Columbia University
Science Olympiad

CUSO 2024– Test #1
Cybersecurity

Proctors: Geoffrey Wu, Connor Li

2024/01/27

Name(s): _____
School Name/School Code: _____

This exam contains 6 pages (including this cover page) and 4 sections. Total of points is 100. Good luck and Happy reading work!

Distribution of Marks

Section	Points	Score
1	40	
2	25	
3	20	
4	15	

Section 1

ECC

[1] Write the general form of an elliptic curve.

[2] Consider the following elliptic curve $y^2 \equiv x^3 + 2x + 3 \pmod 5$.

- Find the number of points on the curve. List those points.
- Find the order of the curve.
- Find a generator of the curve.

[3] Using the EC $y^2 \equiv x^3 - x + 4 \pmod 5$, find the following EC addition $(2, 0) + (4, 3)$.

Diffie-Hellman Key Exchange

[1] True or False. The Diffie Hellman key exchange is a building block for the SSH and SSL/TLS protocols.

[2] Determine and fill in the missing step in the below key exchange.

1. Alice and Bob agree on two large prime numbers, p and g, and a public key exchange algorithm.
2. Alice chooses a secret integer, a, and computes $A = g^a \mod p$. She sends A to Bob.
3. Bob chooses a secret integer, b, and computes $B = g^b \mod p$. He sends B to Alice.
4. Alice computes $s =$ _____. Bob computes $s =$ _____.
5. Alice and Bob now both have the shared secret key s, which they can use to establish a secure communication channel.

[3] Name one vulnerability of this type of key exchange.

Hashing

[1] What is hash collision?

[2] Explain the difference between Hash Function and Encryption.

[3] True or False. A hash function is a one-way function.

[4] Write a piece of code to create a simple Hash Function converting each character in the input key into its corresponding ASCII value.

XOR

[1] Fill in the following XOR table.

x	y	x $\oplus$ y
0	0	
0	1	
1	0	
1	1	

[2] Swap two values x and y in-place, i.e. without using any helper variables and using the XOR function.

Classical Ciphers

[1] True or False. monoalphabetic ciphers are stronger than polyalphabetic ciphers because frequency analysis is tougher on the former.

[2] Is the Caesar Cipher is an example of a monoalphabetic or a polyalphabetic cipher?

[3] Use Caesar Cipher to encrypt the following plaintext with key $k = 10$.

$$\text{Columbia Science Olympiad} \implies ?$$

Modern Ciphers

[1] True or False. Rivest-Shamir-Adleman, or RSA, is an algorithm used for symmetric key cryptography.

[2] In password protection, what is the name of a random string of data used to modify a password hash called?

[3] One of the triumphs of modern cryptanalysis was the breaking of what cipher used by German U-Boats during World War II?

[4] CHELSEA and ARSENAL are both 700 kms away from you. SPURS 1800 kms away from you. WOLVES 200 kms away from you. How far are from MANCITY?

[5] What is the units digit of $6789^5 \mod 5$?

Section 2

Web Architecture

[1] What is an API and what does it do?

[2] Name the 4 most common HTTP methods (verbs).

[3] What is the difference between HTTP and HTTPS?

[4] What are 200 OK response codes in HTTP?

[5] Name the 3 parts of a HTTP response.

[6] What is the role of Public Key Infrastructure (PKI) in HTTPS?

Cybersecurity Principles

[1] A password, a physical token and iris scan are common methods of what?

[2] Alice, using her private key encryption, created an email to Bob which provides a digital signature authenticating that it was Alice sending an email to Bob. Alice realizes she cannot take back her email and claim it was never sent by her. What is this an example of?

[3] Describe what a DDoS attack is.

[4] What is Kerckhoff's principle?

[5] Name the 5 main consequences of a cyber attack for an organization.

[6] Explain CIA triad.

[7] What are some of the common cyberattacks?

[8] Name all the layers of the OSI model.

Section 3

Data Structures Problem. Link to the problem is also provided here.

Section 4

Recursion-Focused Problem. Link to the problem is also provided here.