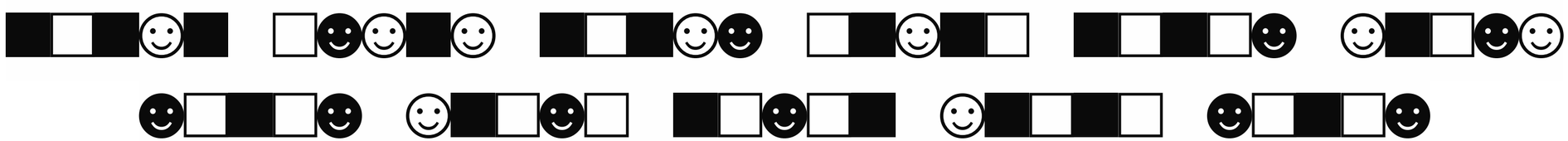


# [Codebusters]

John Toebes

john@toebes.com

# CodeBusters

- Introduction
- How to make things work this year
- Review of code types
- Coaching for success
- Test tools
- Questions

# Introduction

# CodeBusters - 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**
- **Encrypt** - Convert **Plaintext** into **Ciphertext** given a **Key**
- **Cryptanalysis** - Analyzing **Ciphertext** to determine the **Key** then **Decrypt**
- **Crib** - a few known **Plaintext** letters for some **Ciphertext**

# Rule summary

# Codebusters - Rule Summary
## (but see official rules!)

Description:

- "Teams will cryptanalyze and decode encrypted messages using cryptanalysis techniques for historical and modern advanced ciphers."
- Team of up to 3 students

Online Test:

- An online experience intended to mimic the paper test
- Students can communicate via zoom, conference call, etc.
- Up to 3 students collaborating on the same test online
- Up to 3 "simple" calculators: +, -, ×, ÷, %
  (Not a scientific one!)

# Codebusters - Changes

Division C

- Added Railfence cipher with offsets
- Eliminate RSA (it moves to CyperSecurity)
- Add Porta cipher (Vigenère variant)
- K3 Alphabet for Aristocrats and Patristocrats
- Key Phrases for K1/K2/K3 Alphabets
- Key Phrase/Keyword for answer instead of decrypted text
- Special Bonus questions provide 150,450, or 750 points

Division B

- Add Porta cipher (Vigenère variant)

# Special Bonus Questions

Up to three questions on the test will be marked as a special bonus.

- They can not be an Aristocrat/Patristocrat/Xenocrypt
- Solving it means that the answer to the question receives the full amount with no penalty points. (i.e. up to two mistakes on a Baconian or zero mistakes for computing a Hill decryption matrix)
- If a team solves any one of them they are awarded a 150 point bonus
- Solving any two of them results in a 450 point bonus
- Solving all three results in a 750 point bonus

# Codebusters Ciphers

| Cipher | A | B | C |
|---|---|---|---|
| Aristocrat | ✓ | ✓ | ✓ |
| Caesar | ✓ | ✓ | ✓ |
| Vigenère | ✓ | ✓ | ✓ |
| Atbash | ✓ | ✓ | |
| PigPen/ Masonic | ✓ | | |
| Tap Code | ✓ | | |

| Cipher | B | C |
|---|---|---|
| Rail Fence | ✓ | ✓ |
| Baconian | ✓ | ✓ |
| Morbit | ✓ | ✓ |
| Patristocrat | ✓ | ✓ |
| Pollux | ✓ | ✓ |
| Xenocrypt | ✓ | ✓ |
| Affine | ✓ | ✓ |
| Porta | ✓ | ✓ |

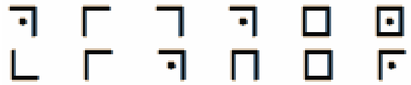
| Cipher | C |
|---|---|
| Hill | ✓ |

Div A

# CodeBusters A - Cipher Types

- **Aristocrat** - Mono-alphabetic substitution
- **Vigenère** - Mono-alphabetic substitution with a key
  VIGENERE ⇄ FMEORCBI
- **Caesar** - Mono-alphabetic substitution CAESAR ⇄ DBFTBS
- **Atbash** - Mono-alphabetic substitution  ATBASH ⇄ ZGYZHS
- **PigPen/Masonic** - Symbol based substitution
- Tap Code - Substitution Cipher

●●●● ●●●● ● ● ●●● ●●●●● ● ●●●
●●● ●●●● ● ●●●● ● ●●●●●



# Codebusters B & C - Regional Code Types

- Aristocrat - Mono-alphabetic substitution
- Patristocrat - Mono-alphabetic substitution without spaces
- Vigenère - Mono-alphabetic substitution with a key VIGENERE ⇄ FMEORCBI
- Caesar - Mono-alphabetic substitution CAESAR ⇄ DBFTBS
- Affine cipher (encryption/*decrypting*)
- Baconian cipher - decryption symbols and words
- Xenocrypt - no more than one in Spanish *(Expect one!)*
- Hill Cipher - (2x2) Encrypting plaintext or decrypting ciphertext, com
- Pollux and Morbit - Decrypting Morse code ciphertext
- *Porta Cipher - Decrypting ciphertext*
- *Railfence Cipher - Decrypting shuffled Ciphertext*

# CodeBusters B - State and National Code Types

- All regional code types
  - Note: Regional tests are intended to be easier than the state test.
- Xenocrypt - at least one cryptogram will be in Spanish
- Cryptanalysis of Vigenère cipher (*at least 5 plaintext given*)
- Affine cipher (mathematical) cryptanalysis (*at least 2 plaintext given*)
- Cryptanalysis of Pollux and Morbit ciphers

# CodeBusters C - State and National Code Types

- All regional code types
  - Note: Regional tests are intended to be easier than the state test.
- Xenocrypt - at least two cryptogram will be in Spanish
- Cryptanalysis of Vigenère cipher (*at least 5 plaintext given*)
- Hill cipher (2x2 or 3x3) Encrypting plaintext or decrypting ciphertext
- Affine cipher (mathematical) cryptanalysis (*at least 2 plaintext given*)
- Cryptanalysis of Pollux and Morbit ciphers

# CodeBusters B/C - Aristocrat/Patristocrat

- Mono-alphabetic substitution - problem classes
  - Aristocrat
    - contains spaces between words; may or may not have a hint.
    - contains spaces between words, but could have spelling and/or grammer[sic] errors; may or may not have a hint.
  - Patristocrat
    - spaces between words are removed (historically represented in blocks of 5 letters); may or may not have a hint.

# Codebusters B/C - Aristocrat/Patristocrat

## Mono-alphabetic substitution

- Random alphabet
- K1 - with a Keyword or *Key Phrase*
- K2
  - Like K1 -- keyword *or key phrase* goes in the replacement
  - Frequency counts encrypted letters in the K2.
  - Decoding has an additional level of indirection.  K2 letter is used to find the replacement letter that maps to the decoded letter (in the K2).
  - (Contrast with a K1, where decoding is done directly by mapping the K1 letter to the replacement letter.)
- K3
  - Like K1 except the same alphabet is used for both alphabets, but shifted

Instead of the decoded phrase, a question may ask for the Keyword/Key Phrase used for the K1/K2/K3 alphabet

# Codebusters B/C - Keyword Answer

Instead of the decoded phrase, a question may ask for the Keyword/Key Phrase used for the K1/K2/K3 alphabet.

Repeated letters in Keyword/Key Phrase are eliminated when constructing the alphabet, but the solution must indicate the dropped letters.

E.g. `THIS IS A KEY PHRASE` would generate an alphabet of

**THISAKEYPRBCDFGJLMNOQUVWXZ**

The answer block shows how many letters are needed



**IMPORTANT:**

When the keyword answer is requested,

**zero** mistakes are required for full credit.

# CodeBusters - Caesar

Letter shifts will only be 1-3 characters

Pick a short word and try all the options

Once a word looks good...
use the Vigenere table to map the others.

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

# CodeBusters - Vigenère

Standard substitution cipher with a key.

This is just like a Caesar cipher but the alphabet shifts with each key letter.

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.

# Codebusters - Porta

Standard substitution cipher with a key.

This is just like Vigenere with a different table with only 13 different possibilities.

Write the key on top of the letters making sure to skip spaces, etc.

For A-M, Use the key letter as the row, find the ciphered letter in the column top and the decoded letter in the key letter row.  For N-Z, the top is the decoded letter and the row letter is the ciphered letter.

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

**We use the ACA Porta table**

# Codebusters B/C - Railfence

This is the only positional cipher.

The solution is found by putting the letters in the correct zigzag order. For example the text TELHERISRA decoded with three rails:

```
T   E   L
 H E R I S
  R   A
```

Produces the answer THREERAILS when the letters are read off in zig zag order.

The encoder tool gives good guidance on the math to figure out the rails.

*For Division C, there can be an offset to the zigzag.*

# Codebusters B/C - K1 vs. K2 in Mono-alphabetic Substitution

- Example: Message: **`Hello world`**
  Keyword/offset: **`keyword/0`**

**MBPPE DEFPG**
**HELLO WORLD**

| K1 | 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 | | 1 | 2 | 1 | 1 | | | | | | 1 | | | 3 | | | | | | | | | | | |
| Replacement | K | E | Y | W | O | R | D | A | B | C | F | G | H | I | J | L | M | N | P | Q | S | T | U | V | X | Z |

**AOGGJ UJNGW**
**HELLO WORLD**

| Replacement | K | E | Y | W | O | R | D | A | B | C | F | G | H | I | J | L | M | N | P | Q | S | T | U | V | X | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K2 | 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 | | | | | | 3 | | | 2 | | | | 1 | 1 | | | | | | 1 | | 1 | | | | |

# Codebusters C - K3 in Mono-alphabetic Substitution

- Example: Message: **Hello world** Keyword/offset: **keyword/1**

**IYMMR ORDMA**
**HELLO WORLD**

| K3 | 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 | | | 1 | | | | | 1 | | | | 3 | | 1 | | | 2 | | | | | | | 1 | |
| Replacement | D | A | B | R | K | C | F | G | H | I | Z | J | L | M | W | N | P | O | Q | S | T | U | Y | V | E | X |

The alphabet is constructed just like a K1/K2, except instead of mapping to the alphabet, it maps to a shifted copy of itself.

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

Div A Div B

MICHIGAN science olympiad

# CodeBusters A/B - Atbash

The mapping is always the same and reversible A ⇄ Z  B ⇄ Y  E ⇄ V

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

# Solving Pollux/Morbit ciphers

Pollux/Morbit - morse code based ciphers

- Morse code table will be given

Morbit

- Say we have 3 symbols: •, -, x. Taking them 2 at a time, we have 9 possible unique groups of 2 characters. Assign them the numbers 1-9. Use ‘x’ as a divider between letters. Use 2 ‘x’ for a divider between words

| | |
|---|---|
| 1 | •• |
| 2 | •- |
| 3 | •x |
| 4 | -• |
| 5 | -- |
| 6 | -x |
| 7 | x• |
| 8 | x- |
| 9 | xx |

# Solving Pollux ciphers

Digits 0-9 represent one of: •, -, x. Typically there is a fairly even distribution of the symbols and they can be in any order.

| | |
|---|---|
| 1 | • |
| 2 | • |
| 3 | • |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | x |
| 8 | x |
| 9 | x |
| 0 | x |

# Solving Morbit ciphers encrypt SOS

**SOS**

••• --- •••

•••x---x•••

•• •x -- -x •• •x

1 3 5 6 1 3

| | |
|---|---|
| 1 | •• |
| 2 | •- |
| 3 | •x |
| 4 | -• |
| 5 | -- |
| 6 | -x |
| 7 | x• |
| 8 | x- |
| 9 | xx |

# Solving Morbit ciphers decrypt 6438

**6348**

-x •x -• x-

-x•x-•x-

- • -• -

T E N T

| | |
|---|---|
| 1 | •• |
| 2 | •- |
| 3 | •x |
| 4 | -• |
| 5 | -- |
| 6 | -x |
| 7 | x• |
| 8 | x- |
| 9 | xx |

# Solving Pollux ciphers decrypt 68184195

**68184195**

-x•x-•x-

- • -• -

T E N T

| | |
|---|---|
| 1 | • |
| 2 | • |
| 3 | • |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | x |
| 8 | x |
| 9 | x |
| 0 | x |

# Coaching for success

# Suggested Teaching Order

1. Aristocrats
2. Caesar and Atbash (Division B)
3. Vigènere and Porta (Division C)
4. Baconian
5. Patriscocrat
6. Pollux and Morbit
7. Affine
8. Hill (2x2 and 3x3) (Division C)
9. Rail Fence
10. Xenocrypt

# CodeBusters - Coaching for Success

- Practice, practice, practice.
- Put three students on the team.
- Divide and conquer … split the test up with team.
- Get really comfortable with “mod 26” and your calculator.
- Take advantage of the “up to two wrong is ok” rule.
- What works best for the team?
  spend time on one 500 point question or five 100 point questions?
- If stuck, just try something!
- Practice, practice, practice…
- Take advantage of the K1/K2/K3 Alphabet
- Look for the special bonus questions
- Learn Morse Code and Baconian alphabet

# Codebusters - What do Teams Struggle with?

- Be familiar with how the online test runs
- Learn Morse Code
- Learn the Baconian Alphabet
- Understand how Baconian Word Problems go
- Understand the Vigenère Table
- Recognize the different ciphers

# CodeBusters - Online Testing this year

- Attempts to replicate the paper experience online
- Students simultaneously take the same test in their own web browser.
- As one student types, the other students see it on their test (like Google docs)
- Everything typed on the test by each student is timestamped and recorded on the server
- Timing is enforced to start all tests at the same time
- Work areas for each problem also shared
- Students can collaborate using phone, hangouts, zoom, etc.
- Coaches can schedule online samples for their own team

# Tools and Demo

# CodeBusters - Test Generation Tools

- https://www.toebes.com/codebusters
- All Regional Tests and the State Test will be generated using this tool
- Great for coaches to generate their own practice tests
- Tool overview video: https://youtu.be/pcz_3ql8ebM
- If you think you find a bug or have suggestions for improvements, enter them at https://github.com/toebes/ciphers/issues
- Questions?  You can email:
  - john@toebes.com (John Toebes)
  - rlabaza@gmail.com (Randy Labaza)

# CodeBusters - Test Generation Tools

MICHIGAN science olympiad

Features of the tools:

- Coaches can generate interactive tests to practice online
- Ciphers are tagged with the division they are used in
- Select the type of test by division and tournament
- All NC tests from all previous tournaments
- Warning messages if hints are not stated in question text
- Warning messages if the cipher used in a question is not valid for the test type.  (Not prohibited from keeping it.)
- Ability to provide custom HTML on the front page of the test
- Schedule a test
- ‘Coach mode’ on a scheduled test, where a coach can ‘join’ the test and make suggestions as the students work the problems.
- System tracks potential copying from external source

# Codebusters - Resources

- https://toebes.com/codebusters/ – has lots of tools for writing exams and solving ciphers.
  (Tool overview video: https://youtu.be/pcz_3ql8ebM)
- http://www.cryptograms.org/tutorial.php – One of the best tutorials for solving Aristocrats.
- http://www.dcode.fr/tools-list#cryptography – Has a lot of tools for encoding/decoding ciphers.
- https://quipqiup.com/ – Solves any Aristocrat or Patristocrat.
- http://www.gregorybard.com/cryptogram.html – includes practice problems and suggested textbooks.

# Codebusters - Practice Sample Resources

- https://toebes.com/codebusters/ – has copies of many previous tests
- http://www.cryptogram.org/ – is the website of the American Cryptogram Association (ACA) if you are looking for even more resources or a fun organization to join.
  *Note: I am a member of the ACA and ACA members have contributed questions for the tests.*
- http://cryptograms.org/ – Puzzle Baron's site with tons of Aristocrats
- http://www.cryptoclub.org/ – Has practice ciphers
- https://www.brainyquote.com/quotes/topics.html –
  a great source of quotes to encode.
  Keep in mind the length of the quotes however.

# Any Questions?

John Toebes

codebusters@toebes.com

Follow us on twitter:

@NCSO_cb