CYBERSECURITY
Division C
Southern California Trial Event

1. **DESCRIPTION:** Competitors must compete in hands-on tasks and answer questions about cybersecurity.

   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 will not have access to the internet during the event. Teams may also provide their own mouse.
   c. Supervisors will provide a computer capable of running repl.it. Tournament Directors are encouraged to provide computer specifications to the teams at least one month in advance. For Satellite and Mini Tournaments, participants will provide their own computer. The computer may only be used in the hands-on portion of the exam.

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 can work on both parts simultaneously during the entire event.

   Part I: Written Test (50%)

   a Participants will complete a written test consisting of these two topics: **Cryptography and Web Architecture**.
      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
            e. **Division C Only:** Elliptic Curve Cryptography
         (2) Identifying and exploiting vulnerabilities in implementations of common cryptosystems in a chosen programming language
         (3) Encrypting and decrypting messages with the use of cryptosystems using a chosen programming language
         (4) Auditing custom cryptosystems written in Python
         (5) Common applications and uses of the topics in the Cryptography section (3.a.i).
         (6) **Division C Only:** Post-quantum cryptography
      ii Web Architecture
         (1) History of the internet
         (2) Web page anatomy: HTML, CSS, JavaScript, APIs, frontend vs. backend.
         (3) HTTP: requests, responses, headers, query parameters, status codes, verbs
         (4) URL syntax and structure
         (5) Storage, session management, and cookies
         (6) **Division C:** Types of networks and connections including TCP/IP, WiFi, and SOHO and how information travels through these networks
         (7) **Division C:** Authentication and security best practices

Part II: Hands-On Tasks (50%)

b The hands-on portion will consist of two parts: Programming and Cryptography. Each portion will be worth 25% of the test.

i The **Programming** portion of the hands-on tasks will consist of multiple programming problems. Competitors must use an online IDE such as repl.it. Each problem must be solved using any of the following supported languages: C, C++, C++11, Java, Python 2, Python 3. Only the standard library for these languages may be used unless otherwise stated. Language-specific details may vary; other languages may or may not be supported. Competitors are recommended to include important documentation on their notesheet.

(1) Programming, consisting of applications and implementations of various common algorithms to various types of problems and test cases. Competitors will be asked to demonstrate these skills by writing code. Topics may include, but are not limited to:

a. String manipulation
b. Boolean expressions
c. Control structures
d. Implementation of math operators and integer evaluation, such as primality tests and prime sieves.
e. Recursion

(2) Test cases for programming challenges will be provided to teams to test their program. The problem statement may include time and memory constraints; any given test case may fail if these constraints are exceeded.

(3) 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 test cases passed.

(4) Teams will be required to submit their code to the tournament supervisor at the end of the event.

ii The **Cryptography** portion of the exam will consist of multiple cryptographic challenges with topics from the written portion (3.a.i). Each challenge must be solved using any version of the Python 3 programming language with the aid of any or all of any version of the following libraries: pycrypto, pycryptodome, sagemath, numpy, sympy, and any module in the Python Standard Library. Any of the aforementioned libraries may be banned for specific questions at the Event Supervisor's discretion.

4. **SCORING:**
   a. High score wins.
   b. The written portion will account for 50% of each team's score, and the hands-on portion will account for 50% of the team's score.
   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 based off of the hands-on portion of the event. Ties will be broken by 1) hands-on tasks score, 2) selected questions from the written test.

Recommended Resources:

1. **Competitive Programming past problems, such as USACO (http://www.usaco.org/).**
2. **CTF "Capture the flag" computer security competitions, such as picoCTF (https://picoctf.com/) for applications of Binary Exploitation, Cryptography, Reverse Engineering, and Web Exploitation.**
3. **Various CyberPatriot (https://www.uscyberpatriot.org/) resources.**