CODEBUSTERS C

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

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

   A TEAM OF UP TO: 3 **APPROXIMATE TIME:** 50 minutes

2. **EVENT PARAMETERS:**
   a. Teams must bring only writing utensils.
   b. No resource materials or other tools, except those provided by the Event Supervisor, may be used.
   c. The exam packet must be printed single-sided to facilitate separation and writing answers by individual team members. Using a separate answer sheet is not recommended.
   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 as needed for the questions on the exam. The resource sheets may be printed double-sided.

3. **THE COMPETITION:**
   a. This event consists of participants decrypting ciphertext 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 Kl, K2, K3, or random alphabets as defined by the American Cryptogram Association (ACA) with or without a hint
         (1) Aristocrats - ciphertext with spaces included.
         (2) Patristocrats - ciphertext with spaces removed and letters grouped in sets of 5 encoded using a K1 or K2 alphabet.
      ii. For aristocrats encoded using a Kl, 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 (maximum of 2) - messages in Spanish encoded with a K1 or K2 English keyword alphabet.
      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 5x5 Checkerboard Cipher – Decrypting ciphertext given the Polybius key. **For the Checkerboard cipher, all letters used for the row and column keywords must be present in the ciphertext.**
      xi. **Cryptanalysis of the Homophonic Cipher - Decrypting ciphertext given a "crib" which indicates at least 2 letters of the keyword. For the Homophonic cipher, the keyword must have four unique letters.**
   f. The code types that may be used on the exam at State and National competitions are as follows:
      i. All Regional code types.
      ii. Xenocrypt - at the State and National levels, at least two cryptograms and no more than three will be in Spanish, encoded using a K1 or K2 English keyword alphabet.
      iii. Cryptanalysis of the Porta Cipher with a "crib" of at least 3 plaintext characters.
      iv. Cryptanalysis of the Nihilist Cipher with a "crib" that is no shorter than double than the length of the keyword used.
      v. 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.

vi. Cryptanalysis of the 5x5 Checkerboard Cipher encoded with two 5-letter keywords and a Polybius key given a "crib" of at least 5 characters.
vii. **The Homophonic Cipher - Decrypting ciphertext given at least 2 letters of the keyword.**

g. For Aristocrats, Patristocrats, and Xenocrypts, no letter can ever decrypt to itself.
h. The first question of the exam will be timed.
   i. The first question will be the decoding of an Aristocrat as defined by 3.e.i.(1).
   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 "time", or quietly raising hand).
   iv. The time in seconds, to the precision 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 with two or fewer errors, or until 10 minutes have elapsed. After 10 minutes, the timed question can still be answered but the timing bonus is zero.
i. Up to three questions which are not Aristocrats, Patristocrats, or Xenocrypts will be marked on the exam as special bonus questions. **At least one special bonus question will use the Homophonic Cipher (3.e.xi. or 3.f.vii.).**
j. For Cryptanalysis problems providing a "crib" (3.e.iii., 3.e.v., 3.e.xi., 3.f.iii., 3.f.iv., 3.f.vi.) with the exception of the Complete Columnar Cipher (3.e.viii., 3.f.v.), the placement of the "crib" on the ciphertext will be clearly identified.

4. **SCORING:**

a. The high score wins.
b. Final Score = Exam Score + Timing Bonus + Special Bonus.
c. The scores for each question will be added together to determine the Exam Score.
d. Unless otherwise specified, the final points will be determined based on the number of errors found in the decoded plaintext as is appropriate to the question.
   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.
e. For answers involving the keyword or key phrase for a K1, K2 or K3 alphabet (3.e.ii.) the final points will be determined based on the number of errors found in the keyword or key phrase. For the Cryptarithm (3.e.vi.), the final points will be determined based on the number of errors found in the decoded word or 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.
f. 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.
g. 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.
h. 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

i. 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.