CYBERSECURITY

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

1. **DESCRIPTION:** Competitors will be assessed on their knowledge of cybersecurity through hands-on tasks as well as theoretical questions focused in the areas of cryptography and web architecture.

   A TEAM OF UP TO: 2 **APPROXIMATE TIME:** 50 minutes

2. **EVENT PARAMETERS:**
   a. Each team may bring up to two 8.5" x 11" sheets of paper, which may be in a sheet protector sealed by tape or laminated that may contain information on both sides in any form and from any source without any annotations or labels affixed.
   b. Each team may also bring tools, supplies, and writing utensils. Teams may use the internet during the competition only to access an online IDE, reference the official documentation for their programming language of choice, and visit any other website required for the event by the Event Supervisor. Teams may also provide their own mouse.
   c. Supervisors will provide a computer capable of accessing the internet. Tournament Directors are encouraged to provide computer specifications to the teams at least one month in advance.

3. **THE COMPETITION:**

   Both Part I and Part II of the event will be provided to the participants at the beginning of the event. Participants may work on both parts simultaneously during the entire event.

   Part I: Written Test (65%)
   a. Participants will complete a written test consisting of the topics Cryptography and Web Architecture, as well as general cybersecurity principles and concepts.
      i. Cryptography
         (1) The cryptographic protocols are limited to:
            (a) Hashing algorithms
            (b) The XOR operation
            (c) Classical Cryptography: Substitution Ciphers, Transposition Ciphers
            (d) Modern Cryptography: RSA, Diffie Hellman Key Exchange, Block Ciphers, Stream Ciphers, Elliptic Curve Cryptography
         (2) Identifying vulnerabilities in implementations of cryptosystems
         (3) Common applications of the topics in the Cryptography section (3.a.i)
         (4) Post-quantum cryptography
      ii. Web Architecture
         (1) History of the internet
         (2) Web page construction: HTML, CSS, JavaScript, APIs
         (3) HTTP: requests, responses, headers, query parameters, status codes, verbs
         (4) URL syntax and structure
         (5) Storage, session management, and cookies
         (6) Types of networks and connections including TCP/IP, WiFi, and SOHO and how information travels through these networks
         (7) Common web exploitation techniques
      iii. Principles of Cybersecurity
         (1) Authentication and security best practices
         (2) Cybersecurity ethics
         (3) Online safety

   Part II: Hands-On Tasks (35%)
   a. The programming portion of the hands-on tasks will consist of multiple programming problems. Competitors must use an online IDE to write code, and it is suggested that HackerRank is used to host the problems. Each problem must be solved using any of the following supported languages: C, C++, C++11, Java, Python 2, or Python 3. Only the standard library for these languages may be used.
      i. Competitors will write code to implement various common algorithms to a variety of problems and test cases. Topics may include, but are not limited to:
         (1) String manipulation
         (2) Boolean expressions
         (3) Control structures
         (4) Implementation of math operators and integer evaluation, such as primality tests and prime sieves

(5) Recursion

ii. Test cases for programming challenges will be provided to teams to test their program. The problem statement may include time and memory constraints, and these constraints may vary by language; any given test case will fail if these constraints are not met.

iii. Each problem will be checked against the answer and the code submitted. Point values may vary between questions based on difficulty and points given may be determined by the number of test cases passed.

iv. Teams will be required to submit their code to the event supervisor at the end of the event.

4. **SCORING:**

a. High score wins.

b. The written portion will account for 65% and the hands-on portion will account for 35% of the total number of available points.

c. In the written portion, points will be awarded based on accuracy of the responses. In the hands-on portion, points will be awarded based on accuracy of outputs.

d. Ties will be broken by 1) Part II score, 2) Selected questions from the written test.

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

Topic Rotation

Year	Topic 1	Topic 2
Year 1	Web Architecture	Cryptography
Year 2	Cryptography	Data Forensics
Year 3	Data Forensics	Web Architecture