Code Busters 2018

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

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

2. **EVENT PARAMETERS:**
   a. Teams must bring writing utensils.
   b. Each team may bring up to three (3) non-graphing, non-programmable, non-scientific 4- or 5- function calculators dedicated to computation.

3. **THE COMPETITION:**
   a. Teams will be issued a sequence of increasingly difficult codes to break in an exam booklet. Examples of code types assessed in order of their difficulty are as follows:
      i. 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 at www.gregorybard.com or www.cryptograms.org
      ii. The affine cipher and modular arithmetic
      iii. The Hill Cipher (matrix based)
         a. Only 2x2 or 3x3 matrices will be used
      iv. The Vigenère Cipher
      v. 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 plain text English writing into encoded cipher text.
   b. The event supervisor will announce whether solutions will be written on provided index cards provided or within the exam booklet itself.
   c. The point awards for breaking each code will be written in the exam booklet.
   d. 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.
   e. 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.
   f. Teams may choose to have their participants work together, independently, or in a combination of both to break any code in any order at any time.
   g. The first code of the exam will be timed. A participant should signal when his or her team has broken the cryptogram. The event supervisor will announce at the start of the event the nature of the signal (e.g., shouting "bingo", raising hand) that should be used. The time to solve the cryptogram will be recorded by the event supervisor and will serve as a tie-breaker as well as a source of bonus points.
   h. 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 by the team. There is no bonus nor penalty for intermediate, incorrect, or attempted answers.
   i. Teams who do not answer the timed question correctly are automatically placed into Tier II.
   j. For added security, the event supervisor may enclose the timed cryptogram in a sealed envelope to be simultaneously opened by all teams at the "start" signal of the event.
   k. For very long codes, it is acceptable for the problem in the exam booklet to clearly state an abbreviated option for solution (e.g., providing 2-3 complete sentences or providing the key).

4. **SCORING:**
   a. High score wins.
   b. Points will be assigned by the event supervisor for each problem based on the difficulty of the solution.
   c. Those scores will be added for each correctly solved question to determine the baseline team score.
   d. 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).
   e. Ties will be broken as follows:
      i For teams that answered the timed question successfully, the timing bonus will be used as a tie breaker.
      ii For teams that do not answer the timed question successfully, they will be placed in Tier II behind the teams that answered the question successfully and the percentage of letters, or "spots", correctly identified in the timed question will serve as a tie breaker.

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

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.