Full Name: _____ Gannon Identification Number: _____

CYENG 351: Embedded Secure Networking
Spring 2023, First Examination
Gannon University (GU)
February 22, 2023

Please do not turn the page until you are informed.

Rules:
- The exam is closed-book, closed-note, closed shared calculator, and closed electronics.
- Please stop promptly at **2:10 PM**.
- There are **30 points** total, distributed **evenly** among **3** questions.

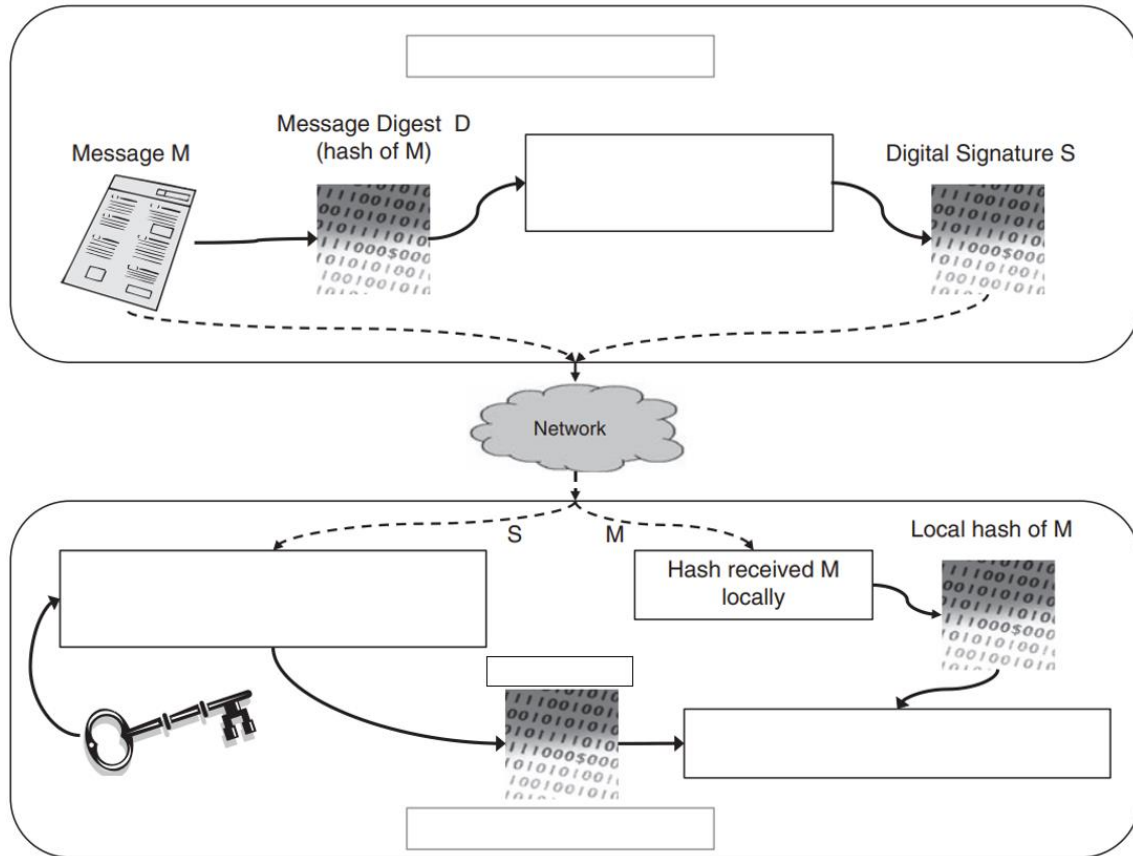| Question	Maximum	Earned
1	10	
2	10	
3	10	

Advice:
- Read questions carefully. Understand a question before you start writing your answer.
- Write down thoughts and intermediate steps so you can get partial credit. Clearly circle your final answer.
- The questions are not necessarily in order of difficulty. **Skip around.** Make sure you get to all the problems.

Wishing you the best of luck,
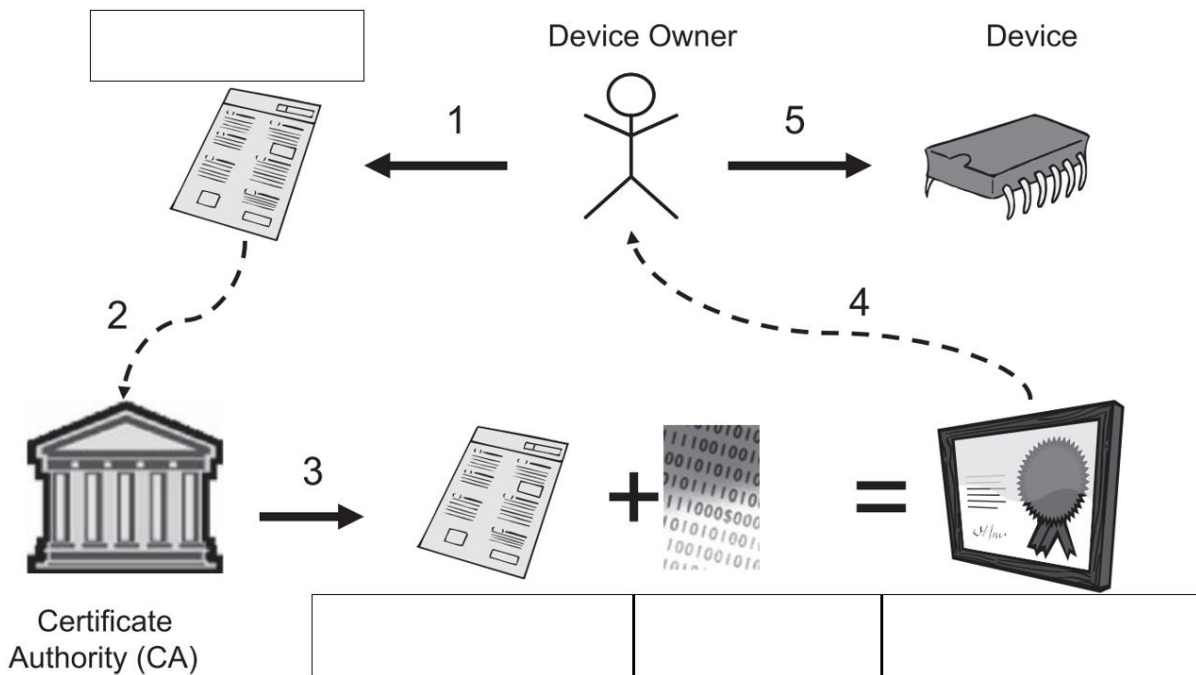**Dr. Shayan (Sean) Taheri**

Full Name: _____ Gannon Identification Number: _____

Question 1. (10 points) Complete **the empty boxes** in the following computational flows, determine <u>their usages</u>, and provide their **step-by-step/algorithmic descriptions**.

Message M

Message Digest D
(hash of M)

Digital Signature S

Network

S   M

Local hash of M

Hash received M
locally

Question 1. (Cont.)

Device Owner

Device

1

5

2

3

Certificate
Authority (CA)

+

=

Full Name: _____ Gannon Identification Number: _____

Question 2. (10 points) Mention <u>the positive and the negative aspects</u> of **public-key authentication**. Explain how **a security protocol** (<u>with provision of its name</u>) can <u>resolve</u> (some of) the mentioned issues.
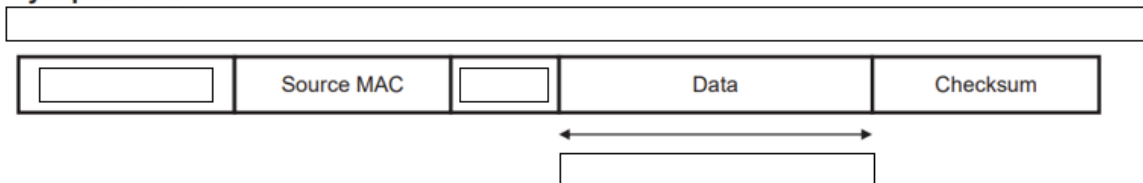
Full Name: _____ Gannon Identification Number: _____

Question 3. (10 points) Complete the following items.

A. Specify the name and the usage of the following table based on the terminology of Embedded Networks and complete its empty cells.
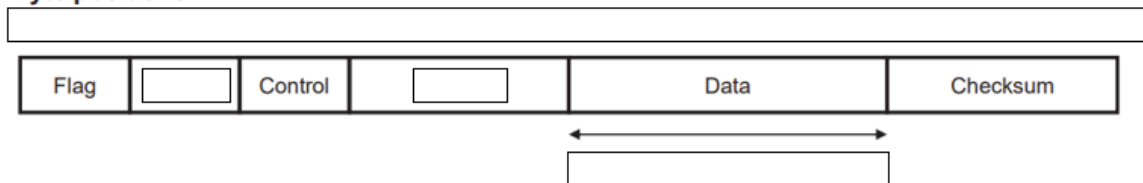
Layer	Examples
	TCP, UDP, SSL/TLS
Physical	
Application	
	IP, ARP, IPSEC
Link	

B. Fill out the empty boxes and specify the names and the usages of the following arrangements.

Byte positions

	Source MAC		Data	Checksum

Byte positions

Flag		Control		Data	Checksum

5

C. Fill out the empty cells and explain the communications and the computations in the following embedded network.

Device A
MAC: 11:AA:22:BB
IP: 1.2.3.4

ARP Response

Device B
MAC: FF:99:EE:88
IP: 9.8.7.6

ARP broadcast

ARP Cache
Before broadcast

MAC Address	IP Address

Ethernet

ARP Cache
Before broadcast

MAC Address	IP Address

After response

MAC Address	IP Address

After broadcast

MAC Address	IP Address