
History of Cryptology

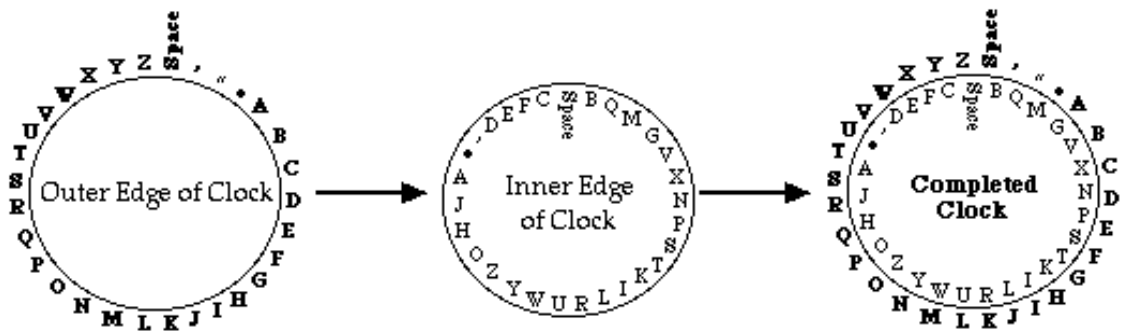


Table of Contents

HISTORY OF CRYPTOLOGY	4
SIMPLE CODES & CIPHERS	5
DESCRIPTION	5
LUMPING WORDS (FORMAT).....	5
CHARACTER BLOCKS.....	5
BACKWARDS ENGLISH.....	6
SELECTED CHARACTERS.....	6
PIN MARKS	6
ALPHABET WHEEL	6
CIPHER CLOCKS.....	6
MAKING YOUR CIPHER CLOCK	7
ALPHABET & WORD CORRELATED CIPHERS	7
COMPASS CIPHER - A METHOD FOR ALPHABET SUBSTITUTION.....	8
LETTER SPOKES CIPHER CLOCK	9
SPIRAL CIPHER CLOCKS	9
PIG LATIN	10
GRILLE METHOD	10
CONCEALMENT CIPHERS	11
VIGENERE TABLE	11
VIGENERE METHOD.....	12
THE AUTOCLAVE CIPHER	13
MATRIX CIPHERS.....	13
BIFID CIPHER	14
TRANSPOSITION CIPHERS.....	14
DOUBLE TRANSPOSITION CIPHERS	15
PIG PEN CIPHER	15
MAP CIPHER	15
DIAGRAPHIC SUBSTITUTION	16
INVISIBLE INK & MIRROR IMAGES.....	16
INVISIBLE INK.....	16

MIRROR IMAGES 17

CAMOUFLAGE CRAYONS 17

LETTER, SYLLABLE, & WORD FREQUENCIES 17

READING SAMPLE 18

5 BUILDING BLOCKS OF GOOD DESIGN 18

STRATEGIES FOR DECIPHERING 18

FREQUENCY TABLES FOR DECIPHERING 19

CRYPTOLOGY REFERENCES 19

History of Cryptology

Cryptology is the study of hidden writing. It comes from the Greek words *Kryptos*, meaning hidden, and *Graphen*, meaning to write. Cryptology is actually the study of codes and ciphers. Concealment messages aren't actually encoded or enciphered, they are just hidden. Invisible ink is a good example of a concealment message.

A code is a prearranged word, sentence, or paragraph replacement system. Foreign languages are just like secret code, where the English word "hi" is represented as the word "Hola" in Spanish, or some other word in another language. Most codes have a code book for encoding and decoding.

The name cipher originates from the Hebrew word "Saphar," meaning "to number." Most ciphers are systematic in nature, often making use of mathematical numbering techniques. One example of a cipher is the Spartan stick method.

The Spartans enciphered and concealed a message by using a scytale, a special stick and belt. The encipherer would wrap the belt around the stick and write a message on it. The belt was then unwound from the stick and sent to another person. Using a stick of similar size, the decipherer would wrap the belt around the stick to watch the secret message appear. If a stick of the wrong size appeared the message would be scrambled. Try this with 2 or 3 pencils bound together to make a stick, a long strip of paper, and another pencil for writing.

Julius Caesar used a simple alphabet (letter) substitution, offset by 3 letters. Taking the word "help" you would move ahead in the alphabet 3 letters to get "jgnr." This worked for a while, until more people learned to read and studied his secret cipher.

Gabriel de Lavinde made cryptology a more formally understood science when he published his first manual on cryptology in 1379. A variety of codes and mechanical devices were developed over the next few centuries to encode, decode, encipher, and decipher messages.

In the 1600's Cardinal Richelieu invented the grille. He created a card with holes in it and used it to write a secret message. When he was done he removed the card and wrote a letter to fill in the blanks and make the message look like a normal letter. The grille proved to be difficult to solve unless the decoder had the card which created the encrypted message.

In 1776 Arthur Lee, an American, developed a code book. It wasn't long before the US army adopted a code book of their own for use in the military.

The Rosetta Stone (black basalt), found in Egypt in 1799, had a message encrypted on its surface in three different languages! Greek, Egyptian, and Hieroglyphics messages all said the same thing. Once the Greek and Egyptian languages were found to have the same message the Hieroglyphics language was deciphered by referencing each letter to a symbol!

Morse Code, developed by Samuel Morse in 1832, is not really a code at all. It is a way of enciphering (cipher) letters of the alphabet into long and short sounds. The invention of the telegraph, along with Morse code, helped people to communicate over long distances. Morse code can be used in any language and takes only 1 to 10 hours of instruction/practice to learn! The first Morse code sent by telegraph was "What hath God wrought?", in 1844.

During WWI Karl Lody sent the following telegram "Aunt, please send money immediately. I am absolutely broke. Thank heaven those German swine are on the run." The clerk realized that this message didn't make any sense and forwarded it to the proper authorities who found Karl Lody guilty of espionage (spying). Can you see why his message must be a secret code or cipher? Why doesn't it make any sense?

In 1917, during WWI, the US army cryptographic department broke the code of the Germans. The code was actually stolen by Alexander Szek, a man working in a radio station in Brussels at the time. Unknown to the Germans, Szek was an English sympathizer and was stealing a few code words every day. When the Zimmerman telegraph was sent in 1918, asking Mexico to go to war against the United States, the US army cryptography department broke the code and decoded the telegraph.

The Germans learned from this experience and changed their codes. But the British were able to obtain copies of new code books from sunken submarines, blown up airplanes, etc., to continue breaking the new codes. By WWII

navy code books were bound in lead to help the code books sink to the bottom of the ocean in the event of an enemy takeover.

The little known native Indian language of the Navajo was used by the US in WWII as a simple word substitution code. There were 65 letters and numbers that were used to encipher a single word prior to the use of the Navajo language. The Navajo language was much faster and accurate compared to earlier ciphers and was heavily used in the battle of Iwo-jima.

The Germans in WWII used codes but also employed other types of secret writings. One suspected spy was found to have large numbers of keys in his motel room. After inspecting the keys it was found that some of the keys were modified to unscrew at the top to show a plastic nib. The keys contained special chemicals for invisible ink! However, codes and secret ink messages were very easily captured and decoded.

The Germans, responsible for much of the cipher science today, developed complex ciphers near the end of WWII. They enciphered messages and sent them at high rates of speed across radio wave bands in Morse code. To the unsuspecting it sounded like static in the background. One gentleman tried to better understand the static and listened to it over and over again. The last time he played his recording he forgot to wind his phonograph. The static played at a very slow speed and was soon recognized as a pattern, Morse code!

The invention of computers in the 20th century revolutionized cryptology. IBM corporation created a code, Data Encryption Standard (DES), that has not been broken to this day. Thousands of complex codes and ciphers have been programmed into computers so that computers can algorithmically unscramble secret messages and encrypted files.

Some of the more fun secret writings are concealment messages like invisible inks made out of potato juice, lemon juice, and other types of juices and sugars! Deciphering and decoding messages take a lot of time and be very frustrating. But with experience, strategies, and most of all, luck, you'll be able to crack lots of codes and ciphers.

Simple Codes & Ciphers

Description

A lot of codes are simple in design. Just by changing the order of words, letters, or the way you read them can turn a message into a secret code. Translating messages into code is called encoding. Translating messages into ciphers is called enciphering. When you attempt to figure out what a secret message is you are decoding or deciphering. To decode you need a code book.

Lumping Words (format)

Get rid of spaces and returns to lump words together. Use upper case letters to make the code harder to read and decode.

IBETTHISISHARDFORMANYPEOPLE.

Answer: I BET THIS IS HARD FOR MANY PEOPLE.

Character Blocks

Block letters of a message by 2, 3, or more characters.

IL IK EI CE CR EA M.

After combining all of the letters above you get "ILIKEICECREAM." Looking for words in the message you'll find "I LIKE ICE CREAM."

Backwards English

Writing words, sentences, or entire message backwards can be very confusing!

EES UOY TA EHT EROTS.

Reading EES backwards yields the answer SEE. The answer to this encrypted message is "SEE YOU AT THE STORE."

Selected Characters

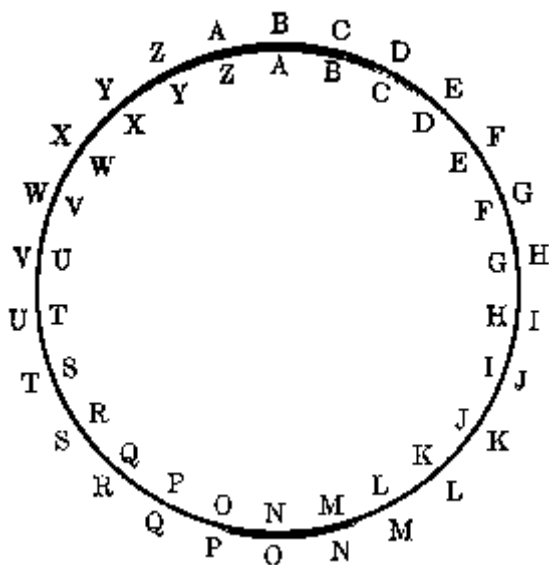
Choose a mathematical algorithm or pattern to create or decipher a secret message from a plain message. This example uses a pattern to make a secret message: *D id e veryone a t the h ouse ...etc.* "DEATH" is the secret message with the words in this message.

Pin Marks

Next time you sit down and read the newspaper use a pin to make tiny holes under letters as you read. By making a series of pin pricks in the paper, barely visible to the eye, you can actually create a message for your friends to decipher.

Alphabet Wheel

An alphabet wheel, often called a cipher clock, is a graphical picture of values that can be used to represent the letters of the alphabet. Most wheels have the plain alphabet in the inside the circle and the cipher alphabet on the outside. Using the picture below you can see that the letter "A," inside the circle, is equal to the cipher character "B." Thus, when you write the enciphered word "CAT" it would actually be written as "DBU." Deciphering is made easier when the alphabet wheel is used.



The example above is fairly easy to decipher if you don't have the original alphabet wheel. This is due to the pattern seen in both the plain and enciphered alphabets surrounding the wheel. Both alphabets are in sequence, in order. To make your alphabet wheel cipher harder to break you may want to arrange letters in a more random fashion or add in extra characters or symbols to distract the decipherer.

You can even make up your own alphabet wheel cipher with special symbols for each letter of the plain alphabet. Would you use a pattern, or do it randomly? Why? What is the benefit of using patterns versus random assignment of letters?

Cipher Clocks

Cipher clocks can be made to correlate the value of a letter to another letter, number, or symbol. Start by making a linear list of cipher values. See the examples below:

Offset by four: Counting the letter you start with, count forwards 4 letters.

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

Letters represented by numbers:

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 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Random letter substitution:

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

Random letters substituted by numbers:

A C B Z R T W N O M L J P U E I D K F V G H S X Y Q
 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 26

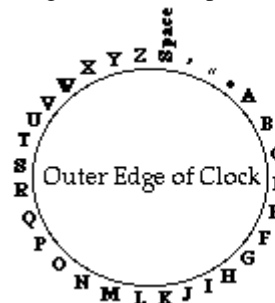
Random letters substituted by symbols:

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

Making Your Cipher Clock

Once you have a cipher you like, make a cipher clock from two circular pieces of paper. Place the smaller piece of paper on top of the larger piece. Then write your alphabet, with desired punctuation on one piece of paper, your cipher equivalents on the other. Make sure you space all the letters out equally so that the cipher letters/symbols align with the alphabet as you turn your clock. Put a paper faster in the middle and start en/deciphering!

Larger Piece of Paper



Smaller Piece of Paper



Completed Clock!



Can you figure to how to have more than one cipher on a cipher clock?

Alphabet & Word Correlated Ciphers

Sometimes keywords are used to help encipher a message. By writing out a sentence(s) that contains all the letters of the alphabet you can correlate plain alphabet letters to letters within a word found in the keyword phrase to make the ciphering a bit more difficult to decipher.

The keyword phrase "The quick brown fox jumps over the lazy dog." contains all the letters of the alphabet. Even though some letters appear more than once it shall serve as a keyword phrase because it still contains all the letters of the alphabet. To get started, write out your keyword phrase and number each word:

THE	QUICK	BROWN	FOX	JUMPS	OVER	THE	LAZY	DOG
1	2	3	4	5	6	7	8	9

Then write out your message in the plain alphabet: **Johnson is a spy**

To encipher the plain message you find the first word that contains the plain alphabet letter. In the example above, "J" is the first letter to find. It first appears in word five, "JUMPS." Write down the number of the word, 5, and then the position of the letter from within the word. In this case, "J" is the first letter of the word "JUMPS." Thus, the cipher value for "J" is 51. In other words, "J" is the first character in the fifth numbered word of your keyword phrase.

Use the partially completed cipher below to finish the enciphering process:

J	O	H	N	S	O	N	I	S	A
51	33	12	35	55	33	35	23	55	82
S	P	Y							
55	?	?							

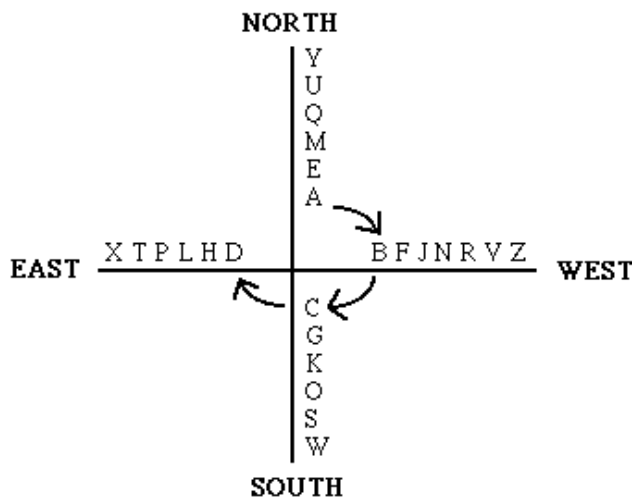
As you can see, letters that repeat like "O" are always the same number since you always find the first word it occurs in. Thus, "O" will always have the value of 33 in the example above. If you are a smart decipherer you'll notice common patterns of numbers that repeat and will be able to figure out which numbers are most likely an "E" or other common vowel or consonant.

Can you figure out a different way to use a keyword phrase to encipher a message? Can you make the cipher above even harder? What are the strengths and weaknesses of the cipher above?

Can you use different phrases as keyword phrases? What must every keyword phrase have in order to work for this type of cipher? Encipher a message using the method above. Then, create a variation on the method above and encipher the message again. Compare and contrast patterns of the two enciphered messages.

Compass Cipher - A Method for Alphabet Substitution

The compass cipher makes use of a well known pattern, the directions of north, south, east, and west. There are lots of ways to create a compass cipher key. One way, as shown below, is to make a cross in the center of your paper and write out the letters of the alphabet along each line, spiraling outwards.



The arrows show the direction used to fill in the compass lines. You can mix up your compass by making the cipher with a counter-clockwise rotation, random assignment, or unique patterns that you find useful.

Once you have all the letters written into your compass write out the letters, from outside in and then combine all of the letters into a long line. Finally, write out the plain alphabet below it to come up with an alphabet substitution cipher!

NORTH
YUQMIEA

EAST
ZVRNJFB

SOUTH
WSOKGC

WEST
XTPLHD

Compass Key: YUQMIEAZVRNJFBWSOKGCXTPLHD (NESW order)

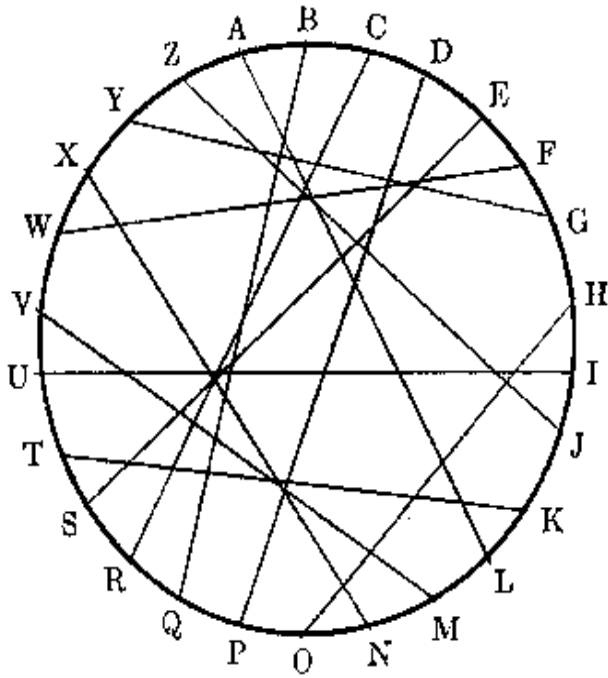
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

To make a new key try putting the letters together in a different order (SNEW?).

Letter Spokes Cipher Clock

Description

The letter spokes cipher clock, developed by Angie Wimer, resemble the spokes of a wheel. It's another way of making up a random alphabet substitution wheel. Simply take each letter in the wheel and line it up with another letter somewhere else in the wheel. When you get your encrypted message use the letter spokes decipher clock to find the letter tied to the encrypted letter. See if you can decipher the encrypted message "ALIYO VHCS LXP OLMS WIX" by making use of the Letter Spokes cipher clock below.



Answer

LAUGH MORE AND HAVE FUN

Notice how the first word, "ALIYO," can be decoded by finding the letter on the wheel that it is linked with? "A" is linked up with "L." Make up your own set of links and create a secret message. To make it harder create a cipher clock with all the letters placed along the edge in random order; write the message as lumped words, character blocks, backwards English, or Pig Latin; multiply the enciphered letter number values by 2, 3, or some other number.

Spiral Cipher Clocks

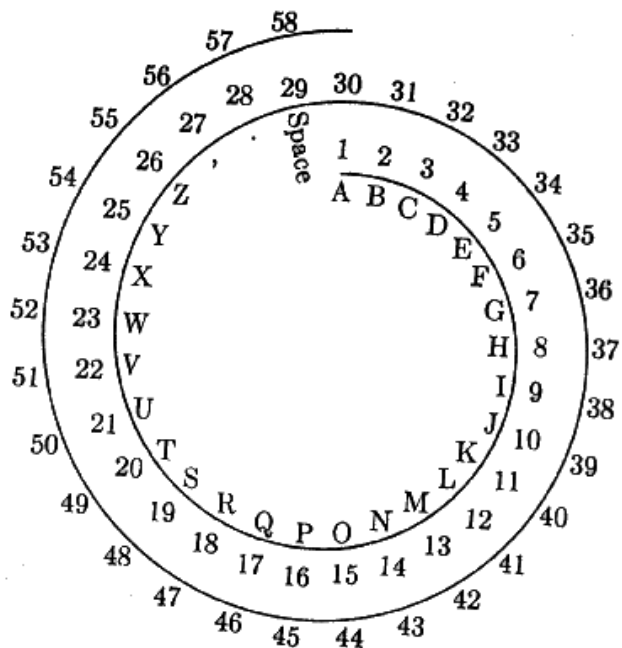
To make a cipher clock even harder you may want to create a spiral cipher that gives each character on your cipher clock multiple values. The picture below shows a spiral cipher clock with letters A-Z, a comma, period, and a space. Each character on the clock can be represented with a number. In the first spiral the letter A is equal to 1. B is equal to 2.

As the spiral continues around the cipher clock each character is given another value that can be used in your cipher. A is also equal to the number 30, in the second spiral. Can you figure out what the value for A is on the third spiral? Look for the answer below the picture.

Answer: Letter A is equal to values 1, 30, 59, 88, and so on. Simply add 29 to the original value of A to get the value for the next spiral. You add 29 because there are 29 characters in the entire cipher clock. Using the spiral you can write a cipher using any of the values for each character on the spiral cipher clock. Using the spiral above see if you can decipher the message:

21,14,4,58,18,19,20,30,14,33.

Answer is "understand." Notice how "d" is represented with two different values? Make your spiral cipher clocks even harder by using non-sequenced letters and extra characters.



Pig Latin

Most words in Pig Latin end in "ay." Use the rules below to translate normal English into Pig Latin.

1. If a word starts with a constant and a vowel, put the last letter of the word at the beginning of the word and add "ay."

Example: Happy = Yhappy + ay = Yhappay

2. If a word starts with two constants move the two constants to the end of the word and add "ay."

Example: Child = Ildch + ay = Ildchay

3. If a word starts with a vowel add the word "way" at the end of the word.

Example: Awesome = Awesome +way = Awesomeway

Putting It All Together

The sentence "Pig Latin is hard to speak." is written below in Pig Latin:

Gpiay Nlatiay isway dharay otay eakspay.

Notice how "Gpiay" is actually "Pig." Because the last character of pig is moved to the front, with "ay" added to the end, it makes Pig Latin very hard to read.

Decoding Pig Latin

Because Pig Latin is a method for translating words of the English language into a different language you can make up a code book for each commonly used word. Write your code book like a foreign language dictionary:

Pig Latin Plain English

airway air
ecoday code
phelay help Phelay emay otay ecoday.
emay me
otay to
ethay the
etc...

Grille Method

The grille method, developed by Cardinal Richelieu in the 1600's, was a secret message that could only be deciphered by a special card punched with holes in strategic locations. It's still an effective method for sending secret messages today! The picture below shows a plain message and the associated grille card that is used to decipher the secret message from the plain message.

Plain Message Secret Message Via Grille

You can create a grille message two different ways: Write a message and then create a grill card just for that message; create a master grille card and write message to fit within the predetermined hole punched locations.

In the example above the message was written out and the grille card was punched out as needed to create the secret message. Since the message was fairly long it was easy to get all the necessary characters to create the secret message "Meet me at the church." However, the encipherer is now stuck with the problem of needing to create a second grille card for their friend and must get both the grille card and the secret message to their friend using separate means. Otherwise an enemy could intercept the message and use the enclosed grille card to decipher it.

A better, but more complicated method, for creating a grille method is to make up a set of master grille cards that have hole punches in the same location on each card. Make sure you note which end is up on each of the card to ensure proper orientation. Then you write a message so that the letters for your secret message land in the grille punched locations.

Concealment Ciphers

Concealment ciphers, ciphers that are concealed (not obvious), have been used successfully in some very important matters. Long ago, in England during the time of Cromwell, Sir John Trevanion was locked up in Colchester Castle. He had been accused of a crime against his government and was waiting to be put to death. One day, he received the following letter from his loyal servant R. J.:

Worthie Sir John:- Hope, that is the best comfort of the afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me: Tis not much I can do: but what I can do, bee you verie sure I wille. I knowe that if deathe comes, if ordinary men fear it, it frights not you accounting is for a high hounour, to have such a rewarde of your loyalty. Pray yet that you may be spare this soe bitter, cup I fear not that you will grudge any suffereings; onlie if bie submission you can turn them away, this the part of a wise man. Tell me, as ifyou can, I do for you anything that you can wolde have done. The general goes back on Wednesday. Restinge your servant to command. R.J.

Can you figure out the secret cipher in the message above? Looking carefully at the letter it appears that the writer doesn't spell very well and doesn't know how to use punctuation either. Perhaps the misspelled words, misplaced letters, or punctuation are actually a secret cipher?

After Sir John read his letter he asked to go to the chapel to pray in his last hour before death. His jailers granted the request and waited for Sir John to finish his prayers. After several hours they entered the chapel to find it empty. Sir John had escaped!

The jailers analyzed the message and found that a concealment cipher was used to send Sir John a secret message. By picking out the third letter after every punctuation mark you get the message: panel at east end of chapel slides. Sir John made use of this information to move the panel and escape. Can you come up with your own concealment cipher? See if your friends can identify it!

Vigenere Table

Description

Use the table below to decipher any sequential alphabet substitution. All 26 possibilities are presented in the 23 rows of substitution values. You can also use it for Vigenere ciphers!

Key Word Letters

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
M	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
e	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
s	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
s	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
a	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
g	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
e	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
L	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
e	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
t	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	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
e	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
r	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
s	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

Simple Alphabet Substitution

The first row represents no substitution at all, A = A, B = B, and so on. The second row, starting with "B", is offset by 1 letter. Thus, A = B, B = C, C = D, and so on. For example, if I wrote out the encrypted word "EBE" it would be "DAD" in the second row (offset by one letter). Use this chart to quickly check for patterns that emerge from sequential alphabet substitution deciphering. This decryption key does not include punctuation. Be sure to take that into account when decoding! Ciphers with punctuation are more difficult than A-Z.

Vigenere Method

The Vigenere method is very difficult to break. A key word is usually used to encipher the message. A message is written out with the key word written above it (repeatedly). Look at the example below to see how to encipher messages using the Vigenere table from the previous page:

Key Word: CASH
 Message: This is cool.

Enciphering

Key Word Letters: CASH CA SHCA
 Message Letters: THIS IS COOL

Notice how the key word cash is written over the top of the message. Then correlate the key word letter with the message letter on the Vigenere table. Following the key word column "C" down to the message letter row "T" you find the enciphered letter "V." See if you can finish the enciphering of the message below:

Key Word Letters:	CASH CA SHCA
Message Letters:	THIS IS COOL
Enciphered Letters:	VHAZ K

Making the Cipher Even Tougher!

To make the enciphered message even more difficult use other enciphering methods. For example, once you encipher the word "This" with the key word "Cash," as seen above, you get the enciphered word "vhaz." Encipher "vhaz" into Pig Latin and you get "azvhay." Then you could encipher "azvhay" into a backwards code as "yahvza." In order to decipher this example you would have to write the code backwards (to the original order), decipher the Pig Latin format changes, and use the key word "Cash" and the Vigenere table to correlate key letters and enciphered letters with the message letters! Needless to say, this system of enciphering wasn't broken for a long period of time!!!

The Autoclave Cipher

The autoclave cipher is a variation of the Vigenere cipher, making use of the same table found on the previous page. A key letter is used instead of a key word. For example, you may choose "R" as your key letter. As you encipher your message the enciphered letter becomes the next key letter! Look at the example below to see how it works:

Key Letter:	RVCG Y
Message Letters:	THIS IS COOL
Enciphered Letters:	VCGY

Notice how the key letter "R" correlates with the message letter to give you the enciphered letter "V." "V" is used as the first enciphered letter of the enciphered message and serves as the next key letter. Then "C," the next enciphered letter, becomes the next key letter, etc...

Matrix Ciphers

A matrix is something that resembles an array, such as the regular formation of the letters of the alphabet written into columns and rows. By making use of a matrix, similar to references in an "X, Y" graph, a cipher can be created. The matrix below uses column and row labels to create a secret cipher.

Since the letters are written into a matrix, the letters for column and row labels can be combine to identify the location of a letter within the matrix. As an example, the letter "A" is in column "G," row "N." Thus, "A" could be written into an enciphered messages as "GN." Look at the example below to see how the word "DOG" is enciphered using the matrix above.

Plain Message:	D	O	G
Enciphered Message:	LN	MR	HO

Can you make the matrix grid above a little harder? Think about the sequencing of letters, the number of possible matrix cipher values created by columns and rows references, and the number of rows or columns used.

Do you think it is possible to decipher a message encoded with the system above without having the matrix to refer too? How could you break the cipher system of another person's matrix cipher? Make up your own matrix cipher and see if your friends can decipher the message!

Bifid Cipher

The Bifid cipher is a type of matrix, or columnar transposition, cipher. Start by creating a 5 by 5 matrix of letters, with the rows and columns labeled 1 to 5.

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

To start, find the value of each letter by reading the row and the column values. The two numbers are then written vertically on a piece of paper below the plain letter. All the plain letters within the secret message are written next to one another as seen below:

Plain Message:	S	E	N	D		R	E	I	N	F	O	R	C	E	M	E	N	T
Row Value:	4	1	3	1		4	1	4	3	2	3	4	1	1	3	1	3	4
Column Value:	4	5	4	4		3	5	4	4	1	5	3	3	5	3	5	4	5

Notice how the letter "S" has the value of 44. "E" is 15 since it is found in row 1, column 5. Y and Z share the position of (5,5) in the matrix above. After the message has been written out, with row and column values written as shown above, you rewrite the message from left to right, combing numbers into groups of 2.

41 31 41 43 23 41 13 13 44 54 43 54 41 53 35 35 45

The last step is to take each group of numbers, such as 41 and 31 in the beginning of the line above, and find the corresponding cipher values in the same matrix above. 41 is row 4, column 1, the letter "P." See if you can finish filling in the cipher letters below:

41	31	41	43	23	41	13	13	44	54	43	54	41	53	35
35	45													
P	K	P	R	H										

Transposition Ciphers

Transposition ciphers, sometimes called "rail fence ciphers," are a unique and fun way to encipher a message. There are lots of ways to create transposition ciphers. An example of one type of transposition cipher is given below.

Write our your secret message on two lines, writing one letter on the top line, the next letter on the second line, until the entire message has been written. Then write out your message by writing the the characters from the first and then second line in order!

Plain Message: THIS IS FUN!
 Line 1: T I I F N
 Line 2: H S S U !
 Enciphered Message: TIIFNHSSU!

You can try other ways for making a transposition cipher as well. After transposing your message on two lines you may want to write out your enciphered message by starting at the end of the second line, working your way right to left, until the entire message is written. An example is given below.

Plain Message: THIS IS FUN!
 Line 1: T I I F N
 Line 2: H S S U !
 Enciphered Message: !USSHNFIIT

Can you think of another way to encipher a transpositioned message?

Double Transposition Ciphers

Double transposition ciphers are very similar to normal transposition ciphers but are more complex in their design and are harder to decipher. There are also multiple methods for creating a double transposition cipher. One example is shown below:

Start with a keyword such as "shoes." Create a matrix grid below the keyword and write in your secret message from left to right. Then assign an order of sequencing to the columns or rows in your matrix. In the example below the cipher is made more difficult by ordering the columns out of order. The letter "Z" is used to fill in blank spaces found inside of the matrix. Each column or row, in numbered order, is then written down in blocks of 3 to 5 letters, in all uppercase, to encipher the message.

Plain Message: Pay me by Sunday or suffer the consequences.

Enciphered Message: PGDSR OUSEN RECQE ZAYAU TNEZM UOFEE CZYSY FHSNZ

To decipher the message you need to know how many letters are in the keyword and what order to arrange the columns for rewriting the enciphered letters into the matrix. To make it even harder you may want to try other patterns of enciphering your message with a keyword. Try spiraling outwards from the middle letter in your matrix, go right to left from the bottom corner to the upper left corner, or zig zag up and down through different columns or rows.

*Can you figure out why the enciphered message is in all uppercase? What does uppercase hide from your enemy? What would case sensitive text give away?

Pig Pen Cipher

Description

By creating a matrix of the alphabet within a tic-tac-toe box a pig pen cipher can be created. This method of enciphering was developed by Baptista dell Porta in the 1600's. Each symbol is created by referencing a letter position with the lines:

Once you figure out the pattern it is easy to find the letter represented by each symbol. I usually find the box pattern first, to locate which three letters must be possibilities. I then find the location of the dot to determine exactly which letter is represented by the symbol.

Making It Harder!

To make the cipher even harder, mix up the letters inside of the matrix. Put letters like "Z T O" in the upper left, replacing "A B C." Do the same for the entire matrix. Whenever you mix up the letters inside of a pig pen matrix it makes the cipher much harder to decipher. You can even try variations of the cipher as seen below:

Can you figure out how to use this variation of the Pig Pen cipher?

Map Cipher

Maps have been used by people for centuries to aid in navigation. However, if you look closely at some maps you may be able to identify a pattern. Map ciphers are maps that look normal but have a secret cipher hidden within.

To create your own map cipher you need to create a set of symbols that stand for each letter in the alphabet. The example below uses tree branches and a matrix to create an alphabet of trees. The position of each letter in the matrix determines the number of branches on the left or right side of the tree. Look at letter "C", located in the matrix position of (1, 3). Place on branch on the left, 3 on the right.

Using the matrix above, can you figure out what the secret message is below?

You may want to use mountains, tributaries to streams, or other objects that don't give your secret message away. The key to any good cipher is to make it look normal. If the enemy doesn't suspect anything your message will likely remain a secret.

Another thing you might want to do is randomly place letters into the matrix so that your cipher doesn't have such an easy pattern to decipher. Perhaps put letter "A" in (1, 4) and put letter "B" in (3, 2), etc. Maybe you'll use extra matrix locations to put in punctuation marks or distraction letters?

Diagraphic Substitution

Diagraphic substitution is a slightly more complex way of enciphering plain text letters with two letters found within a matrix. However, the matrix used is actually four matrices. There are two matrices used to identify two plain text letters at a time. The other two matrices are used to identify the corresponding cipher text values. Each individual matrix has all the letters of the alphabet:

The dashed line above was drawn to identify letters in the plain text matrices labeled P1 and P2. The letter "H" is identified in P1 and "I" in P2. Thus, the plain text letters spell out the word "HI." The corresponding cipher values can be found in C1 and C2 matrices. In this case, "H" in P1 corresponds to "A" in C1. "I" in P2 corresponds with "T" in C2. Thus, the enciphered letters for "HI" are "AT."

To decipher "AT" you simply find the corresponding plain text value in the same row, opposite plain text matrix.

Use the matrices above to encipher the message: Keep him alive. Start by writing out the two letter blocks of the message to form the rectangle for each encipher. After drawing the rectangle for each pair of letters find the corresponding cipher values:

Plain: KE EP HI MA LI VE
Cipher: NC BL

Can make the matrices differently than shown above? What must all matrices have in common? Does the order of letters in a matrix make a difference?

Invisible Ink & Mirror Images

Invisible Ink

Invisible ink has been used to conceal secret messages for a long time. You might remember the spy that used keys to hide invisible ink chemicals? Well the science of creating invisible messages has come a long way in the last 100 years. Professional scientists have developed invisible inks that are difficult to detect, even by the professional spy. If you'd like to experiment with invisible ink you can use some simple materials from home:

Invisible Ink Ingredients - Developed by Brady Schaures

1/4 cup white grapefruit juice
1/3 tsp. lemon juice
Pinch of sugar

Directions

Use a Q-tip to dip into the invisible ink and write your message on white paper. After the message dries you can use a hot iron, burning match, or lighter to burn the ink on the paper. CAUTION - Don't try this at home unless you have direct adult supervision. It is recommended that you use an iron to avoid the chance of fire.

The paper will turn brown and eventually burn up if you overheat the paper. The secret is to heat up the paper a little, see if the message has appeared, and then try again until you can see the message on the paper.

You may want to experiment with other liquids around the house until you can create an invisible ink that can't be seen on paper until it is burned. Other juices are a great way to write invisible ink on colored paper as well. Try orange juice, cranberry juice, and others.

Mirror Images

By making use of a computer you can easily create images that are backwards, only readable when seen in a mirror. Simply write your message and use painting or drawing tools to flip the message horizontally. Then print your message and hold it up to a mirror. The message below has been flipped horizontally and can be read in a mirror.

What is the message above?

Flip the text horizontally once you're ready to make it a mirror image.

Camouflage Crayons

Another way to hide a message is to use crayons. Use a pencil to write a message as lightly as possible on some paper. Then use crayons to cover up the message. If possible, draw a picture that is unsuspecting and looks normal. To see the secret message use a sharp knife or razor blade to scrape off the crayon marks. Be careful when handling the knife!

(*Histiaeus, in 500 B.C., wrote a secret message on a slave's head, waited for his hair to grow back, and sent his slave cross enemy lines. When his head was shaved the message appeared!)

Letter, Syllable, & Word Frequencies

When trying to decipher an enciphered message you may find letter and syllable frequencies to be helpful. The most common letters, numbers, or symbols used in the message are likely to be the most common letters of the plain alphabet, spaces, or punctuation marks. By identifying patterns and the frequency of letters, syllables, two and three letter words, etc, you can better decipher secret messages.

Let's say you get an enciphered message reading:

NMO GRBTF MZW ZTGZCW POOV NMO WXDO; ZVF NMOBO MZW ZTGZCW POOV ZW DSUM KRRF
QRBNSVO ZW PZF XV XN

What two and three letters are used more than once? What is the most common letter? Which letter is most likely a vowel like the letter "e"? The deciphered answer is:

THE WORLD HAS ALWAYS BEEN THE SAME; AND THERE HAS ALWAYS BEEN AS MUCH GOOD
FORTUNE AS BAD IN IT. -Quote by Machiavelli, "Discorsi"

Do you see how the word "THE" is represented by "NMO"? "O" is one of the most frequent letters because it is actually the letter "E." The following assignment will help you to identify your own frequency charts to use when deciphering messages like the one above.

Use the reading attached to this document to identify a frequency count for:

- a) letters a-z
- b) two and three letter words (an, of, etc.)
- c) syllables (ll, tt, etc.)
- d) first character of each word (like how many words start with "w", etc.)
- e) punctuation marks (,?:"!...)

Perhaps you should start by writing out a list of each frequency assignment above. Then count the frequency for each assignment, a-e, as shown above. When you are all done, analyze the results and write out an ordered list of frequencies for each assignment above.

The report for assignment a may look something like:

Total Characters = 354

Letter Frequency

Reading Sample

5 Building Blocks of Good Design

1. Proportion of a Single Item

How a single item is displayed. As an example: Rather than using a square to outline text or graphics use a proportional rectangle that is pleasing to the eye. The Greeks used a rectangle, now called the golden rectangle, that used proportions of approximately 1 to 1.618. Photographs are now printed on paper in a standard 3X5" because it is a shape that is fairly close to that of a golden rectangle, a shape that is more pleasing to the eye.

2. Proportion of a Relative Sizes

How two or more objects on a page compare to one another with respect to your message. As a general rule, larger items on a page are usually the more important items in your overall message.

3. Balance

It's important to maintain a balance of size and position of objects to provide the reader with a clear and interesting message. The visual center (golden mean) of a 8.5X11" paper is slightly above and to the left of the mathematical center. It's often a good idea to place the dominant object in the visual center or visual starting point of your document. Consider the visual weight of each object based on the objects properties: size, color, pattern, angle of display. Making use of white space to separate items can sometimes have a dramatic and effective roll upon the acquisition of balance.

4. Contrast

A paper without contrast is like a speech in monotonic presentation. Contrast adds to the importance of items, gathers interest, and spices up your document. Contrast is often added to documents by varying the type used for the text (font, style, size, color, etc.). Use of graphics, such as graphs, tables, photographs, borders, and illustrations are another method for providing contrast. Be careful not to overdo the contrast, creating a busy and irritating document that shouts at you rather than captures your interest in a pleasing way.

5. Rhythm

How are items placed on your document? Are you leading the reader's eyes around the document, or is it unorganized and hard to follow? Design your document to force the reader's eye to move up and down, left to right, in a circle, etc., as needed to capture the reader's interest and clearly direct them towards skimming and scouring modes of reading.

Strategies for Deciphering

The first things you should do is **get organized!** Compile a list of known codes and cipher methodologies that you can use on secret messages. Once you have tried all the methods you know of, use a hit and miss method, trial and error. The structure of the English language enables cryptologists to see patterns that emerge from normal messages. Just by looking at this paragraph of text, or playing Wheel of Fortune, you can figure out which letters are most common.

Vowels and spaces are the most frequent in the English language. A few constants, such as "S, T, N, etc." are more common than others. Finally, a few known bigrams (2 letters), such as "ll, ee, ss, etc." are more common than others. By recognizing patterns in ciphers you can often guess what the letters are decipher the message. The computer application "Cryptogrammer" teaches you how to decipher this way. Ask your instructor if you are interested in playing Cryptogrammer.

Most Common Letters

In order of most comon to least common:

1. E

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

Bigram Frequency

In order from most common to least common:
 TH, HE, AN, RE, ER, IN, ON, AT, ND, ST, ES, EN, OF, TE

Bigram Same Letter Frequency

In order from most common to least common:
 LL, EE, SS, OO, TT, FF, RR, NN, PP, CC, MM, GG

Trigram Frequency

THE, ING, CON, ENT, ERE, ERS, EVE, FOR, HER, TED, TER, TIO, VER

Initial Letters

T, A, O, M, H, W, C, I, P, B, E, S

Second Letters

H, O, E, I, A, U, N, R, T

Third Letters

E, S, A, R, N, I

Final Letters

E, T, S, D, N, R, Y, G

- *More than 50% of English words end with "E."
- *More than 50% of English words start with T, A, O, S, or W.

Frequency Tables for Deciphering

It's a good idea to **create a table of the counts** for letters of the alphabet, bigrams, trigrams, and initial and ending letters to see how many times a certain letter(s), number(s), or symbol(s) from an encrypted message occurs. The highest occurrence of a single letter/number/symbol is most likely to be "E" as seen in the frequency table above. The most common 2 letter/number/symbol bigram is likely to be "TH." If you can place a few likely letters you will often see a few short words, like "THE" appear.

Once words start to appear you're on to something. See if there is an easy pattern to get the rest of the letters. If not, continue **analyzing frequency tables** to decode the rest of the letters.

Use **trial and error** and replace letters/numbers/symbols with different letters until more words begin to appear. Try this method on the simple cipher below. Can you figure out what the encrypted message says?

Wpxfmt bsf uif nptu dpnnpof mfuufs

Cryptology References

Intel Corporation (1995). The Journey Inside: The computer (kit).

Keller, E. (1992). *The Big Book of Ready to Use Theme Units* . Scholastic Internet Libraries.

Snyder, L. (1994). Cryptogrammer Software. Internet archives.

World Book Encyclopedia (1989). The World Book Encyclopedia.

Sears, P. (1986). Secret Writing: Keys to the Mysteries of Reading and Writing. Teachers & Writers Collaborative program.

Miller, Marvin. Boy's Life: Codemaster Series. Boy Scouts of America.

Konheim, A. (1981). Cryptography A Primer. John Wiley & Sons.

Sinkov, A. & Irwin, Paul (1980). Elementary Cryptanalysis A Mathematical Approach. Mathematical Association of America.

Kohn, B. (1968). Secret Codes and Ciphers. Prentice Hall.

Laffin, J. (1964). Codes and Ciphers. Abeland-Schuman.

Epstein, S. & Epstein, B. (1956). The first book of codes and ciphers. Franklin Watts.