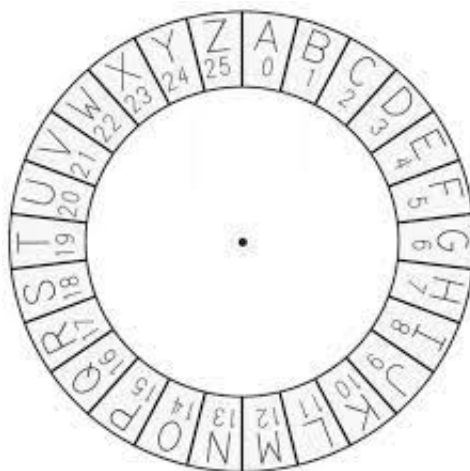


## 1 Introduction

Below are the answers to the code breaking handout. Please email us if you have any questions.

## 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. MATH
2. CIRCLE
3. BRIGHT BALLOONS

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. HOME RUN
2. GOLF BALL
3. RACE CAR

## 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. CORRECT
2. \*IGNORE THIS PROBLEM\*
3. MAYBE
4. MATH
5. (Challenge) ALPHABET

## 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. PAPER
2. ONTHECOB
3. PEACHESANDCREAM

## 5 Aristocrat Cipher

IF THERE IS ANYTHING WE WISH TO CHANGE IN THE CHILD, WE SHOULD FIRST EXAMINE IT AND SEE WHETHER IT IS SOMETHING THAT COULD BETTER BE CHANGED IN OURSELVES.

## 6 Problems and Practice!



1. WINNER
2. Seven Caesar Ciphers (movie quotes):
  - I'LL BE BACK - Terminator
  - MAY THE FORCE BE WITH YOU - Star Wars
  - I AM YOUR FATHER! - Star Wars Episode V: The Empire Strikes Back
  - MY PRECIOUS! - The Lord of the Rings: Two Towers
  - JUST KEEP SWIMMING - Finding Nemo
  - MIRROR MIRROR ON THE WALL, WHO IS THE FAIREST OUT OF ALL - Snow White and the Seven Dwarfs
  - TO INFINITY AND BEYOND! - Toy Story
3. ULLO
4. IF YOU MUST BREAK THE LAW, DO IT TO SEIZE POWER: IN ALL OTHER CASES OBSERVE IT.
5. DO NOT CHOOSE YOUR WIFE AT A DANCE BUT IN THE FIELD AMONG THE HARVESTERS.
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.