Codebusters Science Olympiad

By Tarang, Ivan, and Mehar.

Starting Off

Codebusters is a Science Olympiad event consisting of only a testing portion. This event focused on encrypting and decrypting as many messages as possible in 50 minutes. A select few cryptography techniques are used and range in difficulty. The 2018-2019 list of ciphers is shown in the rule manual below:

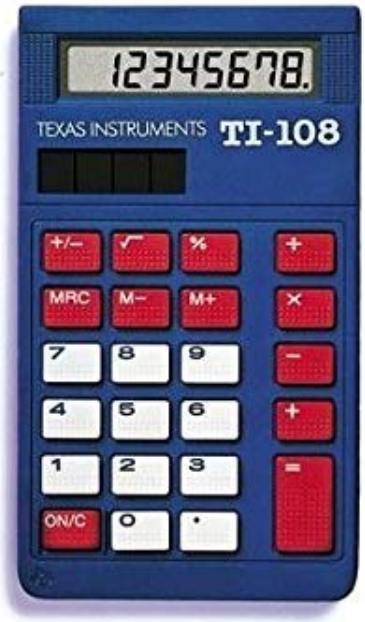
e. **The code types that may be used on the exam at Invitational and Regional competitions are as follows**:
   i. Atbash Cipher (in English, not Hebrew)
   ii. The Caesar Cipher, also called a shift cipher.
   iii. Mono-alphabetic substitution (can use K1, K2, or random alphabets as defined by the **American Cryptogram Association (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) 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
   iv. Affine cipher - encryption only (i.e. producing the ciphertext for a given plaintext & key)
   v. 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)
   vi. The Baconian cipher, and its variants
   vii. Xenocrypt - no more than one cryptogram can be in Spanish
   viii. Mathematical Cryptanalysis of the Hill Cipher - either producing a decryption matrix given a 2x2 encryption matrix or computing a decryption matrix given 4 plaintext-ciphertext letter pairs.
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 Vigenère cipher with a "crib" (a known-plaintext attack)
   iv. The RSA Cipher
   v. The Hill Cipher - encrypting with a 2x2 or 3x3 encryption matrix provided, or decrypting with a 2x2 or 3x3 decryption matrix provided.
   vi. Xenocrypt - at the state and national levels, at least one cryptogram will be in Spanish.
   vii. Mathematical Cryptanalysis of the Affine Cipher
g. For aristocrats, patristocrats, and xenocrypts: no letter can ever encrypt to itself.

As for the rules, there is not much to say. Question types and point values vary at each invitational, and the entirety of the event is testing based.

Event Rules / Materials

As for materials, only a few are allowed and they are:

- A 4-Function Calculator. **Scientific Calculators are not allowed!**



- Any pencils or pens necessary (Pencil preferably)

And the main rule that you have to keep track of is the timed question. At the beginning of every test, there will be a timed aristocrat, for which you only have 10 minutes to solve. The quicker you can solve this question, the more points you are rewarded for it. The points obtained are calculated as shown:

$$Number\ of\ points\ =\ 4 \cdot (600 - seconds\ taken\ to\ solve\ cipher)$$

Getting this timed question down is key, and results in a ludicrous amount of free points.

Ciphers and how to tackle them

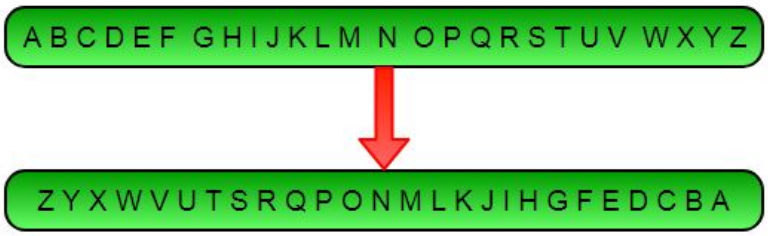
Here we will list the ciphers in order of increasing difficulty:

1. **Atbash**
2. **Caesar**
3. **Vigenere**
4. **Affine**
5. **Baconian**
6. **Aristocrat**
7. **Hill Cipher**
8. **Patristocrat**
9. **Xenocrypt**

10. **RSA Cipher**

Simple Monoalphabetic Substitutions

Atbash- Easiest one by far. Just uses a reversed alphabet to decode a cipher, easy points.



The key

Caesar Cipher: Relatively easy. Shifts the alphabet by a certain amount. Requires repeated guess and check.

Difficult Alphabetic Substitutions

Aristocrat Cipher: Medium difficulty. Requires a lot of practice and a bit of luck. Used for the time question which holds the most points. Should be solved in minutes. Multiple variations such as having grammar mistakes. Make sure at least one person has done sufficient practice with this cipher.

Patristocrat Cipher: Decently difficult. Same as aristocrat but with no spaces. Requires good aristocrat skills and some luck. Worth a lot of points.

Xenocrypt Cipher: Difficulty depends on your Spanish skills. Same as Patristocrat but in Spanish. Requires good Patristocrat skills and decent Spanish vocabulary. Worth a lot of points.

Mathematical Ciphers

Affine Cipher: Medium difficulty. Requires some good math skills. Does not take too much time and worth medium points.

Hill Cipher: Difficulty depends on your math skills. Uses matrices to solve. Requires good math skills and is time consuming but worth a lot of points.

RSA Cipher: Hardest cipher by far. Requires really good math skills. Difficult to understand, but worth a lot of points. Must learn to stand a chance in states.

Miscellaneous Ciphers

Vigenere Cipher: Time consuming. Requires using a grid-like chart. Easy points but takes time and concentration.

Baconian Cipher: Ranges in difficulty. Uses binary numbers as letters. Basic baconian ciphers are easy, but difficulty comes from when they use symbols other than 1 and 0 or A and B. Guess and check is used to figure out what symbols corresponds with A and B.

Strategies

Splitting the Work:

Everyone should know how to solve 7+ of the 10 ciphers. However, each member should focus on 2-3 types of ciphers. Here is how we split the work:

- Atbash and Caesar are easy and do not require a dedicated person
- 2 people focused on learning aristocrat for the timed question
- Person 1 did Vigenere, Affine, Aristocrat and Patristocrat
- Person 2 did Aristocrat, Patristocrat, Xenocrypt
- Person 3 did Hill and Baconian

Frequency:

Be sure to memorize the letter and word frequencies (link in the resources section). This will allow you to make better guesses, especially for aristocrat and patristocrat ciphers. However, be wary that harder questions will likely NOT follow the frequencies.

K1 and K2 Alphabets:

These are variations in the alphabet used for the cipher. They can appear in basically any of the ciphers and if you understand them, they can actually be an advantage and help you solve ciphers quicker.

Timed Question:

Solving the timed question is mandatory for even a chance at placing. Although the aristocrat cipher is intimidating and difficult at first, practicing consistently will allow you to greatly improve. For reference, our first practice aristocrat was solved in 1+ hour, but by our final one in states, we solved it at around 3 minutes. See the resources section for tools to help you practice.

Resources

Cryptogram Apps: Use to practice aristocrat cipher. Download on your phone and practice in your free time.

https://www.sciencenc.com/resources/high-school/codebusters/: Practice tests

https://toebes.com/codebusters/: Tool used to create codebuster tests

http://www.cryptogram.org/wp-content/themes/wp-opulus-child/images/SampleCryptogram.pdf: Practice test

https://www3.nd.edu/~busiforc/handouts/cryptography/cryptography%20hints.html: Letter and word frequency data

Good Luck, and have fun with this event :)