

Codebusters

An intro to cryptology, cryptography, and cryptanalysis

Who am I?



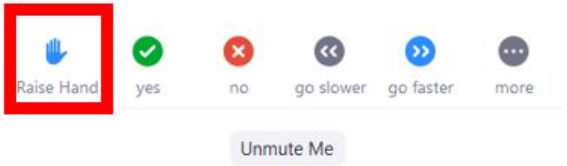
William Lee

- Junior at Mason High School in Ohio
- 3rd year of Science Olympiad (and Codebusters)
- I do Codebusters, Chem Lab, Sounds of Music, Experimental Design, and Ping Pong Parachute

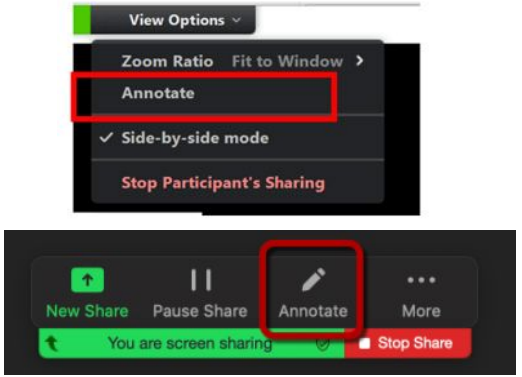
williamlee0416@gmail.com

Zoom Crash Course

Raising your hand



Annotation



Google Classroom

Intro: https://classroom.google.com/c/MjYzNjg5OTU4MDE5?cjc=6d6lap4

Code: 6d6lap4

Advanced: https://classroom.google.com/c/MjY0Mzc4MDMwMDE1?cjc=jtxqgrx

Code: jtxqgrx

This is where I'll post resources + any homework we might have

Terminology

Plaintext: the actual message (what you're trying to say) - HELLO THERE

Ciphertext: the message that has been encoded - ABCCD EABFB

Cryptology: the study of writing and solving codes

Cryptography: the practice of writing and solving codes

Cryptanalysis: decoding a cipher without a given key

Materials

EVENT PARAMETERS:

a. Teams must bring writing utensils with an eraser and may bring up to three (3) stand-alone non-graphing, non-programmable, non-scientific 4-function or 5-function calculators.
b. No resource materials, except those provided by the event supervisor, may be used.
c. The event supervisor will provide scratch paper for each team to use.

Breaking down the rules: Ciphers

Alphabet-based:

- Aristocrat***
- Caesar
- Atbash
- Affine
- Patristocrat Cipher
- Xenocrypt Cipher

Math-based:

- Vigenere
- Baconian Cipher
- Pollux & Morbit Ciphers
- Rail Fence Cipher
- Hill & RSA Ciphers

Cryptograms.org

American Cryptogram Association

Toebes

Monoalphabetic Substitution Ciphers (Monosubs)

Any cipher that is based on one ciphertext letter mapping to one different plaintext letter

- Aristocrats, patristocrats, xenocrypts, etc.

Aristocrats

- Regularly spaced and punctuated messages (monosub)
- The most “normal” cipher
- One letter replaces another letter (but not itself)
    - For example, if the message i was trying to send is “EEE AAA”, it might look like “FFF LLL” in an aristocrat if F maps to E and L maps to A

Format

Pts

If there is a hint, this is where it will be

Directions -->

Timed Question **[300 points]** Solve this Aristocrat quote from Roy T. Bennett When you have solved it, raise your hand so that the time can be recorded and the solution checked.

Cipher -->

ZST DZLX ZR TSUZCLNETVTSK UNS JT TSZCEY KZ GBNLW

GZVTZST'G VZKPHNKPZS KZ UZSKPSCT DPKY N XPRRPUCQK

UYNQQTSET.

Frequency table -->

	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		1	4	2	3		3	1		1	8	3		6		6	3	3	10	11	5	3	1	2	3	12
Replacement																										

Strategies

- Frequency analysis: ETAOIN SHRDLU (not exact but close enough)
- Word patterns: THAT (ABCA)
- Word frequencies: most common word in English is “the”

(There are a lot more advanced methods, but over time you kind of form your own way to do things by mixing them all together - everyone solves in different ways. It will become really easy and natural as you solve more of them.)

**Patristocrats look like aristocrats spaced out in 5 letter groups. Don't get confused, the spaces are not actual spaces, just for viewing comfort.

Walkthrough Aristocrat

SGO OTH OZGOT UQL OTQO TH KNHK XZAR LABNOGKH, OTH

HIHRJ MIAUI SGO OA XHU AI OTNL HQZOT, QIK UTAR AIBJ

OTH LNRYBHLO AX GL QZH XNO OA UNOTLOQIK.

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	
9	3					5	12	7	2	5	7	1	6	18		6	4	2	10	5			4	1	4	

Now try it out yourself

BFZKZ GH SX DZZU SXK TRV SXK FXNK DFZS BVKRSSV LRV

SXB ZSBZK NIXS BFGH WXNSBKV, GC BFZ IZXIOZ OXHZ

BFZGK KXNEFSZHH RST HIGKGB XC TZCGRSWZ.

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
	9	3	2	1	7	7	6	4		10	1		4	2			5	13	3	1	5	2	11		15

Patristocrats

These types of ciphers are similar to aristocrat ciphers except the spaces between the words are removed. Usually, the message will be given to you in groups of five characters and it will be your job to substitute letter to figure out the code.

Useful Tips

- Use a frequency analysis
  - ETAOIN SHRDLU - These are the most common letters (left to right)
    - This is huge since you have to rely less on common word pattern until you have made educated guesses.
    - One strategy is to look at the most frequent letters and try to make the word “the”
- Common Digraphs
  - These are common two letter phrases
    - Examples; th, he, in er, en, re, etc.
- Vowels
  - Vowels are amongst the most frequent letter, but they seldomly appear next to each other. If three high frequency letters are adjacent to each other, they probably not all vowels.

Let's Try an Example!!!

4) **[500 points]** Solve this patristocrat encoded Mark Twain with a K2 alphabet and starts with **I WISH**.

JMJHZ JAPVD IGKWL ZJGVQ ILUHF KQIFZ KFKDP SJQXX

PPIZL KUFJH UJAZL HLQPV XZKQI FZKFM JFZPV FJFJQ

FLDDL AFJHE PSLUF T

	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	3			4	1	12	2	5	5	11	7	8	2			7	6		2	1	4	4	1	3		8
Replacement																										

Cryptograms Solver; Link

JMJHZ JAPVD IGKWL ZJGVQ ILUHF KQIFZ KFKDP SJQXX
PPIZL KUFJH UJAZL HLQPV XZKQI FZKFM JFZPV FJFJQ
FLDDL AFJHE PSLUF T

Xenocrypts

Xenocrypts are mono-substitution ciphers like aristocrats and patristocrats. The difference between aristocrats and xenocrypts are that xenocrypts are in a different language. In Science Olympiad, xenocrypts will always be in Spanish.

Useful Tips

- Use a frequency analysis
  - EAOSRN IDLCT - These are the most common letters (left to right)
    - Using the given frequency table, you can make educated guesses about the identities of certain letters
- Two Letter words
  - El, La, Es, De, etc, are good places to start making educated guesses
- Common Patterns
  - Este (ABCA), Llamo/llego/llevo/etc. (AABCD), Entonces (ABCDBEAF)

Un ejemplo!!!

Cryptograms Solver; Link

MDJ FK FNFACKR IR FV KD CJQIUQCDK ADIFJD MF QIZKYQJ
VRWJF KRV MFADV; FV KD YIQUD ADIFJD.

2) **[300 Points]** Solve this Xenocrypt which is a quote by Albert Einstein in Spanish.

MDJ FK FNFACKR IR FV KD CJQIUQCDK ADIFJD MF QIZKYQJ

VRWJF KRV MFADV; FV KD YIQUD ADIFJD.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	4		3	10		10			6	6	7		3	1				5	4			2	5	1		2	1
Replacement																											

Homework?

Don’t worry about it for this week! Just make sure you make a Puzzle Baron's Cryptograms account * start practicing a little bit, and try to get familiar with both cryptogram.org and Toebes.

Don’t forget about the Event Resources!

https://docs.google.com/document/d/19L2qkWrTsW6P77bJ-zf1ev20_azaaNbN9kFwYBuFwPw/edit?usp=sharing

This assortment of links can get you through the entire learning curve of code, but don’t forget: do your own research as well.