© 2015-16 Wisconsin Science Olympiad Inc. Division B/C

CODE BUSTERS

1. **DESCRIPTION:** Contestants will decode encrypted messages using cryptanalysis techniques, or show skill with advanced ciphers by encoding a message.

   TEAMS OF UP TO: 3 **APPROXIMATE TIME:** 50 MINUTES

2. **EVENT PARAMETERS:** No resource materials may be used during the competition. Each team may use one or more non-graphing, non-programmable 4-function calculators (or 5-function calculators), but not a scientific calculator. Competitors must bring writing instruments.

3. **THE COMPETITION:**
   a) Teams will be issued a sequence of increasingly difficult codes to break in an exam booklet. (See "Hierarchy of Difficulty" below).
   b) The solutions will either be written on index cards (provided by the event supervisor) or on the exam booklet itself, as clearly indicated by the event supervisor.
   c) The point awards for breaking each code will be written on the exam sheet.
   d) Teams may choose to break any code in any order and by any team member at the same time, working together or separately.
   e) The first code of the exam is timed. Once this cryptogram is broken, a team member should signal that. The time to solve the code will be recorded by the event supervisor. The nature of the signal should be announced by the event supervisor before the exam begins (e.g. shouting "bingo", raising hand). The timing is important as it serves as a tie-breaker as well as a source of bonus points.
   f) If a team gets the timed question wrong, they may attempt to answer the question again and again. The timing bonus will be calculated from the start of the event, through to the time when the question is successfully answered. There is no bonus nor penalty for intermediate incorrect attempted answers.
   g) Teams that do not answer the timed question correctly at all are automatically transferred to "Tier II."
   h) All teams will begin and end the event simultaneously, when the event supervisor indicates. Teams should not open the exam booklet nor write anything prior to the "start" signal, nor should they write anything after the "stop" signal.
   i) For added security, the event supervisor has the option to enclose the timed cryptogram in a sealed envelope, to be simultaneously opened by all teams at the "start" signal of the event.
   j) For very long codes, it is acceptable for the problem in the exam booklet to clearly state an abbreviated option for solution: for example, teams providing 2-3 complete sentences or teams providing the key.
   k) Teams may "undo" the staple holding the exam booklet together, to facilitate distributing the workload. The event supervisor should have one or more staplers on hand to reassemble exam booklets (which can be done after the "stop" signal, because this does not require writing on the exam booklet.) The exam booklet should be held together by only a single staple to facilitate this dismemberment.
   l) Solutions are correct if they are an exact match with the true solution, or if they differ by 1 or 2 letters. Those that differ by 3 or more letters are incorrect solutions.

   Hierarchy of difficulty:
   1. Mono-alphabetic substitution
      a. Messages with spaces included, and with a hint (akin to cryptograms published in "newspapers" during the 20th century)
      b. Messages with spaces included, but without a hint (akin to NSA and diplomatic message traffic)
      c. Messages with spaces included, but including spelling errors (akin to FBI and organized crime message traffic)
      d. Messages with spaces removed, and with a hint (akin to NSA and espionage message traffic)

e. Messages with spaces removed, but without a hint [warning: extremely hard]
f. For an added challenge, one cryptogram can be in Spanish. At the state-level competition, there will be exactly one cryptogram in Spanish.
g. (Examples of these can be found on the website listed below.)

2. The affine cipher and modular arithmetic.
3. The Hill Cipher (matrix based), but only 2x2 or 3x3 matrices would be used.
4. The Vigenère Cipher
5. Sir Arthur Conan Doyle's cipher from "The Adventure of the Dancing Men."

Note: Because cryptanalysis with an affine cipher, the Hill Cipher or a Vigenère Cipher is rather difficult, a problem might ask the team to *encrypt* with one of those ciphers. (In other words, to encode plaintext English writing into encoded ciphertext.)

4. **SCORING:** Points will be assigned by the event supervisor for each problem based on the difficulty of the solution (e.g. 1000, 500, 1500, 3500, 2000, etc…). Those scores will be added for each correctly solved question to determine the baseline team score. The time to decode the first question (in seconds) will be recorded. The timing bonus is equal to one million divided by the number of seconds spent on question one. (e.g. if exactly 10 minutes are spent, the bonus is 1666.666… points).

5. **TIE BREAKER:** The timing bonus is a sufficient tie-breaker among those teams who answer the timed question successfully, particularly because the time is recorded to the second. However, some teams might not get the timed question correct. Such teams will be automatically transferred to "Tier II." In this case, the percentage of letters (or "spots") correctly identified in the timed question will serve as a tie breaker among the teams that did not get the timed question correct.

Resources:
Examples for practice can be found in the following books, sorted from easiest to hardest.

- "*The Cryptoclub: Using Mathematics to Make and Break Secret Codes*" by Janet Beissinger and Vera Pless. Published by A&K Peters in 2006. (There is also a free pdf workbook available as a companion text.)

- Simon Singh's "*The Codebook: How to Make It, Break It, Hack It, Crack It*," published in 2002. Not to be confused with his other book "*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum* Cryptography," published in 2000.

- *"Elementary Cryptanalysis: A Mathematical Approach, 2nd edition*" by Abraham Sinkov and Todd Feil. Published by the Mathematical Association of America in 2009.

- Chapter 2 of "*Cryptography with Coding Theory 2nd Edition*," by Wade Trappe and Larry Washington. Published by Pearson/Prentice Hall in 2005.

- The following website has some online tools for practice of mono-alphabetic substitution:
  www.gregorybard.com
  (Just click on "Cryptograms.")
  A major upgrade to the site is expected to occur in November of 2014.

- The website www.cryptograms.org is run by "Puzzle Barron," and also has excellent mono-alphabetic substitution ciphers.

- The short story "The Adventure of the Dancing Men" is to be found in *The Return of Sherlock Holmes* by Sir Arthur Conan Doyle, published in 1903. It is only slightly more difficult than a mono-alphabetic substitution.