

Ciphers

Cipher: a secret or disguised way of writing; a code.

Throughout history, ciphers have been used as tools to convey secret messages. Some are ancient, and some were created during the birth of our country, but all have served the same purpose; to send secret messages!

Caesar Cipher

The first cipher on our list is called the “Caesar Cipher”. It is the oldest known substitution cipher, and was used by Julius Caesar himself, though historians think the cipher was around long before he was.

The Caesar cipher shifted the entire alphabet over **three letters**, so that each letter served as a different letter.

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

CIPHER: 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

So if you wanted to send this message: MEETING TOMORROW, you would write it as PHHWLQJ WRPRUURZ. Nothing to it!

1. Encipher these messages:
 - a. DELIVERY OF SUPPLIES DELAYED
 - b. MEET AGENT IN FRONT OF POST OFFICE

2. Decipher these messages:
 - a. OHDSH WKURXJK WKH VLGH GRRU
 - b. WKH URRVWHU FURZV DW GDZQ

St. Cyr Slide

Another type of cipher is very similar to the Caesar Cipher, but much more customizable. It was named after the French military academy where it was created: The St. Cyr slide

This cipher was accompanied with a device that had two rows of the alphabet, but one slid freely to shift the alphabet left or right at will. Instead of just one cipher, you could have 26 different varieties of the same cipher.

To use the device, slide the letter of your choice to match up underneath the letter A, and encode or decode a message.

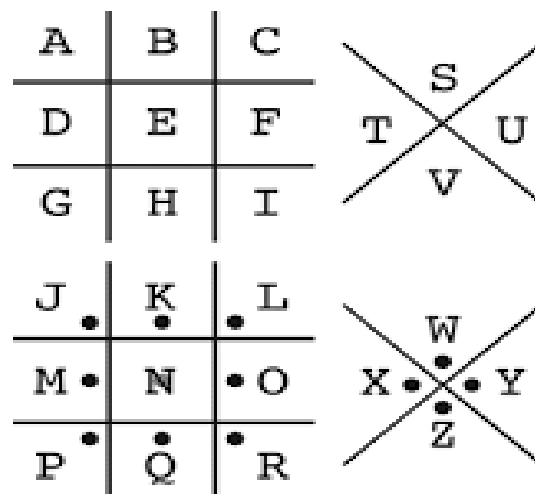
Use the St. Cyr slide (or wheel) you made in class to encipher these messages

(hint: use the letter k as your selected letter)

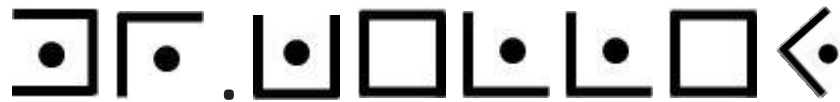
1. Encipher these messages:
 - a. I LIKE TO WRITE CIPHERS
 - b. PRACTICE YOUR CODES AND CIPHERS
2. Decipher these messages:
 - a. MYNOC RKFO MRKXQON RSCDYBI
 - b. LOGKBO YP CZSOC

The Pigpen Cypher

The pigpen Cypher has been around for a long time - over 800 years to be exact! It was originally used during the Crusades, but then it disappeared until the 1700's when the Freemasons picked it up. For this reason, the Pigpen Cypher is also known as the Freemason Cypher. It also resurfaced during the civil war, when a postal worker found the symbols on an envelope addressed to a suspected Confederate spy. Here's what the pigpen Cypher looks like.





To encipher one of these messages, simply use the part of the drawing that corresponds to the letters that you want to encipher. For example, to spell 'Mr. Kelley' it would look like

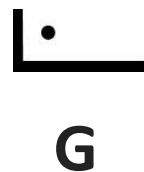
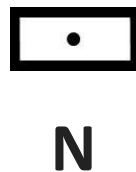


Rosicrucian Cipher

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

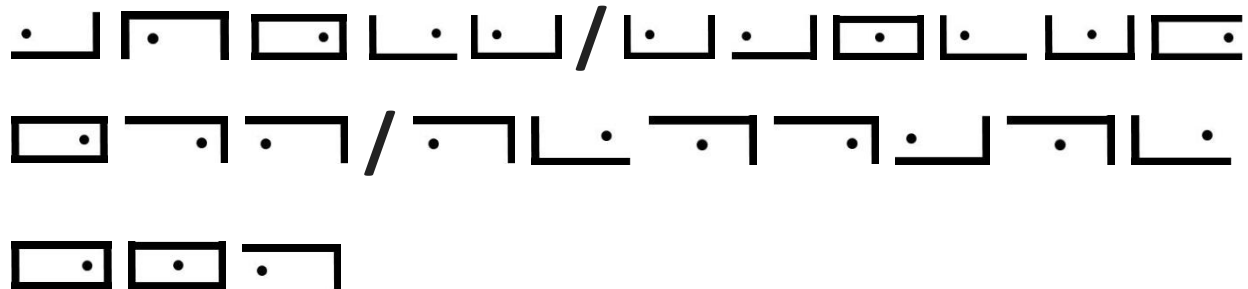
While the pigpen is very useful and easy to remember, a similar, more compact cipher is available. This one is called the *Rosicrucian Cipher*. It uses the same concept as the pigpen cipher, only this one depends on the location of the dot in the code bracket. For example: The letter A in the pigpen cipher is , but the letter A would be  with the Rosicrucian cipher.

Here are some examples of letters:



Practice!

Here is a message to decode using the Rosicrucian cipher:



Greek Square Cipher

This cipher is the earliest multilateral cipher known to man. Polybius, a historian and cryptographer who lived in ancient Greece nearly 2,200 years ago invented the device called the **Polybius checkerboard**, more commonly known as the **Greek square**. Each letter uses a two-number equivalent based on its position in the matrix.

	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

NOTE: Because there are 26 letters in the alphabet, but 25 places in the grid, I and J occupy the same space. Your partner should be able to figure out the difference as they decipher your message.

To encipher a message, you locate the letter you want in the chart. Then list the row, and then column that the letter is in. For example, the letter R would be 42, or the letter K would be 25. The biggest disadvantage is the fact that your message will be twice as long.

Practice!

Decipher these words using the Greek Square:

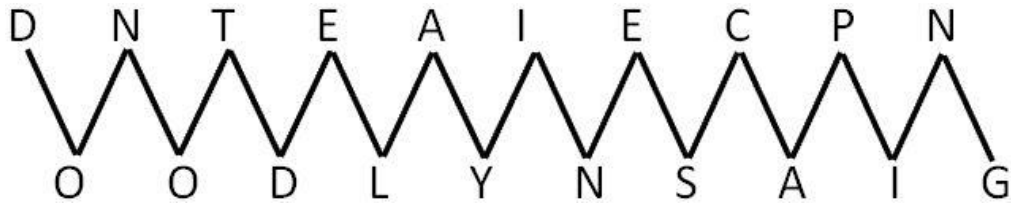
- 352442114415
- 132315132515421234114214

Rail Fence Cipher

This cipher is a very simple transposition process based off of the design of the 'split rail' fences that dotted the American countryside in the nineteenth century. This one splits the message up into two separate gibberish words that can be quickly unscrambled using a zig-zagging line. For example, you would write a message like:

DO NOT DELAY IN ESCAPING

And then you would arrange the letters like this.



Now, to send it as a ciphered message, write the top line, and then the bottom like this:

DNTEAIECPN OODLYNSAIG

Just reverse the process to decipher it!

PRACTICE!

1. EGRLAPESDIHR DAALNOUECPES
2. ECPNWEOLILS SAEObFRALSOT

Null Cipher

One of the most basic ways of concealing a message is the **null cipher**. The tactic used here is making a phrase where only certain letters mean something in the message. The phrase could be a well-crafted letter with two meanings, or it could be a meaningless string of nonsense words. It all depends on what you plan on doing with the letter. Try finding a meaning in this message:

SKUNK AVALANCHE VERTICAL EASY YESTERDAY

OCTOBER USUALLY REMOVE SERIOUS

EVERLASTING LAP FOREVER

Did you get it? Here's a hint: look at the first letter of each word in the phrase. It spells out "save yourself". To use this cipher, you can use any letter in the word, and you can be as creative as you want.

My antelope is not supposed to read enigmatic eulogies tonight

Large orange opals kill underappreciated noseless dragons. Eventually, Remus the hat eater returns umbrella guns.

The Vigenère cipher

One of the most famous ciphers in history is the Vigenère cipher, once known as “le chiffre indéchiffrable” or, “the unbreakable cipher.” Its premise was simple; slide the alphabet over, much like the Caesar cipher, or the St. Cyr slide. But the Vigenère differed in a crucial way in that it switched to a different alphabet for each letter, rather than staying on one. Its style is known as a *polyalphabetic substitution* cipher, and it is incredibly difficult to crack.

To encipher a message, you would first choose a key word that would be used to switch alphabets for each letter. In this example, let’s use the word LEMON to encipher the sentence “ATTACKATDAWN”.

ATTACKATDAWN

LEMONLEMONLE

Much like graphing in algebra, you would use the top row as the alphabet you are using to encipher the letter, and you would find the enciphered letter the same as a Caesar cipher.

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Cipher text: LXFOPVEFRNHR

	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

Practice!

For practice, encipher these two sentences;

-use the code word "spy"

1. Watch For dogs!
2. Secret bookcase

Cracking the Vigenère

(upcoming)

Frequency distribution

Here is a message enciphered using the frequency distribution method. It is a somewhat lengthy process, but using the method of 'frequency distribution' we can make the message at least partially readable.

yfzh zh nj kpktlzhk zj etkmizjq lzwfkth dhzjq vtkcdkjlz bzhytzedyznj. zy zh kmhzhky yn dhk yfzh skyfnb zv gnd zjytklwy m skhhmqk yfmy zh sntk yfmj njk fdjbtb lfmtmlykth zj akjqyf, eklmdhk zj yfmy lmhk, yfk hmswak hzuk zh amtqk kjndqf hn yfmy yfk lfmtmlykt bzhytzedyznj zh sntk azikag yn lanhkag tkhkseak yfmy nv m ygwzlma skhhmqk xtzyykj zj kjqazhf. xk fmok smbk gndt ymhi kmhzhkt zj yfzh kpmiswak eg hkwmimyzjq yfk xntbh zj yfk skhhmqk.

The message is long enough to warrant attempting decryption using frequency distribution. The first step is to make a list of the frequency distribution of the letters in the ciphertext. It is as follows:

a – 11	l – 12	w – 6
b – 7	m – 29	x – 3
c – 1	n – 15	y – 35
d – 10	o – 1	z – 35
e – 6	p – 2	

f – 21	q – 10
g – 7	r – 0
h – 35	s – 10
i – 3	t – 21
j – 21	u – 1
k – 52	v – 3

The following is an approximation of the distribution of letters in English, given a random writing sample of 1000 characters:

A – 73	G – 16	M – 25	S – 63	Y – 19
B – 9	H – 35	N – 78	T – 93	Z – 1
C – 30	I – 74	O – 74	U – 27	
D – 44	J – 2	P – 27	V – 13	
E – 130	K – 3	Q – 3	W – 16	
F – 28	L – 35	R – 77	X – 5	

In the ciphertext above, the letter k appears most frequently, with 52 instances, and the letters h, y and z are next, with 35 instances each. This implies that the cipher “k” probably translates to the plaintext “e,” since “e” is the most commonly-found letter in English, and the cipher letters “h,” “y” and “z” probably translate into three of the letters “a,” “i,” “n,” “o,” “r,” “s” or “t,” since these are the next-most-common letters in English.

-Changing the ciphertext “k” to the plaintext “e,” we have the following:

yfzh zh mj EpEtlzhE zj etEmizjq lzwfEth dhzjq vtEcdEjlg bzhytzedyznj. zy zh EmhzEhy yn dhE yfzh sEyfnb zv gnd zjyEtlEwy m sEhhmqE yfmy zh sntE yfmj njE fdjbtEb lfntmlyEth zj aEjqyf, eElmdhE zj yfmy lmhE, yfE hmswaE hzuE zh amtqE Ejndqf hn yfmy yfE lfntmlyEt bzhytzedyznj zh sntE aziEag yn lanhEag tEhEseaE yfmy nv m ygwzlma sEhhmqE xtzyyEj zj Ejqazhf. xE fmoE smbE gndt ymhi EmhzEt zj yfzh EpmswaE eg hEwmtmyzjq yfE xntbh zj yfE sEhhmqE.

A study of short words (two or three letters) comes in handy here. We notice a few patterns, especially in reference to the most common letters seen in this ciphertext. Since “z” and “h” appear so frequently, and we notice there are five instances of the two-letter word

“zh,” a good guess is that “zh” could be “is,” “in,” “at,” “an” or “or.” Also, there are six times where “zj” appears, giving more strength to this argument. Let’s try the cipher “z” corresponding to the plaintext “i,” with the cipher “h” corresponding to the plaintext “s” and the cipher “j” corresponding to the plaintext “n.” Then we have:

yfIS IS mN EpEtIISE IN etEmiINq llwfEtS dSINq vtEcdENlg bISyIedyInN. Iy IS EmSIESy yn dSE yfIS sEyfnb Iv gnd INyEtIewy m sESSmqE yfmy IS sntE yfmN nNE fdNbtEb lfmtnlyEtS IN aENqyf, eElmdSE IN yfmy lmSE, yfE SmswaE SIuE IS amtqE ENndqf Sn yfmy yfE lfmtnlyEt bISyIedyInN IS sntE aIIEag yn lanSEag tESEseaE yfmy nv m ygwIlma sESSmqE xtIyyEN IN ENqaISf. xE fmoE smbE gndt ymSi EmSIET IN yfIS EpmswaE eg SEwmtmyINq yfE xntbS IN yfE sESSmqE.

Looking at the first two words, “yfIS IS,” one might guess that this means “this is,” especially with the cipher “y” appearing 35 times. Guessing that provides us with:

THIS IS mN EpEtIISE IN etEmiINq llwHEtS dSINq vtEcdENlg bISTIedTInN. IT IS EmSIEST Tn dSE THIS sETHnb Iv gnd INTEtIewT m sESSmqE THmT IS sntE THmN nNE HdNbtEb IHmtmlTEtS IN aENqTH, eElmdSE IN THmT lmSE, THE SmswaE SIuE IS amtqE ENndqH Sn THmT THE IHmtmlTEt bISTIedTInN IS sntE aIIEag Tn lanSEag tESEseaE THmT nv m TgwIlma sESSmqE xtITTEN IN ENqaISH. xE HmoE smbE gndt TmSi EmSIET IN THIS EpmswaE eg SEwmtmTINq THE xntbS IN THE sESSmqE.

Looking at the second line, we find a one-word “m.” Since the plaintext “i” is already used, this must mean the cipher “m” corresponds to the plaintext “a.” This gives:

THIS IS AN EpEtIISE IN etEAiINq llwHEtS dSINq vtEcdENlg bISTIedTInN. IT IS EASIEST Tn dSE THIS sETHnb Iv gnd INTEtIewT A sESSAqE THAT IS sntE THAN nNE HdNbtEb IHAtATEtS IN aENqTH, eElAdSE IN THAT IASE, THE SASwaE SIuE IS aAtqE ENndqH Sn THAT THE IHAtATEt bISTIedTInN IS sntE aIIEag Tn lanSEag tESEseaE THAT nv A TgwIIAa sESSAqE xtITTEN IN ENqaISH. xE HAoE sAbE gndt TASi EASIEt IN THIS EpAswaE eg SEwAtATINq THE xntbS IN THE sESSAqE.

In the second line, there is a two-letter word, “Tn,” which implies that the cipher “n” is the plaintext “o.” Then, in the fourth line, the word “ENndqH” implies “ENOUGH,” so that the cipher “d” is the plaintext “u,” and the cipher “q” is the plaintext “g.” When we put in those three substitutions, we get:

THIS IS AN EpEtIISE IN eEtEAiING IiwHEtS USING vtEcUENlg bISTtIeUTION. IT IS EASIEST TO USE THIS sETHOb Iv gOU INTEtIEwT A sESSAGE THAT IS sOtE THAN ONE HUNbtEb IHAtAITEtS IN aENGTH, eEIAUSE IN THAT IASE, THE SASwaE SIuE IS aAtGE ENOUGH SO THAT THE IHAtAITEt bISTtIeUTION IS sOtE aIIEag TO laOSEag tESEseaE THAT Ov A TgwIIAa sESSAGE xtITTEN IN ENGaISH. xE HAoE sAbE gOUt TASi EASIEt IN THIS EpAswaE eg SEwAtATING THE xOtBS IN THE sESSAGE.

It's getting much easier now, because we can see obvious words formed. For instance, in the third line, "HUNbtEb" implies "HUNDRED," in the fifth line, "ENGaISH" implies "ENGLISH," and in the last line, "sESSAGE" implies "MESSAGE." When we make those substitutions, we see:

THIS IS AN EpERIISE IN eREAIING IiwHERS USING vREcUENlg DISTRIeUTION. IT IS EASIEST TO USE THIS METHOD Iv gOU INTERIEwT A MESSAGE THAT IS MORE THAN ONE HUNDRED IHARAItERS IN LENGTH, eEIAUSE IN THAT IASE, THE SAMwLE SIuE IS LARGE ENOUGH SO THAT THE IHARAItER DISTRIeUTION IS MORE LIIElg TO ILOSElg RESEMeLE THAT Ov A TgwIIAL MESSAGE xRITTEN IN ENGLISH. xE HAoE MADE gOUR TASi EASIER IN THIS EpAMwLE eg SEwARATING THE xORDS IN THE MESSAGE.

Although we have deduced barely more than half the letters of the alphabet so far (14, to be exact), we have deciphered the vast majority of the letters in the ciphertext, and in fact, the rest is almost trivial. The cipher "l" obviously turns into the plaintext "c," and with that, things become clearer still, as shown here:

THIS IS AN EpERCISE IN eREAIING CIwHERS USING vREcUENCg DISTRIeUTION. IT IS EASIEST TO USE THIS METHOD Iv gOU INTERCEwT A MESSAGE THAT IS MORE THAN ONE HUNDRED CHARACTERS IN LENGTH, eECAUSE IN THAT CASE, THE SAMwLE SIuE IS LARGE ENOUGH SO THAT THE CHARACTER DISTRIeUTION IS MORE LIIElg TO CLOSElg RESEMeLE THAT Ov A TgwICAL MESSAGE xRITTEN IN ENGLISH. xE HAoE MADE gOUR TASi EASIER IN THIS EpAMwLE eg SEwARATING THE xORDS IN THE MESSAGE.

Rather than go through the rest of the letters step-by-step, let's look at the message in its entirety:

THIS IS AN EXERCISE IN BREAKING CIPHERS USING FREQUENCY DISTRIBUTION. IT IS EASIEST TO USE THIS METHOD IF YOU INTERCEPT A MESSAGE THAT IS MORE THAN ONE HUNDRED CHARACTERS IN LENGTH, BECAUSE IN THAT CASE, THE SAMPLE SIZE IS LARGE ENOUGH SO THAT THE CHARACTER DISTRIBUTION IS MORE LIKELY TO CLOSELY RESEMBLE THAT OF A TYPICAL MESSAGE WRITTEN IN ENGLISH. WE HAVE MADE YOUR TASK EASIER IN THIS EXAMPLE BY SEPARATING THE WORDS IN THE MESSAGE.

Practice!

Try to crack this enciphered message!

"Bfb K hoy'b yene bq ko luqrg xif teznj," Awqei rpucvkpl.

"Ql, yzc een'e pgpp epcx," slqf xhp Kcx: "wp'zg elw uch hpzg. M'm xif. Cof'zg qao."

"Pqa dz gqy kywy M'm xif?" watl Cpinm.

"Asu xcux bp," acmd epq Gae, wt cof eqylov'v lagm esmp pgve."