Science Olympiad at Georgia Tech®

Codebusters

Division B/C

Georgia Tech Event Workshop Series
2024-25

A Bit About Me & This Workshop

- **Hi, I’m Klebb**!
  - Senior at the University of Illinois Urbana-Champaign
  - Mathematics & Secondary Education
  - Previously Hopkins JHS, Mission San Jose HS (CA-N)
  - Competed 2014 - 2021, Volunteering/ESing/etc. 2021 - Now
- This workshop will be similar to the 2024 Sierra Vista & UT Workshops
  - I wrote and presented at SV, and helped prepare the UT one too.
  - There’s some new stuff, but some of it is repeated :/

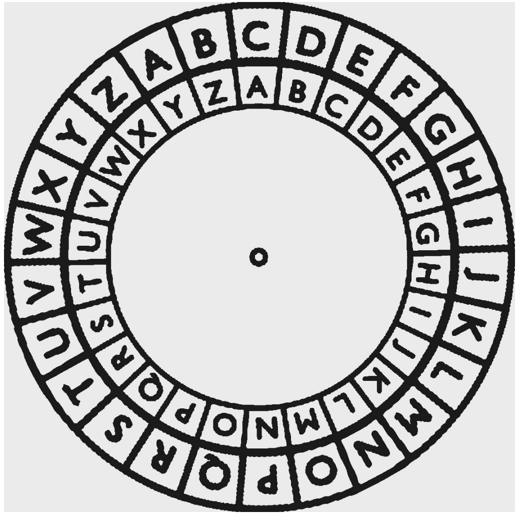
01 RULES

02 MICRO-STRATEGIES

03 MACRO-STRATEGIES

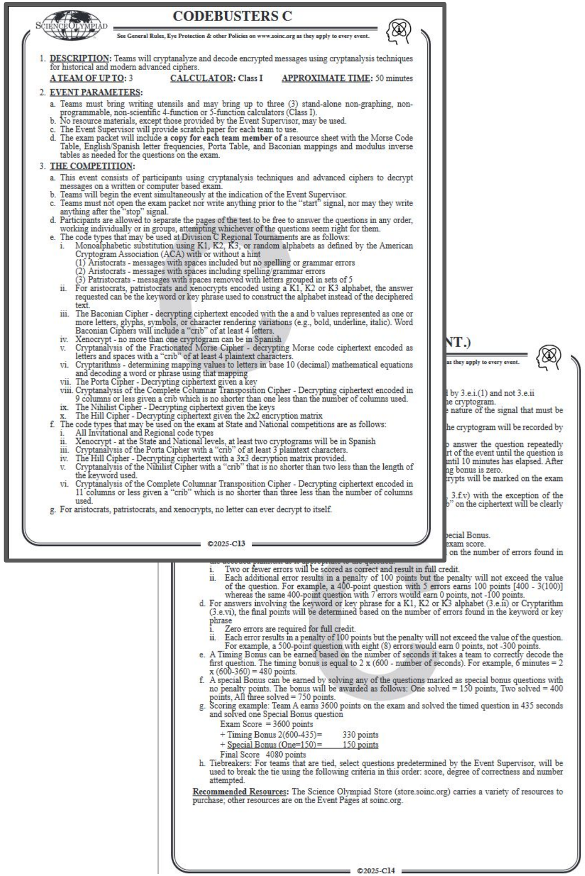
04 HOW TO LEARN

05 RESOURCES / LINKS


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
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

What’s in the Rules?

- **Cipher List 2024 - 2025:**
  - Aristocrats (Random, K1, K2, K3 (C only), Error)
  - Patristocrats
  - Spanish Aristocrats (Xenocrypts)
  - Baconian
  - Fractionated Morse
  - Cryptarithms
  - Porta
  - Complete Columnar
  - Nihilist
  - Hill (C only)
  - Affine, Atbash, Caesar (B only)



CODEBUSTERS C

See General Rules, Eye Protection & other Policies on www.soinc.org as they apply to every event.

1. **DESCRIPTION:** Teams will cryptanalyze and decode encrypted messages using cryptanalysis techniques for historical and modern advanced ciphers.

   A TEAM OF UP TO: 3 **CALCULATOR:** Class I **APPROXIMATE TIME:** 50 minutes
2. **EVENT PARAMETERS:**
   a. Teams must bring writing utensils and may bring up to three (3) stand-alone non-graphing, non-programmable, non-scientific 4-function or 5-function calculators (Class I).
   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.
   d. The exam packet will include **a copy for each team member of** a resource sheet with the Morse Code Table, English/Spanish letter frequencies, Porta Table, and Baconian mappings and modulus inverse tables as needed for the questions on the exam.
3. **THE COMPETITION:**
   a. This event consists of participants using cryptanalysis techniques and advanced ciphers to decrypt messages on a written or computer based exam.
   b. Teams will begin the event simultaneously at the indication of the Event Supervisor.
   c. Teams must not open the exam packet nor write anything prior to the “start” signal, nor may they write anything after the “stop” signal.
   d. Participants are allowed to separate the pages of the test to be free to answer the questions in any order, working individually or in groups, attempting whichever of the questions seem right for them.
   e. The code types that may be used at Division C Regional Tournaments are as follows:
      i. Monoalphabetic substitution using K1, K2, K3, or random alphabets as defined by the American Cryptogram Association (ACA) with or without a hint
         (1) Aristocrats - messages with spaces included but no spelling or grammar errors
         (2) Aristocrats - messages with spaces including spelling/grammar errors
         (3) Patristocrats - messages with spaces removed with letters grouped in sets of 5
      ii. For aristocrats, patristocrats and xenocrypts encoded using a K1, K2 or K3 alphabet, the answer requested can be the keyword or key phrase used to construct the alphabet instead of the deciphered text.
      iii. The Baconian Cipher - decrypting ciphertext encoded with the a and b values represented as one or more letters, glyphs, symbols, or character rendering variations (e.g., bold, underline, italic). Word Baconian Ciphers will include a “crib” of at least 4 letters.
      iv. Xenocrypt - no more than one cryptogram can be in Spanish
      v. Cryptanalysis of the Fractionated Morse Cipher - decrypting Morse code ciphertext encoded as letters and spaces with a “crib” of at least 4 plaintext characters.
      vi. Cryptarithms - determining mapping values to letters in base 10 (decimal) mathematical equations and decoding a word or phrase using that mapping
      vii. The Porta Cipher - Decrypting ciphertext given a key
      viii. Cryptanalysis of the Complete Columnar Transposition Cipher - Decrypting ciphertext encoded in 9 columns or less given a crib which is no shorter than one less than the number of columns used.
      ix. The Nihilist Cipher - Decrypting ciphertext given the keys
      x. The Hill Cipher - Decrypting ciphertext given the 2x2 encryption matrix
   f. The code types that may be used on the exam at State and National competitions are as follows:
      i. All Invitational and Regional code types
      ii. Xenocrypt - at the State and National levels, at least two cryptograms will be in Spanish
      iii. Cryptanalysis of the Porta Cipher with a “crib” of at least 3 plaintext characters.
      iv. The Hill Cipher - Decrypting ciphertext with a 3x3 decryption matrix provided.
      v. Cryptanalysis of the Nihilist Cipher with a “crib” that is no shorter than two less than the length of the keyword used.
      vi. Cryptanalysis of the Complete Columnar Transposition Cipher - Decrypting ciphertext encoded in 11 columns or less given a “crib” which is no shorter than three less than the number of columns used.
   g. For aristocrats, patristocrats, and xenocrypts, no letter can ever decrypt to itself.

©2025-C13

NT.)

as they apply to every event.

by 3.e.i.(1) and not 3.e.ii
he cryptogram.
nature of the signal that must be

he cryptogram will be recorded by

answer the question repeatedly
rt of the event until the question is
ntil 10 minutes has elapsed. After
ng bonus is zero.
rypts will be marked on the exam

, 3.f.v) with the exception of the
b” on the ciphertext will be clearly

pecial Bonus.
exam score.
on the number of errors found in

i. Two or fewer errors will be scored as correct and result in full credit.
ii. Each additional error results in a penalty of 100 points but the penalty will not exceed the value of the question. For example, a 400-point question with 5 errors earns 100 points [400 - 3(100)] whereas the same 400-point question with 7 errors would earn 0 points, not -100 points.

d. For answers involving the keyword or key phrase for a K1, K2 or K3 alphabet (3.e.ii) or Cryptarithm (3.e.vi), the final points will be determined based on the number of errors found in the keyword or key phrase
   i. Zero errors are required for full credit.
   ii. Each error results in a penalty of 100 points but the penalty will not exceed the value of the question. For example, a 500-point question with eight (8) errors would earn 0 points, not -300 points.
e. A Timing Bonus can be earned based on the number of seconds it takes a team to correctly decode the first question. The timing bonus is equal to 2 x (600 - number of seconds). For example, 6 minutes = 2 x (600-360) = 480 points.
f. A special Bonus can be earned by solving any of the questions marked as special bonus questions with no penalty points. The bonus will be awarded as follows: One solved = 150 points, Two solved = 400 points, All three solved = 750 points.
g. Scoring example: Team A earns 3600 points on the exam and solved the timed question in 435 seconds and solved one Special Bonus question

   Exam Score = 3600 points
   + Timing Bonus 2(600-435)= 330 points
   + Special Bonus (One=150)= 150 points
   Final Score 4080 points
h. Tiebreakers: For teams that are tied, select questions predetermined by the Event Supervisor, will be used to break the tie using the following criteria in this order: score, degree of correctness and number attempted.

Recommended Resources: The Science Olympiad Store (store.soinc.org) carries a variety of resources to purchase; other resources are on the Event Pages at soinc.org.

©2025-C14

Rules, Cont.

- **Timed Question:**
  - 1st question: solve within 10 minutes for bonus points!
  - Bonus = 2 * (600 - time taken in s)
- **Up to 3 Special Bonus questions**
  - Not Aristocrats, Patristocrats, or Xenocrypts
- **Scoring:**
  - 2 or fewer errors: full credit
  - Each error over 2 = 100 point penalty (min. of zero)
  - Cryptarithms & Key Extraction (C only) do **not** have this 2-error buffer
- **Materials:**
  - 4 or 5 function calculators, not scientific/graphing!
- **Please go read the rules for yourself for all the details**

Vocabulary

- **Plaintext** - the original message before it has been encoded
- **Ciphertext** - the encoded message
- **Cipher** - a reversible process that transforms plaintext to ciphertext and back
- **Key** - information that is input into an encoding process to generate the relationship between the plaintext and ciphertext
- **Monoalphabetic** - each plaintext letter encodes to the same ciphertext letter every time
- **Polyalphabetic** - each plaintext letter encodes to a different ciphertext letter

MICRO-STRATEGIES

Aristocrats are #1

- The most **fundamental cipher** in all of Codebusters
  - Make sure that **everyone** is proficient at them, no matter your role
  - They make up around **~30%** of tests (and TQ)!
  - Aristocrat skills **transfer to other ciphers** very well
- **Phases of Aristocrat Solves:**
  - **Break-in**: first observations you make
  - **A-ha**: observations that give new information based on your break-in(s)
  - **Fill-in**: filling in letters you already know and letters that only appear once or twice to finish
  - Fill-in tends to take the most time, but the other two are harder

Frequency is Overrated

- Aristocrats can be solved on **4** levels:
    - **Letters**: one letter at a time (writing in all the E’s, T’s, etc.)
    - **Letter Combinations:** parts of words (-TION, -ING, -MENTE, etc.)
    - **Words:** especially word patterns (PEOPLE, NOTHING, THAT, etc.)
    - **Phrases +:** grammatical pieces (e.g., ONE OF THE…)
- In general, think **bigger** than you first expect.
    - **Word patterns** are your best friend for break-in
    - Filling is much faster if you think about **reasonable phrases and sentences** instead of going letter-by-letter
    - A-ha’s come from realizing that a **word makes sense** in the plaintext
    - Letter frequency **isn’t useless**, but don’t over-rely on it!

Grammar & Syntax

- Remember that languages have rules!
- Knowing what **parts of speech** are possible in a sentence can narrow down your options a lot!
  - For example, 2021 GGSO #13
- Small rules like **subject-verb agreement** can give you free letters/words!
  - For example, ARE vs. IS, or an S at the end of a noun/verb
- Punctuation can give conjunctions, contractions, etc.
- **Spanish** has much more well-defined rules!
  - Learn how Spanish's grammar works, for example:
    - "-MENTE" changes an adjective to an adverb
    - Most nouns have a [gendered] article (e.g., UN, LA) before them
  - You can get by with a very limited vocabulary, speaking from experience!

Misc. Cipher Tips

- **Patristocrats**
  - Play aggressive! (More on this later)
  - Practice abusing K-alphabets (JK, VWXYZ, aggressive fill-ins)
    - This goes for Fractionated Morse too!
  - Scan the entire ciphertext first before starting (repeated letter combos!)
- **Baconian**
  - Stop writing A's and B's and start writing dots
  - BBxxx does not exist in Baconian
  - Think big picture: does what you're writing down make sense?
- **Hill & Affine**
  - Use negative numbers (and leverage 0, 13, and previous calculations)
  - Don't decode everything

Misc. Cipher Tips - Cont.

- **Cryptarithms**
  - Use the answer line to your advantage
    - E.g., every word needs vowels, letter combos may be impossible
    - You usually don’t need to solve for the entire calculation
  - Google how to take square roots by hand!
- **Two Question Types for Another Time:**
  - K3 Keyword Extraction
  - Nihilist Cryptanalysis
  - Read the guide at toebes.com/codebusters for worked examples
  - Then practice, practice, practice! (more on this later)
- **Complete Columnar**
  - Stack columns on top of each other!

MACRO-STRATEGIES

Timed Question

- Put **at least 2 people** on timed question!
  - 3-person setups can work
  - Some top teams do 1 person on timed, but this is not recommended for most teams
- The main point is to speed up **fill-in**
  - Write simultaneously (one right-handed and one left-handed is great!)
  - Putting your brains together is a secondary help
  - Split up who is writing on what part of the question
- Transition into the test as quickly as possible
  - Have one person look through the rest of the test as the others finish
  - Get started on something else while your TQ is getting checked!

The Test & Roles

- **Have a plan going in** of who is doing what ciphers
  - Find roles that work for your team based on your individual abilities
  - Be flexible! Adapt your plan to the needs of the test
  - Example (based on my old team; ciphers were different back then):
    - **Person 1**: TQ -> Aristocrats -> Caesar/Atbash/Affine -> Flex
    - **Person 2**: TQ -> Patristocrats -> Baconian -> Xenocrypt -> Flex
    - **Person 3**: Scout -> Pollux/Morbit -> Vigenere -> Flex
- Designate a **team leader/shotcaller** to make final decisions
- Keep morale up!
  - Make “All good” your motto mid-test
  - You can discuss what went right and wrong later

Endgame

- **Final 10-15 minutes**: SHIFT GEARS!
  - Move from “doing the test” to **finishing individual questions**
  - Remember, you only get points for (mostly) finishing questions
  - Ending with 3 questions each 60% finished = 0 points!
- Team leader should **direct who is doing what** for the finish
  - Be prepared to make adjustments on the fly
  - Very common to double or triple up on questions now
  - Be **decisive** - better to commit to the wrong call than to only half-commit to the “correct” call
  - But also be realistic on what is feasible
- Play **extra aggressive** here

On Aggression

- Two schools of thought:
  - **Deduction:** Solving step-by-step with almost-sure logical decisions
  - **Intuition:** Solving with assumptions or patterns and checking as you go
  - Essentially: low- vs. high- risk playstyles
- I lean towards intuition, mainly because it's faster
  - Try to suppress the fear of being wrong:
  - Make **fast, bold guesses** (e.g., words & phrases vs. letters)
  - Constantly **sanity check** your work as you go
  - Trust your intuition that is built up from **practice**

Communication

- Practice keeping your communication **frequent, clear, and positive**
    - You can always discuss what went wrong *after* the event is over
- Communication is in 3 main categories:
    - **Facilitation:** Test-wide strategy, starting or finishing a question, which questions are on which page, etc.
        - Make sure we're all on the same page on what is done and what needs to be done by whom.
    - **Help:** Asking for word patterns, Morse Code, Cipher mechanics, etc.
        - For whenever you're stuck, and/or moving on when you're too stuck
    - **Morale:** Keeping your team spirits high
        - Build each other up, and avoid tilt

BUILDING FUNDAMENTALS & PRACTICING

What is Codebusters *actually* about?

- **My answer**: Not really cryptography. Instead, maybe:
    - Linguistics
    - Pattern recognition
    - Puzzle-solving
    - Strategy development
- As a result, Codebusters is much more about **practice** than about **content**.
    - Focus on the **skills you're building** instead of the content you're learning

How to Practice

- **Consistency:**
    - Practice a little bit regularly (e.g., 30 minutes each day)
    - Long sessions can be useful for **endurance** and **team strategy**
    - Make time for strategy development!
- **Scrimmages:**
    - Practice both with and against your teammates / other teams
        - If your school has two or more teams, scrim against each other!
    - Write tests for one another with varied cipher compositions
        - Look up a quote generator if you don't want to write your own
- **Online Resources** (cryptograms.org)
    - Great for learning a lot early on, warming up, staying sharp
    - Diminishing returns

How to Learn Ciphers

- Read up on **how the cipher works** (say, on dcode.fr)
- Play around with an **encoder/decoder**, especially the one on toebes.com
- Work through at least 1 example in full detail
  - You may want to do one already knowing the answer, focusing on how to actually arrive at said answer
- Do a few practice questions until you're comfortable with the cipher mechanically
  - (Have a partner write some for you!)
- In general, spend **more time doing**, and less time reading

Resources

https://cryptograms.puzzlebaron.com/

dcode.fr/tools-list

https://toebes.com/codebusters/

My User Page! (User:Klebb)

THANKS!