



1. **DESCRIPTION:** Teams 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 writing utensils and may bring up to three (3) stand-alone non-graphing, non-programmable, non-scientific 4-function or 5-function calculators.
- 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. **In remote tournament formats, teams may provide their own scratch paper, which should be blank paper free of any additional markings, symbols, or notes.**

3. **THE COMPETITION:**

- a. **This event consists of participants using cryptanalysis techniques and advanced ciphers to decrypt and encrypt 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 codes types that may be used at Division B & C Regional Tournaments are as follows:**
 - i. the Caesar Cipher, also called a shift cipher
 - ii. **Monoalphabetic substitution using K1, K2, or random alphabets as defined by the American Cryptogram Association (ACA)**
 - (1) Aristocrats with a hint - messages with spaces included
 - (2) Aristocrats - messages with spaces included, but without a hint
 - (3) Aristocrats - messages with spaces and hints, but including spelling/grammar errors
 - (4) Aristocrats - messages with spaces and including spelling/grammar errors but no hints
 - (5) Patristocrats with a hint - messages with spaces removed, and with a hint
 - (6) Patristocrats - messages with spaces removed, but without a hint
 - iii. the Affine Cipher - encrypting plaintext or decrypting ciphertext given the a and b values
 - iv. the Vigenère Cipher - Encrypting plaintext or decrypting ciphertext given a key
 - v. 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)
 - vi. Xenocrypt - no more than one cryptogram can be in Spanish
 - vii. the Pollux and Morbit Ciphers - decrypting Morse code ciphertext encoded as digits and spaces given the mapping of at least 6 of the digits
- f. **Division B Only - The following code type may also be used at Regional Tournaments:**
 - i. **The Atbash Cipher (In English, not Hebrew)**
- g. **Division C Only - The following code types may also be used at Regional Tournaments:**
 - i. **For Mono-alphabetic substitution ciphers, a K3 alphabet as defined by the ACA may also be used**
 - 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 Hill Cipher - Encrypting plaintext or decrypting ciphertext given a 2x2 decryption matrix**
 - iv. **The Porta Cipher - Encrypting plaintext or decrypting ciphertext given a key**
 - v. **The Rail Fence cipher - Decrypting transposed text given the number of rails and an unknown offset**
- h. 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 **one cryptogram** will be in Spanish
 - iii. Cryptanalysis of the Vigenère cipher with a “crib” of at least 5 plaintext characters
 - iv. Cryptanalysis of the Affine Cipher with a “crib” of at least 2 plaintext characters
 - v. Cryptanalysis of The Pollux and Morbit Ciphers with a “crib” of at least 4 plaintext characters
 - vi. **Cryptanalysis of the Porta Cipher with a “crib” of at least 4 plaintext characters**



- vii. **Cryptanalysis of The Rail Fence Cipher with a “crib” of at least 5 plaintext characters and a range for the rails**
 - i. **Division C Only - The following code types may also be used at State and National Tournaments.**
 - i. **The Hill Cipher - Encrypting plaintext or decrypting ciphertext with a 2x2 encryption matrix or 3x3 decryption matrix provided**
 - ii. **Xenocrypt - at the State and National levels, at least two cryptograms will be in Spanish**
 - iii. **Cryptanalysis of the Rail Fence Cipher with a “crib” or at least 5 plaintext characters and a range for the rails and offset**
 - j. For aristocrats, patristocrats, and xenocrypts, no letter can ever decrypt to itself.
 - k. No more than 2 cipher questions will be an encryption on the exam.
 - l. The exam packet will include a resource sheet with the Morse Code Table, English/Spanish letter frequencies, Vigenère table, Baconian mapping and modulus inverse tables as needed for the questions on the exam.
 - m. 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.ii.(1) or 3.e.ii.(2)
 - 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 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 has elapsed. After 10 minutes, the timed question can still be answered but the timing bonus is zero
 - n. **Up to three questions which are not aristocrats, patristocrats or xenocrypts will be marked on the exam as special bonus questions.**
4. **SCORING:**
- a. The high score wins. Final Score = Exam Score + Timing Bonus + **Special Bonus.**
 - b. Based on the difficulty of the question, correct answers for each question will earn 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 in the decoded plaintext
 - (1) Two or fewer errors will be scored as correct and 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 earns 100 points whereas the same 400-point question with 7 errors would earn 0 points, not -100 points.
 - iii. **For answers involving the keyword or key phrase for a K1, K2 or K3 alphabet, the final points will be determined based on the number of errors found in the keyword or key phrase**
 - (1) **Zero errors are required for full credit.**
 - (2) **Each 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 3 errors earns 100 points whereas the same 400-point question with 5 errors would earn 0 points, not -100 points.**
 - 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 = $4 \times (600 - 360) = 960$ points.



- d. 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.
- e. 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 4(600-435)	=	660 points
+ Special Bonus (One=150)	=	150 points
Final Score		4410 points

- f. 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 for this event; other resources are on the Event Pages at soinc.org