

# Code Busters Division A

Monica Bergler & Logan Bergler

# Code Busters

- Introduction
- Event rules
- Review of code types
- Coaching for success
- Test tools
- Questions

# Code Busters Introduction

## Definitions:

- Plaintext (Unencoded) - **This is plaintext**
- Ciphertext (Encoded) - **CGGOR AOXFS REC**
- Key - Information used to **Encrypt Plaintext** specific to a particular cipher
- Decrypt - Convert **Ciphertext** into **Plaintext** with or without a **Key**
- Crib - a few known **Plaintext** letters for some **Ciphertext**
- Decryption Table – a table used to **Decrypt Ciphertext**
- Cryptanalysis - Analyzing **Ciphertext** to determine the **Key** then **Decrypt**

# Code Busters Rules Summary (See Official Rules)

## **Description:**

- “Students will be tested on their ability to decode encrypted messages using cryptanalysis techniques and show skills with ciphers by decrypting a message”
- Team of up to 2 students
- Teams only need pencils and erasers
- Students will not be able to finish the test
- Students may answer the questions in any order



# Cipher Types

• **Atbash** - Mono-alphabetic substitution ATBASH  $\rightleftharpoons$  ZGYZHS

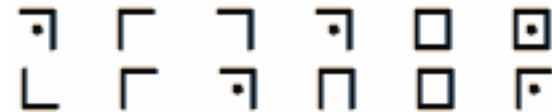
• **Caesar** - Mono-alphabetic substitution CAESAR  $\rightleftharpoons$  DBFTBS

• **Aristocrat** - Mono-alphabetic substitution

• **Vigenère** - Mono-alphabetic substitution with a key

VIGENERE  $\rightleftharpoons$  FMEORCBI

• **PigPen/Masonic** - Symbol based substitution



• **Tap Code** - Substitution Cipher



• **Dancing Men** - Substitution Cipher



# Atbash

The mapping is always the same and reversible  $A \Leftrightarrow Z$   $B \Leftrightarrow Y$   $E \Leftrightarrow V$

Look up each letter in the table and fill in all the matches for that letter.

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

# Caesar

Letter shifts will only be 1-5 characters

Pick a short word and try all the options

<b>Shift</b>	<b>C</b>	<b>A</b>	<b>E</b>	<b>S</b>	<b>A</b>	<b>R</b>
<b>-3 (23)</b>	Z	X	B	P	X	O
<b>-2 (24)</b>	A	Y	C	Q	Y	P
<b>-1 (25)</b>	B	Z	D	R	Z	Q
<b>1</b>	D	B	F	T	B	S
<b>2</b>	E	C	G	U	C	T
<b>3</b>	F	D	H	V	D	U



# Aristocrat

- Monoalphabetic substitution
- Random alphabet
- No letter is mapped to itself
- A hint may be provided depending on the level of difficulty

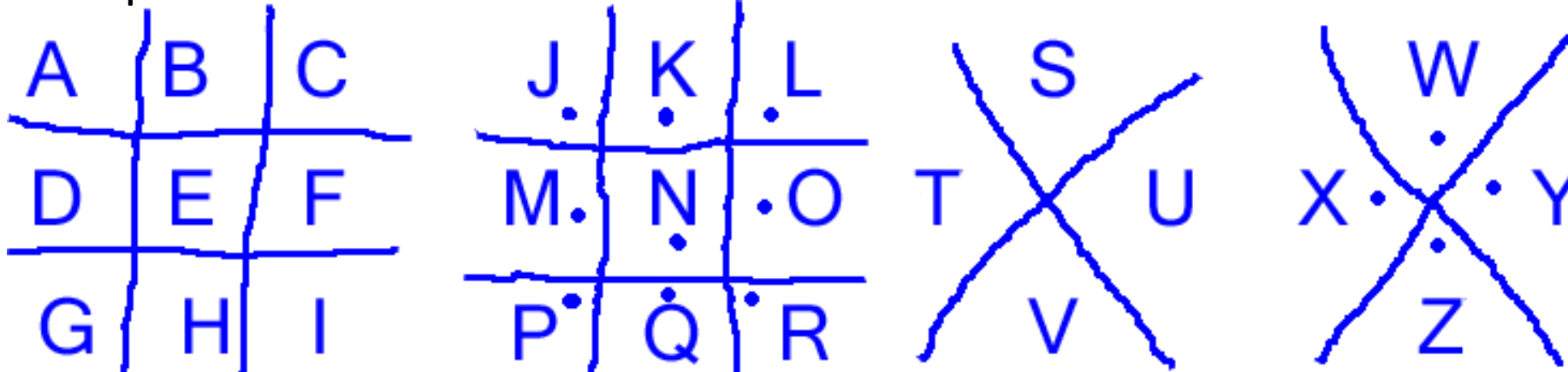
# Vegenère

- Standard substitution cipher with a key
- Write the key on top of the letters making sure to skip spaces, etc.
- Use the key letter as the row in the table to look up the ciphered letter and find the deciphered letter in the column top
- Most common mistakes: Skipping letters when copying the key, looking up the wrong column

	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

# Pigpen/Masonic

The mapping is based on a symbol which is derived from a map which the team needs to memorize



Hence  $\lrcorner$   $\square$   $\Gamma$   $\daleth$   $\boxplus$   $\perp$   $\wedge$   $\triangleright$   $\triangleleft$

Maps to A E I P N L V X Y

# Tapcode

The mapping is based on the position of each letter in a table that they need to memorize.

The row is the 1st number of taps/dots and the column is the 2nd

Hence A is encoded as ● ● (1,1) , E as ● ●●●●● (1,5)  
and Z is the longest at ●●●●● ●●●●● (5,5)

Have the team put marks between each group of 2 and then decode.

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

# Dancing Men

Also known as Running Men

The table of the Dancing Men Characters will be in the resources for the test.  
It looks like this:



These correspond to the letters A-Z and the digits 0-9. Write the letters under each symbol so that you know what they map to. Look up each symbol from the cipher in the table and write the letter under the symbol.

# Codebusters Coaching For Success

- Practice, practice, practice.
- Put two students on the team.
- Divide and conquer ... split the test up with team.
- Learn Pigpen and Tap Code tables
- If stuck, just **try** something!
- Learn pattern words
- What works best for the team?
  - One high point question
  - or five low point questions?

# Codebusters Coaching Strategy

- Atbash
- Caesar
- PigPen
- TapCode
- Dancing Men
- Vigenère
- Aristocrat

# Codebusters Additional Resources

- Macomb Science Olympiad website <https://macombso.org/codebusters>
  - Sample test
  - Video resources
- Science Olympiad CodeBusters <https://toebes.com/codebusters/index.html>
  - Help with how each cipher works
  - Help creating practice test



# Codebusters Questions