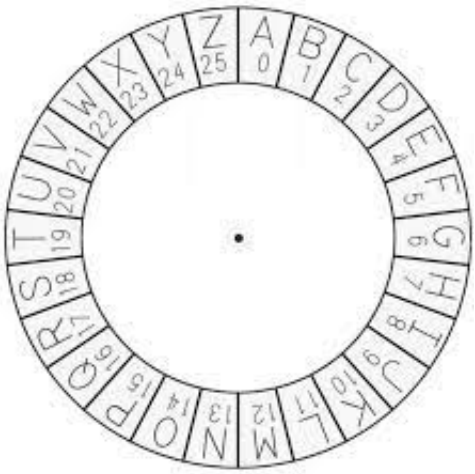
1 Introduction

Today, we'll be cracking codes. Some of these ciphers (ways of turning words/sentences into secret codes) have actually been used in history, especially at times of war. What you're doing now is very similar to what code-breakers have done in history to uncover secret messages. Some of these can be pretty challenging, so don't be afraid to erase your guesses and try new ideas!

2 Warm-up

Below is a circle, where the letters A-Z correspond with the numbers 0-25. If I give a list of numbers, can you decode the word? For example, if my list is **1, 0, 19**, this will create the word **BAT**.



Decode the words/phrases.

1. {12, 0, 19, 7}
2. {2, 8, 17, 2, 11, 4}
3. {1, 17, 8, 6, 7, 19} {1, 0, 11, 11, 14, 14, 13, 18}

What happens if we take out some of the numbers and replace them with question marks in the problems. You will have to use a little bit of trial and common sense to find what the numbers that should fill in the question marks. Below are some "common phrases" for you to decode.

1. {7, ?, 12, 4} {17, 20, 13}
2. {6, 14, ?, 5} {1, 0, 11, ?}
3. {17, 0, 2, ?} {{2, ?, 17}

3 Caesar Cipher

A Caesar Cipher encodes words by shifting letters in the word. For example, if want to encode the word "BAT" with a "shift" of 7, we would add 7 to each number corresponding with a letter:

$$B = 1, 1 + 7 = 8, 8 = \mathbf{I}$$

$$A = 0, 0 + 7 = 7, 7 = \mathbf{H}$$

$$T = 19, 19 + 7 = 26, 26 = 0 = \mathbf{A}$$

Here, we have an example of what happens if an index for a letter is 26 or higher. If this happens, you can continue counting like: 23, 24, 25, 0, 1, 2, ... We treat the alphabet as a cycle, where the letter after Z is A.

Therefore, applying a "shift" of 7 on "BAT" gives us the encoded word "IHA."

Let's practice this a little. Decode the following:

1. Shift of 5: $HTWWJHY$
2. Shift of 4: $AMJIB$
3. Shift of 25: $LZXAD$
4. Shift of ???: $SGZN$ (Hint: What words could this possibly be?)
5. (**Challenge**) Shift of ???: $WHLDWXAP$

4 Vigenere Cipher

Let's see if you can figure out how this one works. I want to encode the word "*house*" with the word "fun," and I get the code word "*mihxy*." The table below is a hint...

	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

Let's do some problems on this.

1. You have the encoded word **EECTV** and you know that the key is **PEN**. What is the decoded word?
2. You have the encoded word **QBKUGQFO** and you know that the key is **CORN**. What is the decoded word?
3. You have the encoded word **UVUKAJJUVWHIYIF** and you know that the key is **FRUIT**. What is the decoded word?

5 Aristocrat Cipher

An Aristocrat cipher is *monoalphabetic*. This means that, for example, if A encrypts to F, then only A encrypts to F, and A only encrypts to F. **Also, no letter can encrypt to itself.**

The chart below the letters shows frequency, or how often those letters appear in the encrypted sentence. Decode the following (REMEMBER THAT THE DECRYPTED MESSAGE SHOULD BE A SENTENCE THAT MAKES SENSE)!

(Hint: It wouldn't make sense to substitute the letter "Z," for example for "D," the most common letter in the message because the sentence has to be made up of words).

(Another Hint: Try substituting **E** for **D** - write E under the **D** column of the chart).....

FR SVDJD FT EBCSVFBK ND NFTV SX IVEBKD FB SVD IVFOM,

ND TVXLOM RFJTS DWEQFBD FS EBM TDD NVDSVDJ FS FT

TXQDSVFBK SVES IXLOM ADSSDJ AD IVEBKDM FB XLJTDOHDT.

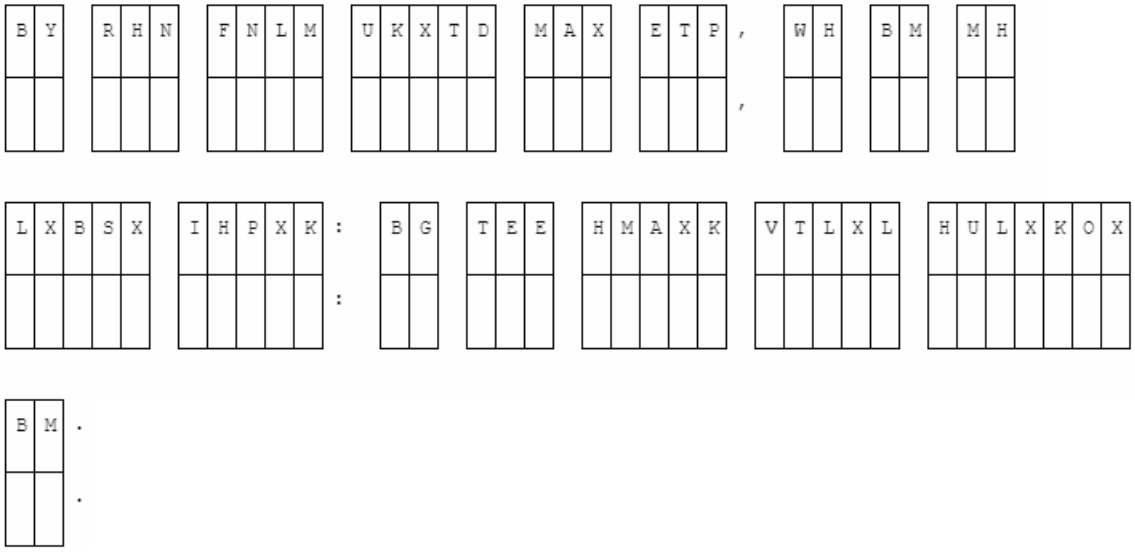
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	2	9	1	19	6	13		1	4	5	4	3	5	4	4		2	2	13	9		12	1	5		
Replacement																										

6 Problems and Practice!

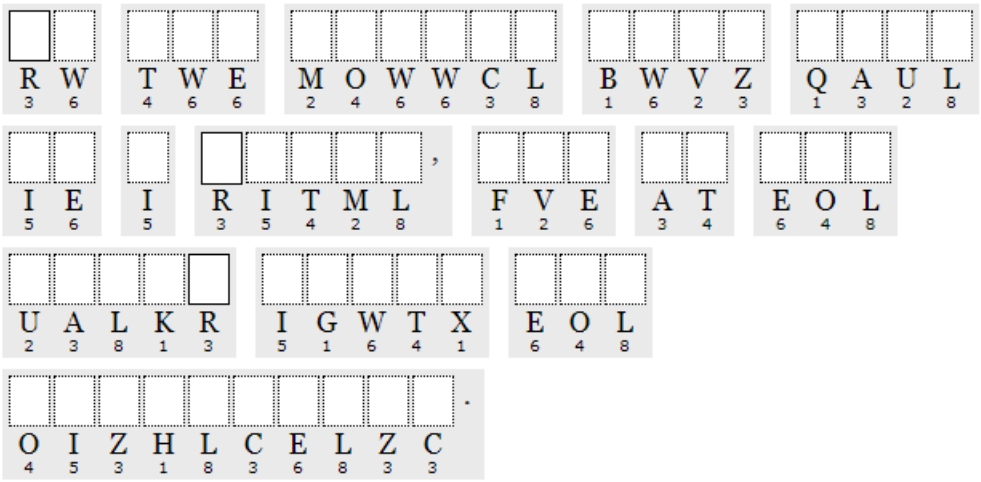
1. A magic word is needed to open a certain box. A secret code assign each letter of the alphabet to a unique number. The code for the magic word is written on the outside of he box. Which of the following words can be the Magic Word?
   - SECRET
   - LOOSER
   - LOTTOS
   - WINNER
2. Seven Caesar Ciphers (movie quotes):
   - **S'VV LO LKMU** - Terminator
   - **WKI DRO PYBMO LO GSDR IYE** - Star Wars
   - **W OA MCIF TOHVSF!** - Star Wars Episode V: The Empire Strikes Back
   - **SE VXKIOUAY!** - The Lord of the Rings: Two Towers
   - **GRPQ HBBM PTFJJFKD** - Finding Nemo

- **OCIKE OKTTQT QP VJG YCNN, YJQ KU VJG HCKTGUV QPG QH CNN?** - now White and the Seven Dwarfs
- **GB VASVAVGL NAQ ORLBAQ!** - Toy Story

3. If FIND is coded as URMW and ME is coded as NV, then how is FOOL coded as?
4. Below is a Vigenere Cipher. Write what message is encoded in the boxes below the encrypted message. Note that the key is not given here!



5. Aristocrat cipher here with the frequency of letters put right underneath the letters.



6. You can go to https://www.icryptograms.com for a whole bunch more Code breaking problems as well! If, somehow, you finished all of this and there's still time, ask a teacher to look over your answers and maybe give more problems.