table to find the total number of letters in the passage. Find the frequency that each letter occurs as a percentage of the passage. Record these calculations in the table below.

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

The Letters Still Count

The following message is enciphered text from Codes and Ciphers by Sean Callery. Can you decipher the message?

RQFHU HPRYH GIURP WKHUR GWKHZ ULWLQ JZDVM XVWDM XPEOH RIOHW
WHUVW KDWZR XOGEH PHDQL QJOHV VLIWK HHQHP BFDSW XUHGL
WLWLV SRVVL EOHWK DWPHV VHQJH UVZRU HWKHI DEULF DVDEH OWZLW
KWKHZ ULWLQ JRQWK HLQVL GHZKH QWKHP HVVDJ HZDVG HOLYH
UHGLW ZDVZU DSSHG DURXQ GDFBO LQGHU LGHQW LFDOL QGLDP HWHUW
RWKHI LUVWR QHDQG FRXOG EHUHDG.

The letters are in groups of five! Word size was not maintained through this cipher! Again with your partner, count and record the number of times each letter occurs in both the dot plot and table below.

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

Use the data you have found to answer the following questions.

1. By comparing the two dot plots, can you make any educated guesses as to which ciphertext letters represent which plaintext letters? Justify your answer.

2. The passage and the message are of different lengths. Now compute the frequency of the ciphertext letters in the message in percentages and record them in the table below.

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

3. Using the table you just completed, what do you notice about this table and the one from the passage? Are they the same? Different? How?

4. In the following table , fill in the ciphertext letter below the plaintext letter it represents.

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

Can you identify the cipher that you just used frequency analysis on?

Day 6 Lesson Plan

Objective:

Students will further their number sense and understanding of operations by exploring increasingly complex congruencies and operations in modular arithmetic.

Materials Needed:

One "An Affinity for Ciphers" worksheet per student.

Launch: (Approximately 5 minutes)

Remind the students of the fact that the frequency distribution of a shift cipher matches that of the English language, only shifted to the right as far as the shift length. Now they will begin working with ciphers whose frequency distribution does not just shift the pattern to a different position. These are the affine ciphers. Hand out "An Affinity for Ciphers" worksheet to each student. Again, have them work in pairs.

Explore: (Approximately 30 minutes)

Allow students time to complete the worksheet. As they are working with their partners, circulate through the room and provide prompting questions where necessary. Avoid providing students with answers. Help them by asking them questions about what knowledge they already have that may be applied to the new situation to aid them in developing their problem-solving skills.

Share: (Approximately 10 minutes)

Once all the pairs have completed their worksheet, have them present their findings. All answers to the first two questions should be the same. If there are differences, address them and aid the students in finding where miscalculations may have occurred. The results of question 3 may vary. Have one or two groups whose cipher they created that worked show their cipher and the message to the class. Also have one or two whose did not work present their findings as well and why they believe it did not work. This will lead into question 4, where the congruence did not work to encipher the message because it enciphered two different plaintext letters as the same ciphertext letter. Engage the class in a short

discussion on why these ciphers did not work and why the first two did. They should analyze the relationship between the various values of a to formulate a theory on why the ciphers had varying degrees of success.

Summarize: (Approximately 5 minutes)

The key characteristic of an affine cipher is that a and 26 must be relatively prime. If they are not, a cipher such as seen in question 4 will result. In that example, 6 and 26 have a common divisor of 2.

NOTE: This lesson may extend beyond one class period depending on the level of students. It may need to be completed the next day, thus resulting in a slight shift of the remaining lessons. To compensate for this, divide the activities so that each is started the second half of one class period and finished during the first half of the next day. This should cause the "Calling All Cryptographers" activity to be completed during the first part of the 9^{th} day, allowing time for review of the different ciphers students have worked with.

Name _____

An Affinity for Ciphers

As you have just recently seen, shift ciphers are quite susceptible to frequency analysis. Now we are going to consider a different cipher whose letter frequency pattern does not match that of the English language.

The new type of cipher that we are going to work with is the affine cipher. Affine ciphers are enciphered using congruencies of the form $C \equiv aP + b \pmod{26}$.

1. To begin with, encipher the message "are we there yet" using the affine cipher $C \equiv 5P + 11 \pmod{26}$:

(Show your work)

Numerical ciphertext: _____

Letter ciphertext: _____

2. Now encipher that message "attack at dawn" using the affine cipher $C \equiv 15P + 4 \pmod{26}$:

(Show your work)

Numerical ciphertext: _____

Letter ciphertext: _____

3. Now create an affine cipher of your own where $0 \leq a,b \leq 25$. Encipher the message "meet at midnight" using the cipher you created. (Show your work)

Numerical ciphertext: _____

Letter ciphertext: _____

Did your cipher work? If not, why does it not work? _____

_____

_____

4. Encipher the message "affines are neat" using the congruence expression $C \equiv 6P + 2 \pmod{26}$: (Show your work)

Numerical ciphertext: _____

Letter ciphertext: _____

Did the cipher work? If not, what about the cipher does not work? _____

_____

_____

Consider the affine ciphers on the front of the page that worked and the cipher above. What is the relationship between each of the numbers and the value of the modulus? Are there any restrictions we need to place on the values of a or b?

Name KEY

An Affinity for Ciphers

As you have just recently seen, shift ciphers are quite susceptible to frequency analysis. Now we are going to consider a different cipher whose letter frequency pattern does not match that of the English language.

The new type of cipher that we are going to work with is the affine cipher. Affine ciphers are enciphered using congruencies of the form $C \equiv aP + b \pmod{26}$.

1. To begin with, encipher the message "are we there yet" using the affine cipher $C \equiv 5P + 11 \pmod{26}$:

(Show your work)

Numerical ciphertext: 11 18 5 17 5 2 20 5 18 5 1 5 2

Letter ciphertext: LSF RF CUFSF BFC

2. Now encipher that message "attack at dawn" using the affine cipher $C \equiv 15P + 4 \pmod{26}$:

(Show your work)

Numerical ciphertext: 4 3 3 4 8 24 4 3 23 4 22 17

Letter ciphertext: EDDEIY ED XEWR

3. Now create an affine cipher of your own where $0 \leq a,b \leq 25$. Encipher the message "meet at midnight" using the cipher you created. (Show your work)

Answers may vary.

Numerical ciphertext: _____

Letter ciphertext: _____

Did your cipher work? If not, why does it not work? _____

_____

_____

4. Encipher the message "affines are neat" using the congruence expression $C \equiv 6P + 2 \pmod{26}$: (Show your work)

Numerical ciphertext: 2 6 6 24 2 0 6 2 0 0 2 0 2 12

Letter ciphertext: CGGYCAG CAA CACM

Did the cipher work? If not, what about the cipher does not work? The cipher does NOT work. As seen above, both A and N are enciphered as C, both E and R are enciphered as A, and both F and S are enciphered as G. A person receiving the message would have no way to determine which plaintext letter any of those ciphertext letters listed above would stand for.

Consider the affine ciphers on the front of the page that worked and the cipher above. What is the relationship between each of the numbers and the value of the modulus? Are there any restrictions we need to place on the values of a or b?

The overall concept for students to grasp through looking at the values of a is that a and 26, the modulus in this case, cannot share any divisors. That is, a and 26 must be relatively prime: $\gcd(a, 26) = 1$.

Day 7 Lesson Plan

Objective:

Further develop students' number sense through modular arithmetic, namely addressing inverse operations. Continue developing problem-solving skills and communication through collaboration.

Materials Needed:

One "Deciphering the Affine" worksheet per student.

Launch: (Approximately 5 minutes)

Begin by reviewing the method for enciphering a message using an affine cipher. Also review how to decipher a shift cipher. This should provide a base for the students to begin working on the worksheet so that they approach the questions posed by using their previous knowledge. Have students get together with a partner and hand out the worksheets for them to begin.

Explore: (Approximately 30 minutes)

During the time the pairs are working on the worksheet, move throughout the room and monitor each group's progress. As needed, provide prompting questions to encourage them to keep making headway. The first few questions are posed for them to see that algebra and modular arithmetic are similar, but not the same. Students should find through their work that operations in the two areas of mathematics do not produce the same results, as may be expected. After students have completed the first page, have them share their results for the deciphering congruence. This may provide an opportunity to have other students show their classmates how they worked with their knowledge of modular arithmetic to reach correct conclusions. Likely, students will have created a congruence that does not work in modular arithmetic; this is an opportunity to point out that multiplication differs between modular arithmetic and algebra. Once the first page has been addressed, allow students to complete the worksheet which will have them begin to work with inverses.

Share: (Approximately 10 minutes)

Students should share their results with the class to see the different findings groups made. After completing the second part of the worksheet, students should have a better understanding of the difference and similarity of finding an inverse in modular arithmetic verses algebra. Have groups present their findings on the last enciphered message and what they found the plaintext to say. It is important to have these groups address how they came to these conclusions to ensure that they have an understanding of the different operations in modular arithmetic.

Summarize: (Approximately 5 minutes)

Emphasize to the students the definition of inverses in both algebra as well as modular arithmetic. Ultimately, the definition is similar, but in modular arithmetic it is reduced by the modulus to provide the final answer. Let the students know that they have will have an opportunity to apply the knowledge that they have acquired so far in cryptography soon.

Name _____

Deciphering the Affine

It is time to decipher affine ciphers! Remember, when you are deciphering, you are doing the opposite of enciphering the message.

1. First, consider the algebraic equation $y = 5x + 2$. Solve the equation in terms of x. Be sure to show your work.

x =

2. Encipher the word "math" using an affine cipher of $C \equiv 5P + 2 \pmod{26}$. Please show your work.

Numerical ciphertext: _____

Letter ciphertext: _____

3. With the knowledge of what congruence expression was used to encipher the word math, and knowing the resulting ciphertext, can you develop an expression that can be used to decipher the message? Show your work, and write the congruence you found below.

$P \equiv$

Be prepared to share your results with the class.

Deciphering the Affine

In modular arithmetic, equations cannot be operated on in the same fashion. As was seen in our example, even though the equation and the congruence were similar, to find the inverse, a different method must be approached.

Find the algebraic inverses of the following:

a) 5 **b)** 7 **c)** (1/3)

Recall that in algebra, the product of an integer and its inverse is 1: $(x)(x^{-1}) = 1$

In modular arithmetic, the product of an integer and its inverse is 1 (mod n): $(a)(a^{-1}) = 1 \pmod{n}$

Using this expression, fill in the blank spaces in the table below. Show your work.

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

To decipher an affine cipher, the expression $P \equiv a^{-1}(C - b) \pmod{26}$ must be used. How does your congruence expression from before compare to the one above? _____

_____

_____

Decipher the following message given that it was enciphered with an affine cipher where $a = 9$ and $b = 5$

VFN UB HB ZGFQB

Name KEY

Deciphering the Affine

It is time to decipher affine ciphers! Remember, when you are deciphering, you are doing the opposite of enciphering the message.

1. First, consider the algebraic equation $y = 5x + 2$. Solve the equation in terms of x. Be sure to show your work.

$x = (1/5)(y - 2)$

2. Encipher the word "math" using an affine cipher of $C \equiv 5P + 2 \pmod{26}$. Please show your work.

Numerical ciphertext: 10 2 19 11

Letter ciphertext: KCTL

3. With the knowledge of what congruence expression was used to encipher the word math, and knowing the resulting ciphertext, can you develop an expression that can be used to decipher the message? Show your work, and write the congruence you found below.

Answers may vary.

Congruence expressions should be written (mod 26).

Correct expression: $P \equiv 21(C - 2) \pmod{26}$

Most likely response: $P \equiv (1/5)(C - 2) \pmod{26}$

Be prepared to share your results with the class.

Deciphering the Affine

In modular arithmetic, equations cannot be operated on in the same fashion. As was seen in our example, even though the equation and the congruence were similar, to find the inverse, a different method must be approached.

Find the algebraic inverses of the following:

a) 5 (1/5) **b)** 7 (1/7) **c)** (1/3) (3)

Recall that in algebra, the product of an integer and its inverse is 1: $(x)(x^{-1}) = 1$

In modular arithmetic, the product of an integer and its inverse is 1 (mod n): $(a)(a^{-1}) \equiv 1 \pmod{n}$

Using this expression, fill in the blank spaces in the table below. Show your work.

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

To decipher an affine cipher, the expression $P \equiv a^{-1}(C - b) \pmod{26}$ must be used. How does your congruence expression from before compare to the one above? Answers vary depending on initial response of student on previous page.

Decipher the following message given that it was enciphered with an affine cipher where $a = 9$ and $b = 5$

VFN UB HB ZGFQB

"way to go Idaho"

Day 8 Lesson Plan

Objective:

Students will apply their previous knowledge and problem-solving skills to decipher a message. Through the deciphering process, they will encounter different operations in modular arithmetic that they will work through to read the message.

Materials Needed:

One "Calling All Cryptographers!" worksheet per student.

Launch: (Approximately 3 minutes)

Inform the students that you have just received an important message from the National Security Agency asking for their assistance. Have them get with their partners and use the class period to decipher the message.

Explore: (Approximately 35 minutes)

Allow students to work on the worksheet. There is only one message that they need to decipher. They need to use their understanding of frequency analysis as well as how affine ciphers work to break the enciphered message. Check on the progress of the pairs throughout the activity. Some pairs may encounter difficulties with the dissemination of information. Encourage them to think about how they have deciphered messages before and how this may be applied to their current situation. Refer to the key to "Calling All Cryptographers" for ideas on information that may be "leaked" from the NSA to the students as they continue attempting to crack the cipher.

Share: (Approximately 10 minutes)

Have students share the deciphered message and how they reached their conclusion. Results should be similar between the different groups. Through their processes, students should recognize how they can work with multiple congruencies to solve for unknown variables.

Summarize: (Approximately 2 minutes)

Deciphering messages takes time, patience and insightful guesswork. The students have worked with a few ciphers and the mathematics behind them. There are many more ciphers to be explored. Some ciphers transpose the plaintext letters in different orders to mask their meaning, whereas others have highly complicated mathematics that require high-powered computers to encipher and decipher.

Name _____

Calling All Cryptographers!

Attention all cryptographers: The National Security Agency has just intercepted a message sent from a high ranking officer of a secret society to the CEO of a powerful corporation. Allegedly, the message has to do with a meeting that has been scheduled soon, and the NSA needs to know what this message says in order to preserve our nation's security. One of their agents uncovered the fact that the message was enciphered using an affine cipher. Please use your knowledge of this type of cipher, as well as frequency analysis, to decipher this message as soon as possible.

FJJIF JLIIO JFLIH YJJYJ GINJQ YJPQL ZGZGZ

Deciphered message: _____

Name KEY

Calling All Cryptographers!

Attention all cryptographers: The National Security Agency has just intercepted a message sent from a high ranking officer of a secret society to the CEO of a powerful corporation. Allegedly, the message has to do with a meeting that has been scheduled soon, and the NSA needs to know what this message says in order to preserve our nation's security. One of their agents uncovered the fact that the message was enciphered using an affine cipher. Please use your knowledge of this type of cipher, as well as frequency analysis, to decipher this message as soon as possible.

FJJIF JLIIO JFLIH YJJYJ GINJQ YJPQL ZGZGZ

For this, students should note that the letter J appears 11 times in the message and the letter I appears 6 times. With this knowledge, they should be able to make the conjecture that E corresponds to J, and that T corresponds to I. Finding that T may take time for students to develop, but since T has the second highest frequency in English and I has the second highest frequency in the message, they likely correspond with each other.

Using this information, they know $C = 9$ when $P = 4$ and $C = 8$ when $P = 19$. They can then create two congruences with this information:

$$9 \equiv 4a + b \pmod{26}$$

$$8 \equiv 19a + b \pmod{26}$$

By subtracting the first congruence from the second, the result is $15a \equiv -1 \equiv 25 \pmod{26}$. The inverse of 15 (mod 26) is 7, so multiplying each side of the congruence by 7 gives $a \equiv 19 \pmod{26}$. Substituting this value into the first equation results in $b \equiv 11 \pmod{26}$. This means that the message was enciphered using the congruence $C \equiv 19P + 11 \pmod{26}$. The inverse used to decipher the message is then $P \equiv 11(C - 11) \equiv 11C + 9 \pmod{26}$.

Deciphered message: meet me at the matinee next wednesday

Message adapted from Elementary Number Theory in Nine Chapters by Tattersall, p. 215.

Name _____

Cryptography Quest

Answer each question fully. Use the space provided to show your work and describe any methods you use to encipher or decipher messages.

1. Using a shift cipher of shift size 11, encipher the following message. Write your answer using the corresponding numerical values of the letters.

ciphers are everywhere

Enciphered message: _____

2. The message below has been intercepted from a spy network. Analysts have concluded that it was enciphered using a shift cipher, and through frequency analysis, they have decided that the ciphertext letter K most likely corresponds with the plaintext letter E. Decipher the message below. Write out the congruence used for deciphering and the congruence used for enciphering the message.

11 17 10 10 25 13 10 8 6 24 25 17 10 6 25 19 20 20 19

Enciphering congruence: _____ Deciphering congruence: _____

Deciphered message: _____

Cryptography Quest page 2

3. Create an affine cipher and encipher the following message with it. Identify the characteristics of your affine cipher that make it a functioning cipher.

"keep your friends close"

Enciphered message: _____

What characteristics of your affine cipher make it a working cipher?

Name KEY

Cryptography Quest

Answer each question fully. Use the space provided to show your work and describe any methods you use to encipher or decipher messages.

1. Using a shift cipher of shift size 11, encipher the following message. Write your answer using the corresponding numerical values of the letters.

ciphers are everywhere

Shown work may vary. Students may elect to write out the alphabet and the shift cipher, or they may show their calculations using modular arithmetic.

Enciphered message: 13 19 0 18 15 2 3 11 2 15 15 6 15 2 9 7 18 15 2 15

2. The message below has been intercepted from a spy network. Analysts have concluded that it was enciphered using a shift cipher, and through frequency analysis, they have decided that the ciphertext letter K most likely corresponds with the plaintext letter E. Decipher the message below. Write out the congruence used for deciphering and the congruence used for enciphering the message.

11 17 10 10 25 13 10 8 6 24 25 17 10 6 25 19 20 20 19

Student work may vary. Key observations they should make is that the numerical value for E is 4, and the numerical value for K is 10. Using this information and the fact that the message would be enciphered using the congruence $C \equiv P + k \pmod{26}$, where k represents the shift size, students should be able to solve for k and thus recreate the enciphering congruence.

Enciphering congruence: $C \equiv P + 6 \pmod{26}$ Deciphering congruence: $P \equiv C - 6 \pmod{26}$

Deciphered message: flee the castle at noon

Cryptography Quest page 2

3. Create an affine cipher and encipher the following message with it. Identify the characteristics of your affine cipher that make it a functioning cipher.

"keep your friends close"

Answers may vary. Affine ciphers are of the form $C \equiv aP + b \pmod{26}$ with $0 \leq a, b \leq 25$, and $\gcd(a, 26) = 1$.

Enciphered message: _____(Answers may vary)_____

What characteristics of your affine cipher make it a working cipher?

Key idea for students to discuss is that a and 26 must be relatively prime in order for the cipher to work. Otherwise, multiple plaintext letters may correspond to the same ciphertext letter, rendering the enciphered message undecipherable by the receiver.

Conclusion

The cryptography units, using the research conducted as a source of content information, address multiple standards described by the National Council of Teachers of Mathematics (NCTM). Each standard is designed to provide an overview of the type of characteristics prekindergarten through grade twelve instructional programs should have.

The Problem Solving standard should enable students to "build new mathematical knowledge through problem solving; solve problems that arise in mathematics and in other contexts; apply and adapt a variety of appropriate strategies to solve problems; monitor and reflect on the process of mathematical problem solving" (NCTM 334). Through the development of the various ciphers in the units, students have opportunities to solve problems that require them to further develop their mathematical thinking. The lesson plan format is designed to have students reflect on and communicate their ideas during the Share portion of a lesson.

During the different activities, students work with multiple operations and consider the relationships among numbers. As NCTM states, the Number and Operations standard should enable students to "understand numbers, ways of representing number, relationships among numbers, and number systems; understand meanings of operations and how they relate to one another; compute fluently and make reasonable estimates" (NCTM 214). When working with the shift and affine ciphers, students work with numbers and basic operations. Especially at the high school level, the involvement with modular arithmetic expands student understanding of the relationships between numbers in different types of number systems.

Connections and Communication are two standards that are also addressed in the units. Cryptography has close connections to the study of languages. This is directly portrayed through the analysis of the frequency distribution of the letters of the English language. Students also connect various mathematical ideas to view concepts as a whole. This is embodied in the activity "Calling All Cryptographers!" where students must use their knowledge of frequency analysis to provide them with insights towards finding the solution. They may then apply their understanding of modular arithmetic to decipher the message.

Through the activities, students are working with partners to explore the world of cryptography. This provides them with the need to be able to convey their mathematical ideas to a peer. These interactions develop and encourage their mathematical language as well as their ability to reflect on their own thoughts. Sharing, as part of the lesson structure, is a way to bring this peer-to-peer interaction to a higher level so that every student in the classroom can listen and speak mathematics with their classmates.

Cryptography is an interesting and intriguing topic within mathematics. Using the lessons and activities developed in this thesis may engage students by providing a different and exciting way to view and work with mathematics. The lessons and activities are designed to foster communication between students, as well as with the teacher and others. A mathematical community may be formed or reinforced through the exploration of cryptography in a mathematical context. Exploring cryptography is an interesting and fun endeavor, and the mathematics classroom provides an excellent venue for students to be introduced to the topic.

Bibliography

Berloquin, Pierre. Hidden Codes & Grand Designs. Sterling Publishing Company. New York; 2008.

Beutelspacher, Albrecht. Cryptology. The Mathematical Association of America. Washington, DC; 1994.

Boone, J.V. A Brief History of Cryptology. Naval Institute Press. Annapolis, MD; 2005.

Callery, Sean. Codes and Ciphers. HarperCollins Publishers. New York; 2008.

Comap, Inc. Mathematics: Modeling Our World; Course 1 Book. W.H. Freeman and Company. New York; 1998.

Kahn, David. The Codebreakers. The Macmillan Company. New York; 1967.

Kippenhahn, Rudolf. Code Breaking. The Overlook Press. New York; 1999.

Konheim, Alan G. Cryptography: A Primer. John Wiley & Sons. New York; 1981.

Hirsch, Christian R. Contemporary Mathematics in Context: Course 1 Book. Everyday Learning Corporation. Chicago, IL: 1998.

Lambert, David. Secret Codes. Sterling Publishing Company. New York; 2007.

Pincock, Stephen. Codebreaker. Walker & Company. New York; 2006.

Pratt, Fletcher. Secret and Urgent. Blue Ribbon Books. New York; 1942.

Principles and Standards for School Mathematics. National Council of Teachers of Mathematics. Reston, VA; 2005.

Tattersall, James J. Elementary Number Theory in Nine Chapters. Cambridge University Press. Cambridge, United Kingdom; 1999.

Young, Anne L. Mathematical Ciphers. American Mathematical Society. Providence, RI; 2006 vol. 25.

Graphics Citation

The Alberti cipher disk: http://starbase.trincoll.edu

English cipher disk: http://www.kidsmakestuff.com

Vigenére Table: http://www.braingle.com