



**NORTH CAROLINA
SCIENCE OLYMPIAD**

Codebusters

Divisions B & C

2025 Coaches Conference

Presented By:

John Toebe & Monica Sieh — National Event Supervisors

codebusters@toebes.com

CAESAR
+ SECRET
= PUZZLE

20

25

Disclaimer

- ◆ This presentation was prepared using draft rules.
- ◆ There may be some changes in the final copy of the Rules.
- ◆ The Rules released in September 2025 will be the official Rules and should be used for all competitions.

Codebusters

- ◆ Introduction and Changes
- ◆ Review of code types
- ◆ New Cipher Types
- ◆ Coaching for success
- ◆ Tools
- ◆ Questions



Introduction and Changes

Codebusters - Rule Summary

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 (2 for Division A)
- ◆ Up to three non-programmable calculators (Class I or II)

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*

Codebusters - Changes



Calculator can be Class II

Misspelled **Aristocrats** are retired

Xenocrypts and **Patristocrats** are encoded with K1(B/C) or K1/K2 (C Only)

New **Checkerboard Cipher**

Special bonus will use at least one **Checkerboard Cipher**



Codebusters Ciphers

Cipher	B	C
Baconian	✓	✓
Cryptarithm	✓	✓
Fractionated Morse	✓	✓
Complete Columnar	✓	✓
Nihilist Substitution	✓	✓
Patristocrat	✓	✓
Porta	✓	✓
Xenocrypt	✓	✓
Checkerboard	✓	✓
Affine	✓	
Hill (2x2 and 3x3)		✓

Cipher	A	B	C
Aristocrat	✓	✓	✓
Caesar	✓	✓	
Atbash	✓	✓	
PigPen/Masonic	✓		
Tap Code	✓		
Dancing Men	✓		
Knights Templar	✓		

Special Bonus Questions

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

- ◆ They will **not** be an [Aristocrat](#)/[Patristocrat](#)/[Xenocrypt](#)
- ◆ One will be the new Checkerboard Cipher
- ◆ 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 a [Cryptarithm](#)
- ◆ Points:
 - ✧ one solved = **+150 points**
 - ✧ two solved = **+450 points**
 - ✧ All three solved = **+750 points**

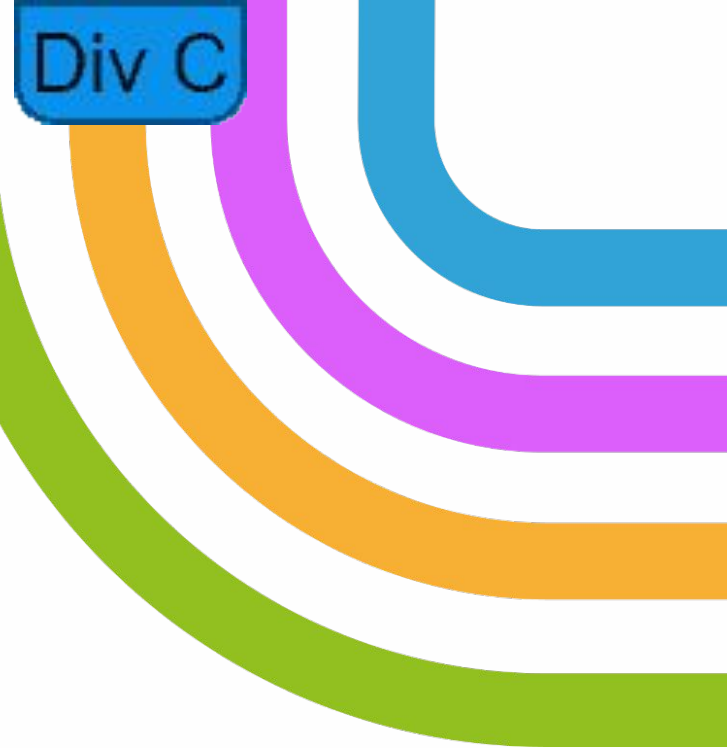


Codebusters B - Regional Code Types

Aristocrat	Mono-alphabetic substitution
Patristocrat	Mono-alphabetic substitution without spaces
Caesar	Mono-alphabetic substitution CAESAR $\rightleftharpoons$ DBFTBS
Atbash	Mono-alphabetic substitution ATBASH $\rightleftharpoons$ ZGYZHS
Complete Columnar	Positional cipher (9 or less columns)!
Checkerboard	Polybius Square with three keys
Affine	Math decryption with a formula
Baconian	Decrypting symbols and words
Porta	Decrypting ciphertext
Xenocrypt	No more than one in Spanish (<i>Expect one!</i>)
Nihilist Substitution	Math decryption with two keys
Fractionated Morse	Decrypting Morse code with a keyword
Cryptarithm	Math problems with letters for numbers

Codebusters B - State and National Code Types

- ◆ All regional code types
 - ◆ Note: State and National tests are intended to be harder than Regionals
- ◆ **Xenocrypt** - at least one cryptogram will be in Spanish
- ◆ Cryptanalysis of **Porta** cipher (*at least 3 plaintext given*)
- ◆ Cryptanalysis of **Affine** cipher (*at least 2 plaintext given*)
- ◆ Cryptanalysis of **Nihilist** cipher (at least double the length of keyword plaintext given)
- ◆ Cryptanalysis of **Checkerboard** cipher (at least 4 letters revealed)



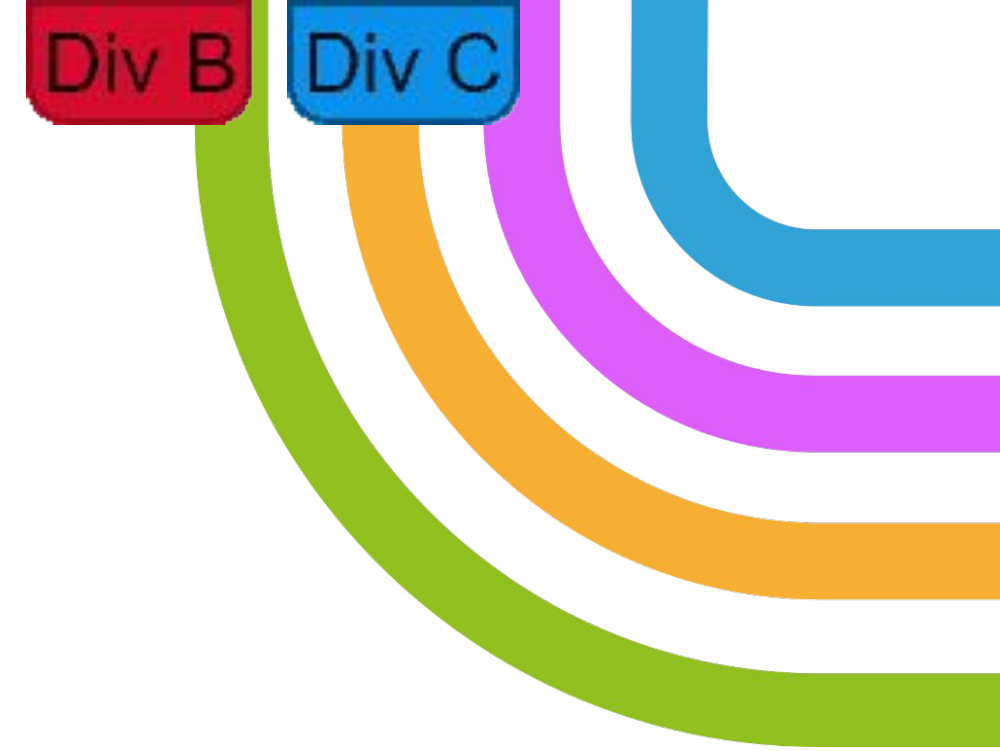
Codebusters C - Regional Code Types

Aristocrat	Mono-alphabetic substitution
Patristocrat	Mono-alphabetic substitution without spaces
Baconian	Decrypting symbols and words
Xenocrypt	No more than two in Spanish (Expect one!)
Hill	Matrix Math decryption with a keyword
Nihilist Substitution	Math decryption with two keys
<i>Checkerboard</i>	Polybius Square with three keys
Fractionated Morse	Decrypting Morse code with a keyword
Porta	Decrypting ciphertext with a keyword
Complete Columnar	Positional cipher (9 or less columns)!
Cryptarithm	Math problems with letters for numbers

Codebusters C - State and National Code Types

- ◆ All regional code types
 - ◆ Note: State and National tests are intended to be harder than Regionals
- ◆ **Xenocrypt** - at least **two** cryptograms will be in Spanish
- ◆ **Cryptanalysis** of **Porta** cipher (*at least 3 plaintext given*)
- ◆ **Cryptanalysis** of **Affine** cipher (*at least 2 plaintext given*)
- ◆ **Hill** cipher (2x2 or 3x3) - Decrypting ciphertext
- ◆ **Cryptanalysis** of **Nihilist** cipher (at least double the keyword *length* plaintext given)
- ◆ **Cryptanalysis** of **Checkerboard** cipher (at least 4 letters revealed)

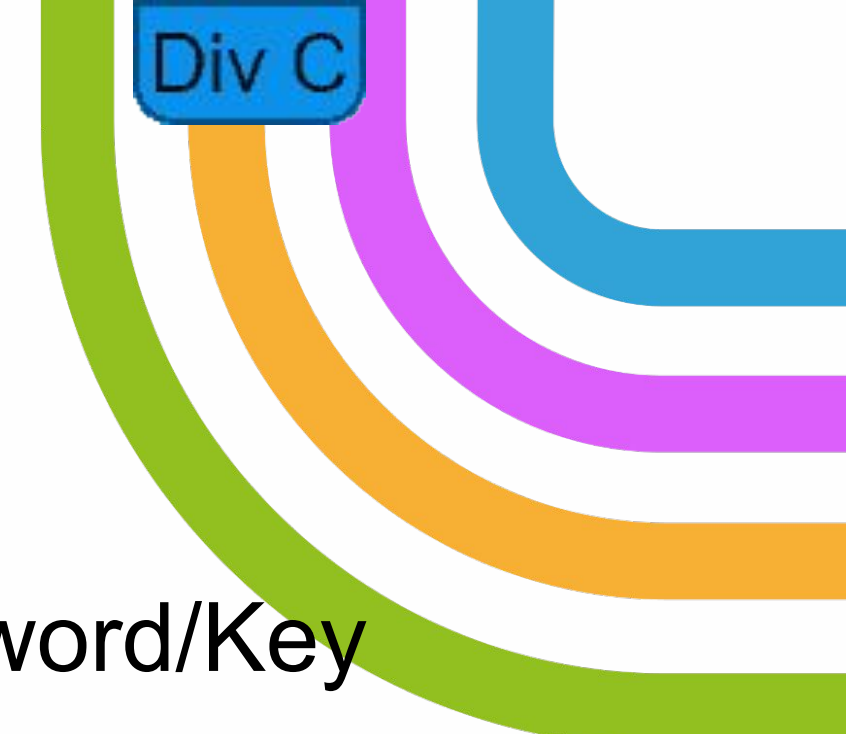
Codebusters B/C - Aristocrat/Patristocrat



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 (Division C Only)**
 - ◆ Like K1 except that the alphabet is used for both alphabets, but is shifted by an amount

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



Codebusters C - Keyword Answer

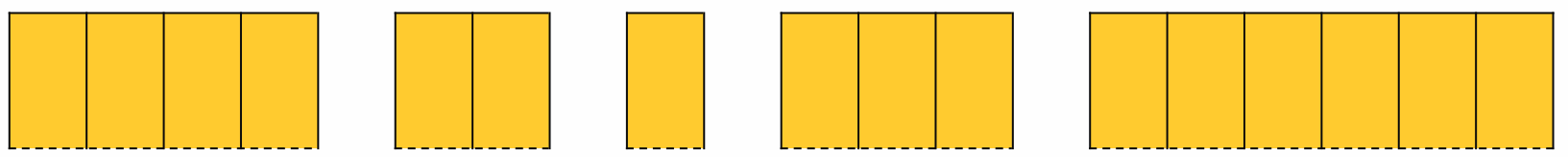
Instead of the decoded phrase, a question may ask for the Keyword/Key Phrase used for the **K1/K2/K3** alphabet.

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

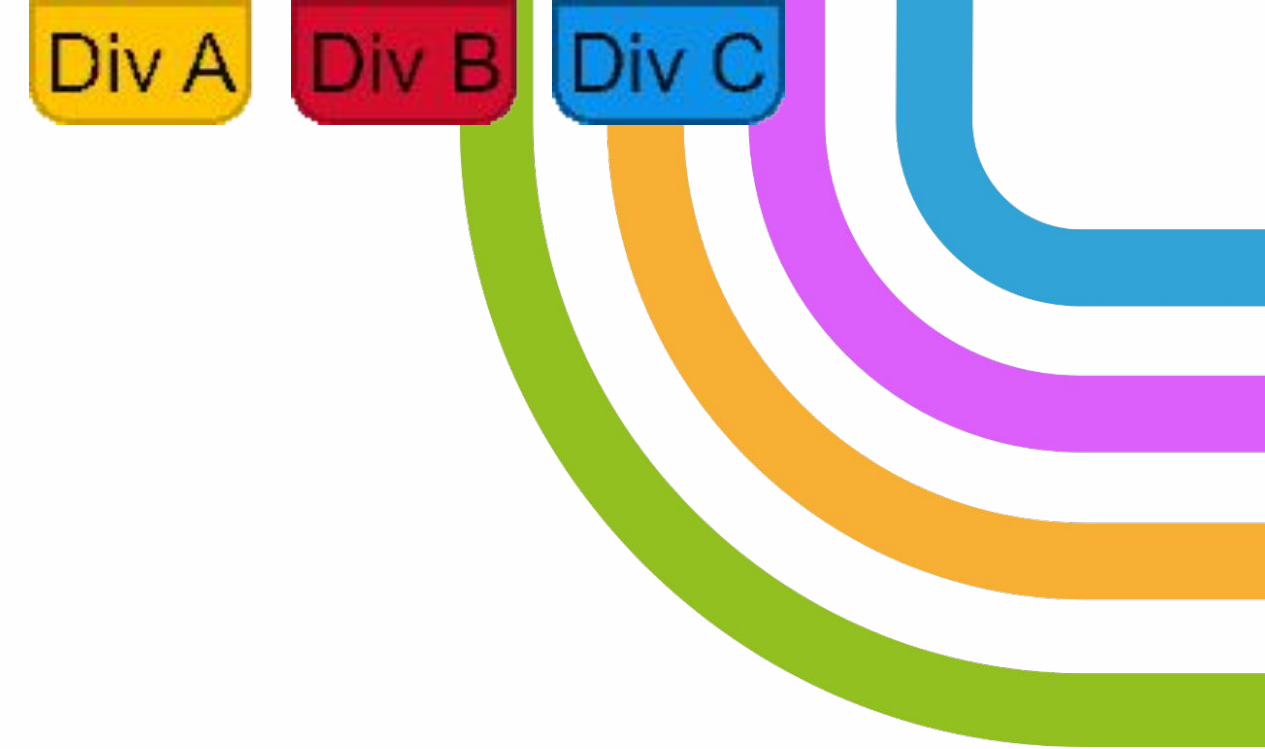
E.g. **THIS IS A KEY PHRASE** would generate an alphabet of

THISAKEYPRBCDEFGJLMNOQUVWXZ

The answer block would show how many letters are needed



NOTE: When the keyword answer is requested, zero mistakes are required for full credit.

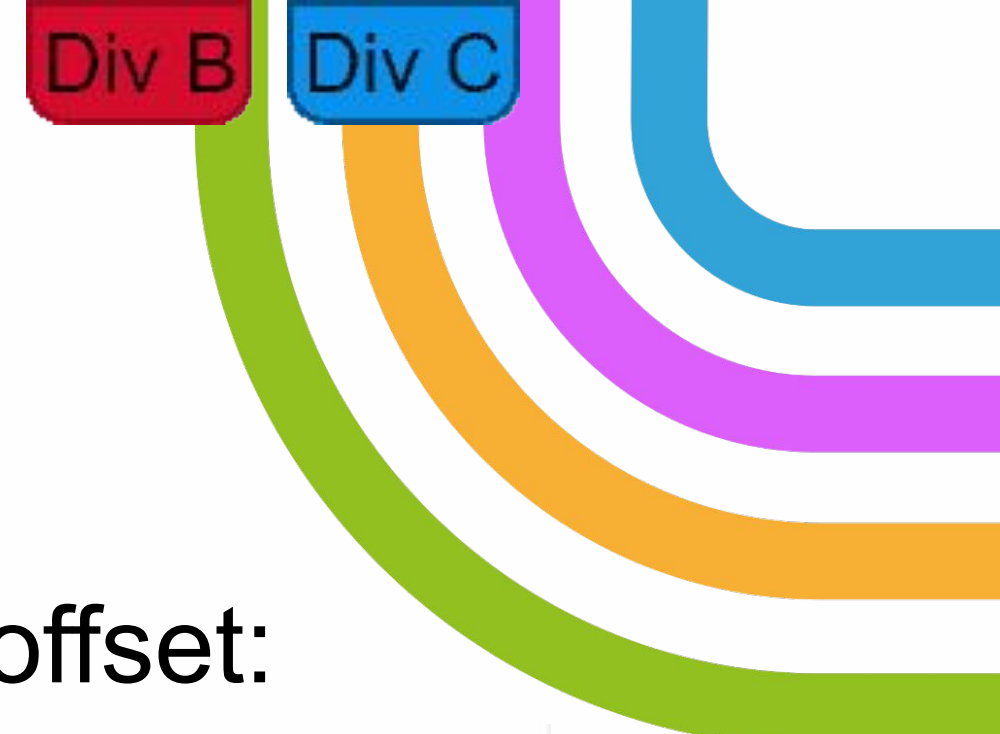


Codebusters B/C - Aristocrat/Patristocrat

Mono-alphabetic substitution - problem classes

- ♦ Aristocrat
contains spaces between words; 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.

Note: Quotes may still have grammar and spelling mistakes based on the origin of the quote

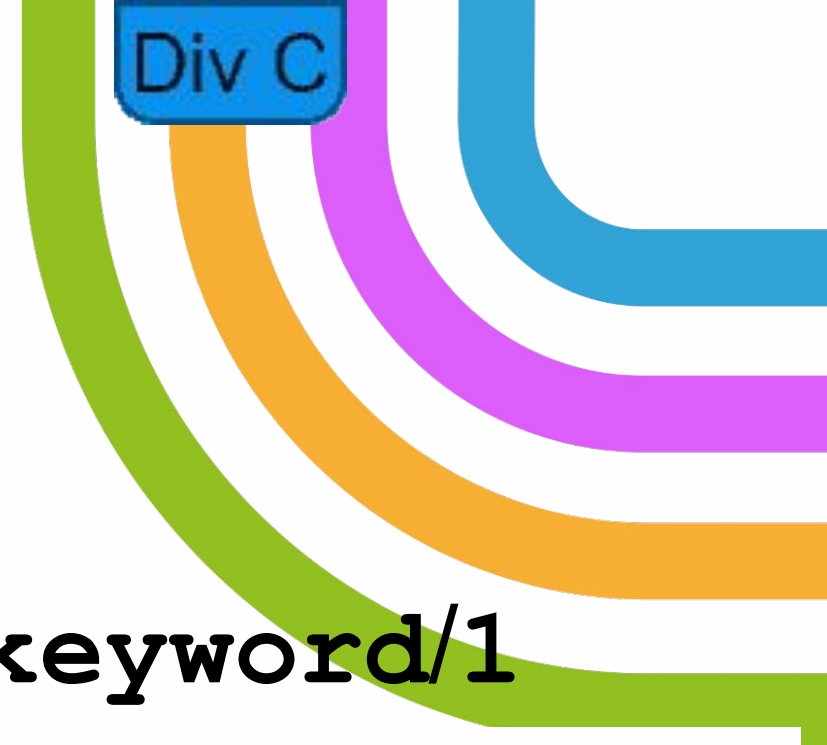


Codebusters B/C - K1 vs. K2 in Mono-alphabetic Substitution

Example: Message: **Hello world** Keyword/offset:

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



Codebusters - Porta

Standard substitution cipher with a key.

This is decoded with a table that has only 13 possibilities.

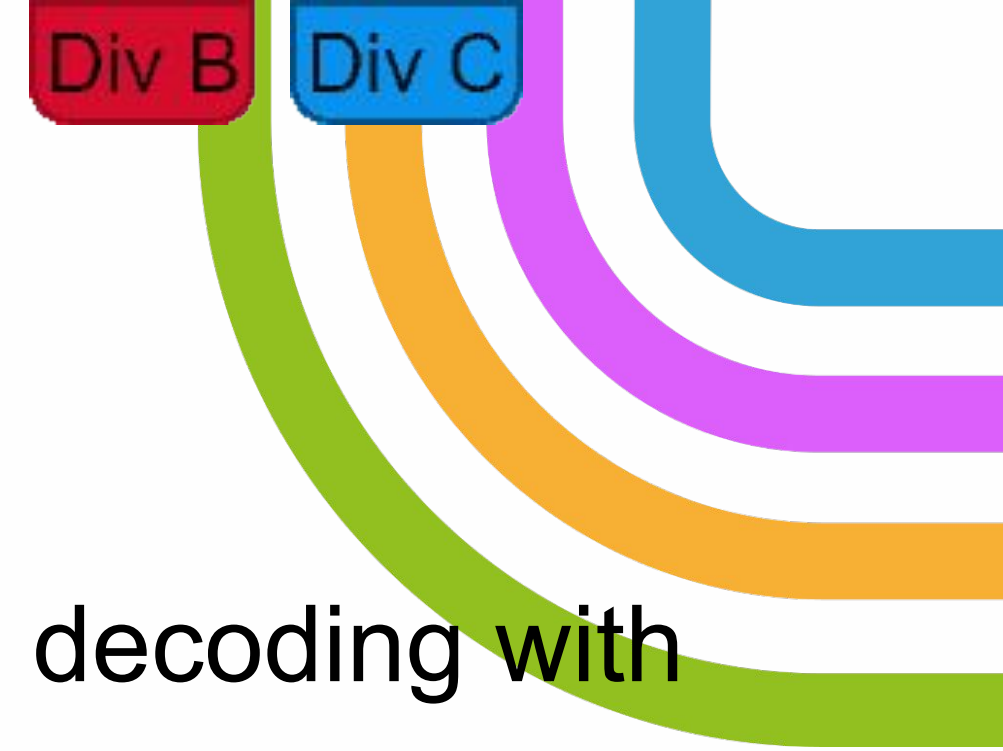
Write the key on top of the letters making sure to skip spaces, etc.

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

Codebusters B/C - Fractionated Morse



The Fractionated Morse Cipher combines morse code decoding with the keywords of a **K1/K2** alphabet.

The keyword determines the mapping of the cipher alphabet to Morse pieces.

The first letter in the keyword will always map to **●●●** and the last letter of the alphabet (typically **Z** if it isn't in the keyword) will map to **××—**

This mapping along with morse code rules make it possible to solve

Codebusters B/C - Fractionated Morse

Morse Code Based Cipher with a Keyword

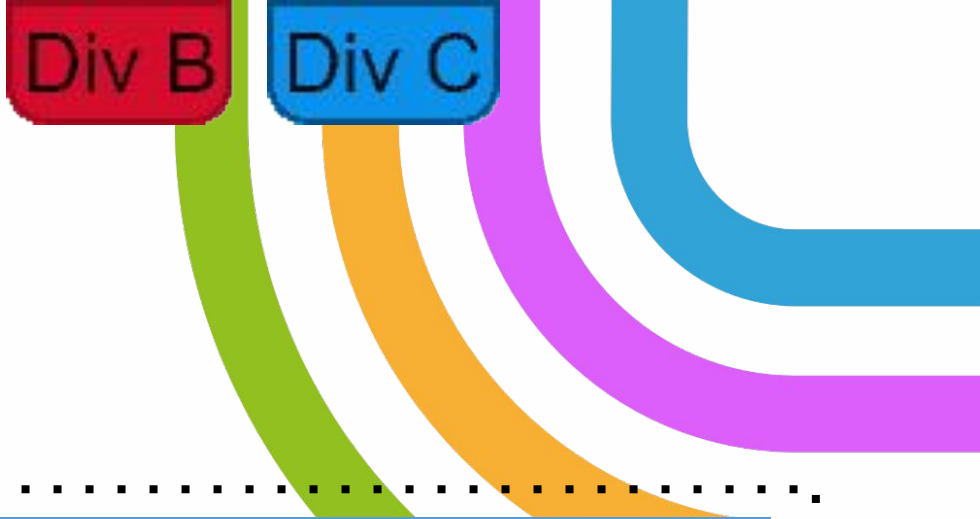
F	A	J	C	S	C	D	R	K	V	D	G	K
—●—●x—	—x—	—x—●●x●x—	●●●x●●—	x●●●x—	x●●●x—	x●●●x—	x●●●x—	x●●●x—	x●●●x—	x●●●x—	x●●●x—	x●●●x—
C	C	D	E	B	U	S	T	E	R	S		
Z	W	P	Q	G	K	D	Q	D	Y			
xx—●—●x●●x●—	—●x●●●●x●x●—	●x●●●●x										
C	I	P	H	E	R	S						

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
•	•	•	•	•	•	•	•	•	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X
•	•	•	-	-	-	X	X	X	•	•	•	-	-	-	X	X	X	•	•	•	-	-	-	X	X
•	-	X	•	-	X	•	-	X	•	-	X	•	-	X	•	-	X	•	-	X	•	-	X	•	-

Codebusters B/C - Cryptarithms

Mathematical operations with Letters

- ◆ Must determine what numbers map to which letters
- ◆ Answer will be one or more words with the order given
- ◆ Problems will have exactly one solution
- ◆ Leading letters will never be 0



CAESAR	158752
+ SECRET	+ 781286
PUZZLE	940038

SEPARATE CLUES
78952568 13487

Codebusters B/C - Nihilist Substitution



Polybius Key: **SCIENCE** **OLYMPIAD**

Two keywords: Polybius Square and encoding.

- ◆ Polybius Square constructed like K1/K2 alphabet except I/J map to the same spot. Letters are placed in the square in row order.
- ◆ The value for the letter is the *row**10+*column*.
- ◆ The Polybius Square values are used to encode both the keyword and the plaintext.
- ◆ If we use an encoding keyword of CODE which maps to 12 21 32 14

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

PlainText	A	G	O	O	D	P	H	R	A	S	E
Encoded	31	35	21	21	32	25	41	44	31	11	14
Keyword	12	21	32	14	12	21	32	14	12	21	32
Encoding	43	56	53	35	44	46	73	58	43	32	46

Codebusters B/C - Checkerboard

Polybius Key: **SCIENCE** **OLYMPIAD**

Three keywords: Polybius Square, Row and Column

- ◆ The CipherText is exactly twice the length of the plaintext
- ◆ Polybius Square constructed like K1/K2 alphabet except I/J map to same spot. Letters are placed in the square in row order.
- ◆ The Row and Column keywords are used to encode the letters.
- ◆ Given the Ciphertext it is possible to anagram the Row and Column keywords.
- ◆ If you treat the letters as individual symbols, it is possible to solve like a Patristocrat

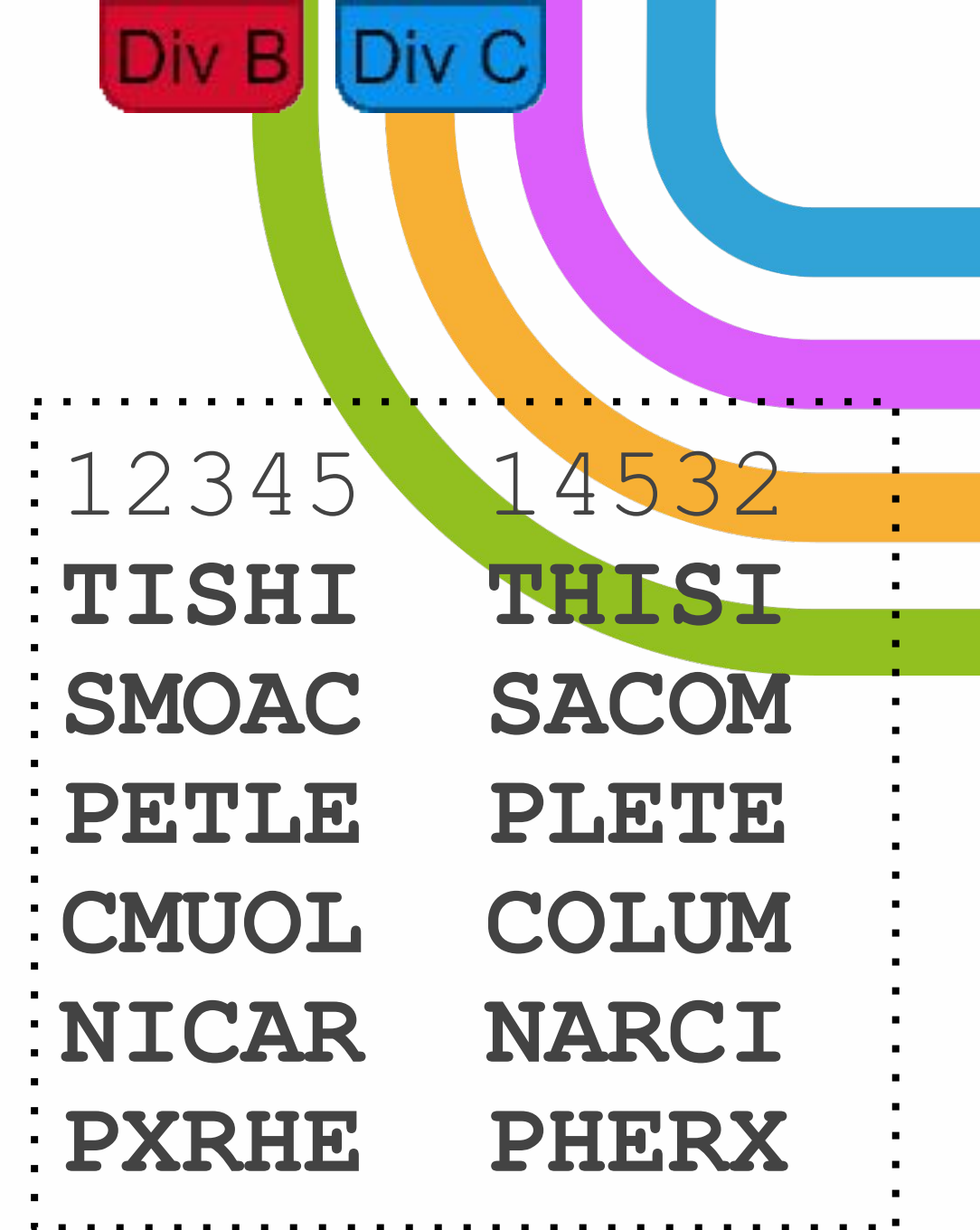
	W	O	R	D	S
G	S	C	I/J	E	N
R	O	L	Y	M	P
E	A	D	B	F	G
A	H	K	Q	R	T
T	U	V	W	X	Z

PlainText	A	G	O	O	D	P	H	R	A	S	E
Ciphertext	EW	ES	RW	RW	EO	RS	AW	AD	EW	GW	GD

Codebusters B/C - Complete Columnar

A transposition cipher based on columns

- ◆ Given a cipher of
TSPCN PIMEM IXSOT UCRHA LOAHI CELRE
We note that it is exactly 30 letters which factors into $3 \times 2 \times 5$ which tells us it is either 3, 5 or 6 columns.
- ◆ Taking a guess at 5 columns we can write it out and look for clues
- ◆ Looking at the last row we see the X which is likely padding
- ◆ That leaves PRHE which must PHER giving us a column order of 14532.
- ◆ Reading the rows off in that order gives us:
THIS IS A COMPLETE COLUMNAR CIPHER X





Coaching for success

Codebusters - Coaching for Success

- ◆ Practice, practice, practice.
- ◆ Put **three students** on the team.
- ◆ Divide and conquer ... split the test up with team.
- ◆ Learn **Morse Code** and **Baconian** alphabet
- ◆ Take advantage of the “**up to two wrong is ok**” rule.
- ◆ What works best for the team?
 - ✧ One 500 point question
 - ✧ or five 100 point questions?

Codebusters - Coaching for Success

- ♦ If stuck, just **try** something!
- ♦ Practice, practice, practice...
- ♦ Take advantage of the **K1/K2/K3** Alphabet
- ♦ Look for the **special bonus questions**
- ♦ Get really comfortable with “**mod 26**” and your calculator
- ♦ Learn **pattern words**
- ♦ Learn cryptarithm math rules

Codebusters B - Coaching Strategy

1. Aristocrat
2. Caesar and Atbash
3. Porta
4. Letter/Symbol Baconian
5. Aristocrat K1 Keyword
6. Patristocrat
7. Fractionated Morse
8. Nihilist Substitution
9. Checkerboard
10. Word Baconian
11. Affine
12. Complete Columnar
13. Cryptarithm
14. Xenocrypt

Codebusters C - Coaching Strategy

1. Aristocrat
2. Porta
3. Letter/Symbol Baconian
4. Aristocrat K1/K2 Keywords
5. Aristocrat K3 Keyword
6. Patristocrat
7. Fractionated Morse
8. Nihilist Substitution
9. Checkerboard
10. Word Baconian
11. Hill 2x2
12. Complete Columnar
13. Cryptarithm
14. Xenocrypt
15. Hill 3x3

Codebusters - Additional Resources

- ◆ National event page
 - ✧ <https://www.soinc.org/codebusters-c>
 - ✧ <https://www.soinc.org/codebusters-b>
- ◆ NCSO event page
 - ✧ <https://ncscienceolympiad.ncsu.edu/resources/elementary/codebustersa>
 - ✧ <https://ncscienceolympiad.ncsu.edu/codebusters-b>
 - ✧ <https://ncscienceolympiad.ncsu.edu/resources/high-school/codebusters>
- ◆ **Codebusters Overview Document**
- ◆ Your favorite search engine
- ◆ Questions: codebusters@toebes.com

Codebusters - Test Generation Tools

- ◆ <https://www.toebes.com/codebusters>
- ◆ Great for coaches to generate their own practice tests
- ◆ New Test Builder: <https://toebes.com/codebusters/TestBuild.html>
- ◆ Provides guidance on how to solve many ciphers
- ◆ 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:
 - ✧ codebusters@toebes.com

Codebusters - Test Generation Tools

Features of the tools:

- ◆ Coaches can generate tests for practice
- ◆ 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
- ◆ Warns if hints are not stated in question text
- ◆ Warns if cipher used in a question is not valid for the test type.
(Not prohibited from keeping it.)

*** Codebusters - Questions?



youtube.com/@Codebusters-sciol



Follow us on X:

 **@NCSO_cb**

THANK YOU FOR PARTICIPATING!

Here's to an amazing season ahead.

