

## CODEBUSTERS B

1. **DESCRIPTION:** Teams will cryptanalyze (decode) encrypted messages using cryptanalysis techniques and show skill with advanced ciphers by encrypting or decrypting a message.  
**TEAMS OF UP TO:** 3                      **APPROXIMATE TIME:** 50 MINUTES
2. **EVENT PARAMETERS:**
  - a. Teams must bring writing utensils and may bring up to three (3) non-graphing, nonprogrammable, non-scientific 4-function or 5-function calculators dedicated to computation.
  - b. No resource materials, except those provided by the event supervisor, may be used.
3. **THE COMPETITION:**
  - a. This event consists of participants using cryptanalysis techniques and advanced ciphers to encrypt or decrypt messages on a written exam.
  - b. All teams will begin the event simultaneously when the event supervisor indicates.
  - 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 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 on the exam at Invitational and Regional competitions are as follows:**
    - i. The Pigpen Cipher (also called the tic-tac-toe cipher or the masonic cipher)
    - ii. Atbash Cipher (in English, not Hebrew)
    - iii. The Caesar Cipher, also called a shift cipher.
    - iv. Mono-alphabetic substitution (can use K1, K2, or random alphabets as defined by the ACA)
      - (1) Aristocrats with a hint - messages with spaces included, and with a hint
      - (2) Aristocrats - messages with spaces included, but without a hint
      - (3) Aristocrats - messages with spaces and hints, but including spelling/grammar errors
      - (4) Patristocrats with a hint - messages with spaces removed, and with a hint
    - v. Affine cipher - encryption only (i.e. producing the ciphertext for a given plaintext & key)
    - vi. The Vigenère Cipher - encryption/decryption only, not cryptanalysis (i.e. producing the ciphertext for a given plaintext & key, or the plaintext given a ciphertext & key)
    - vii. The Baconian cipher, and its variants
  - 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. The running-key cipher
    - iii. Cryptanalysis of the Vigenere cipher with a “crib” (a known-plaintext attack)
    - iv. Xenocrypt - at the state and national levels, exactly one cryptogram will be in Spanish.
  - g. For aristocrats, patristocrats, and xenocrypts: no letter can ever encrypt to itself.
  - h. The first question of the exam will be timed.
    - i. The first question will be the decoding of a mono-alphabetic substitution cryptogram, it will be either an Aristocrat with or without a hint.
    - ii. A team member should signal when his or her team has broken the cryptogram.
    - iii. Before the exam begins, the event supervisor will announce the nature of the signal that must be used (e.g., shouting “bingo”, or quietly raising hand).
    - iv. The time in seconds, **to the accuracy of the device used**, to solve the cryptogram will be recorded by the event supervisor or designee.
    - v. If a team gets the timed question wrong, they may attempt to answer the question repeatedly without penalty. The timing bonus will be calculated from the start of the event until the question is successfully answered by the team, or until 10 minutes has elapsed. After 10 minutes, the timed question can still be answered but the timing bonus is zero.
4. **SCORING:**
  - a. The high score wins. Final score = Exam score + timing bonus.
  - b. Based on difficulty, each question will be worth a clearly indicated number of points.
    - i. **The general point distribution by question type is:**
      - (1) An “easy question” = 100-150 pts
      - (2) A “medium question” = 200-300 pts
      - (3) A “hard question” = 350-500 pts
      - (4) A “very hard question” = 550-700 pts
    - ii. For questions such as cryptograms, with answers composed of letters, **the final points will be determined based on the number of errors found**
      - (1) **Two or fewer errors will result in full credit**
      - (2) Each additional error results in a penalty of 100 points

(3) The penalty will not exceed the value of the question. For example, a 400-point question with 5 errors is worth 100 points whereas the same 400-point question with 7 errors **would be** worth 0 points, not -100 points.

iii. For questions whose answers are numbers, the answer is either correct, or incorrect.

iv. The scores for each question will be added to determine the exam score.

c. **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  $4 \times (600 - \text{number of seconds})$  For example, 6 minutes =  $4(600-360) = 960$  points.

d. Tie Breakers: 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 attempted.

e. Scoring example: Team A earns 3600 points on the exam and solves the timed question in 435 seconds.

Exam Score = **3600 pts.**

Timing Bonus  $4(600-435)$  = 660 pts.

Final Score **4260 pts.**

**Recommended Resources:** The Science Olympiad Store ([store.soinc.org](http://store.soinc.org)) carries the Problem Solving/Technology CD; other resources are on the event page at [soinc.org](http://soinc.org).