[CUSO] Cybersecurity 2024 - Answer Key

Connor Li, csl2192

November 2023

1 Section 1

1.1 ECC

1.1.1 Problem 1

$$y^2 = x^3 + ax + b$$

1.1.2 Problem 2

- Part (a). First, identify that there are 7 points. Then, list any 3 of the following 7 points.

$$(1,1)\ \ (1,4)\ \ (2,0)\ \ (3,1)\ \ (3,4)\ \ (4,0)\ \ \infty$$

- Part (b). The curve is order 7.
- Part (c). The generator for the curve is any of the points in Part (a) except ∞.

1.1.3 Problem 3

$(3,-3)$ mod 5 or any equivalent points

1.2 Diffie-Hellman Key Exchange

1.2.1 Problem 1

True

1.2.2 Problem 2

- Step (3). $B = g^b \bmod p$.
- Step (4). Alice computes $s = B^a \mod p$ and Bob computes $s = A^b \mod p$.

1.2.3 Problem 3

Award points if answer matches any one of the following.

- Exponent attacks: if secret exponents are not chosen randomly
- Small subgroup attacks: if the prime number p has a small subgroup
- Man-in-the-middle attacks: if they can intercept messages and impersonate Alice or Bob

1.3 Hashing

1.3.1 Problem 1

A hash collision is a random match in hash values that occurs when a hashing algorithm produces the same hash value for two distinct pieces of data.

1.3.2 Problem 2

A hash function is one-way, encryption is two way.

1.3.3 Problem 3

True

1.3.4 Problem 4

Java uses typecast to do this.

int ascii = (int) character

Python uses the ord() function.

1.4 XOR

1.4.1 Problem 1

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

1.4.2 Problem 2

Use the following steps.

- $x = x \oplus y$
- $y = x \oplus y$
- $x = x \oplus y$

1.5 Classical Ciphers

1.5.1 Problem 1

False

1.5.2 Problem 2

Monoalphabetic Cipher

1.5.3 Problem 3

Sebkcryq Isyudsu Ebocfyqt or Myvewlsk Cmsoxmo Yviwzskn

1.6 Modern Ciphers

1.6.1 Problem 1

False

1.6.2 Problem 2

Salt

1.6.3 Problem 3

Enigma

1.6.4 Problem 4

2100

1.6.5 Problem 5

4

2 Section 2

2.1 Web Architecture

2.1.1 Problem 1

APIs are connections (interfaces) between two or more endpoints, such as programs or systems, that allow for the endpoints to communicate and share functionality.

2.1.2 Problem 2

The four most common HTTP methods are GET, PUT, DELETE, and POST.

2.1.3 Problem 3

HTTPS uses encryption (TLS or SSL), HTTP does not.

2.1.4 Problem 4

Successes! The request has succeeded.

2.1.5 Problem 5

The three parts of an HTTP response are the status line, header, body.

2.1.6 Problem 6

The role of PKI in HTTPS is to provide a framework for the encryption and decryption processes in HTTPs.

2.2 Cybersecurity Principles

2.2.1 Problem 1

These are common methods of authentication.

2.2.2 Problem 2

This is an example of non-repudiation.

2.2.3 Problem 3

A DDoS attack is an attack that overwhelms a server to disrupt the flow of normal traffic.

2.2.4 Problem 4

Kerckhoff's principle says that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

2.2.5 Problem 5

Consequences include financial, legal, reputational, asset, and time.

2.2.6 Problem 6

IA stands for Confidentiality, Integrity, and Availability. CIA is a model that is designed to guide policies for Information Security. It is one of the most popular models used by organizations.

2.2.7 Problem 7

Common cyberattacks include Malware, Phishing, Password Attacks, DDoS, Man in the Middle, Drive-By, Downloads, Malvertising, Rogue Software.

2.2.8 Problem 8

Layers include Application, Presentation, Session, Transport, Network, Datalink, Physical.