Guide Questions (Answer in your worksheet):

- What is the purpose of encrypting data?

  - Encrypting data protects it from unauthorized access. It scrambles the data into an unreadable format, called **Ciphertext**, which can only be decoded by a person or system with the correct key. This process ensures **confidentiality** and **security** of the information whether it's stored on a device or being transmitted across a network.

- How does encryption contribute to **confidentiality**?

  - Encryption directly contributes to confidentiality by making data unreadable to anyone who doesn't have the proper decryption key. This process transforms **plaintext** (readable data) **ciphertext** (scrambled, unreadable data).

    Even if unauthorized parties gain access to the encrypted data, they can't understand it without the key, rendering it useless. This protects sensitive information whether it's stored on a device (**data at rest**) or being transmitted over a network (**data in transit**).

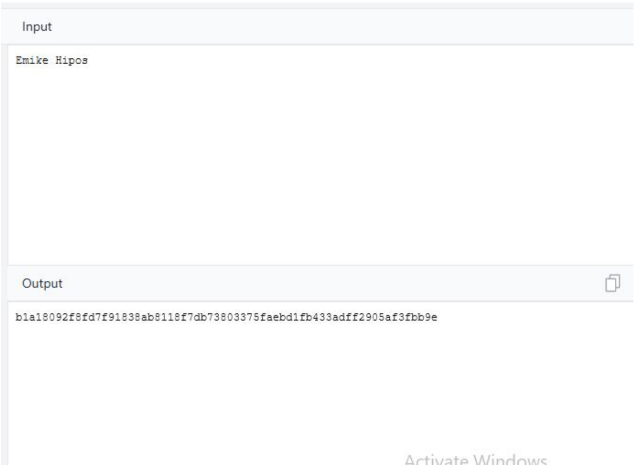
- What would happen if someone intercepted the encrypted data but didn’t have the password?

  - If someone intercepts encrypted data without the password or decryption key, the data will be **unreadable** and **useless** to them. This is because encryption transforms readable data into an unintelligible, scrambled format.

    Even if an attacker successfully intercepts encrypted information, its confidentiality remains intact. Modern encryption algorithms are designed to be practically impossible to reverse without the key, making the data secure as long as the key is not compromised.

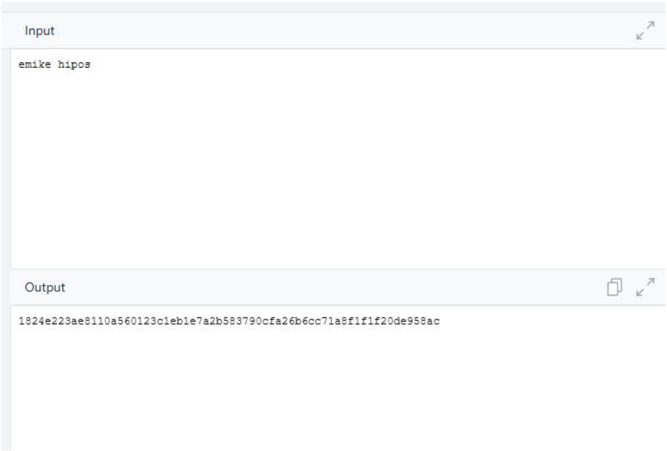
B. Integrity Test – Hash Comparison

Tool: Online SHA-256 Hashing Tool *https://emn178.github.io/online-tools/sha256.html*



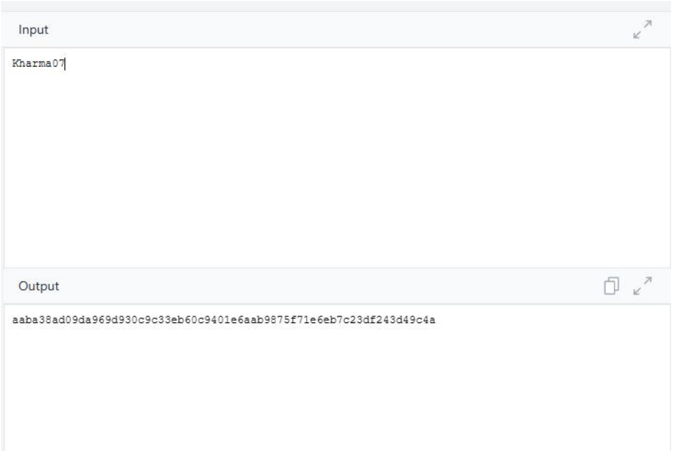
```
Emike Hipos
```

```
b1a18092f8fd7f91838ab8118f7db73803375faebd1fb433adff2905af3fbb9e
```



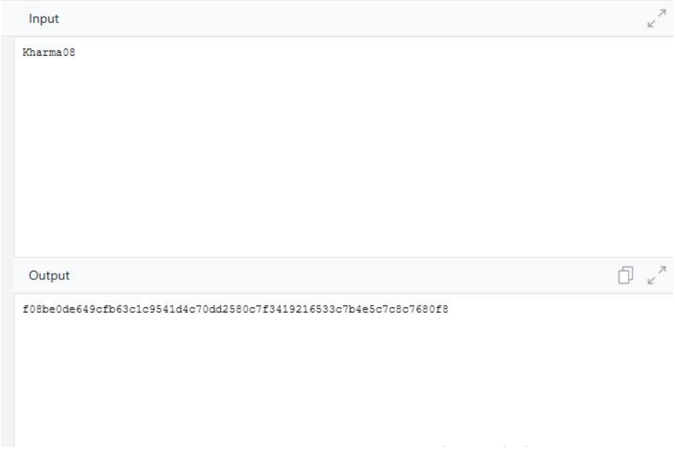
```
emike hipos
```

```
1824e223ae8110a560123c1eb1e7a2b583790cfa26b6cc71a8f1f1f20de958ac
```



```
Kharma07
```

```
aaba38ad09da969d930c9c33eb60c9401e6aab9875f71e6eb7c23df243d49c4a
```



```
Kharma08
```

```
f08be0de649cfb63c1c9541d4c70dd2580c7f3419216533c7b4e5c7c8c7680f8
```

Guide Questions:

- Did the hash values change? Why or why not?
  - No, the hash values did not change. Hashing is a one-way process that converts data into a unique, fixed-size string of characters called a hash value.

    The hash value will only change if the **original data is modified**. Since the data was not altered and only its hash was generated, the hash value will remain the same every time it's calculated on that specific data set.

- How does hashing help protect **integrity**?
  - Hashing protects data **integrity** by providing a unique digital fingerprint, called a **hash value**, for any piece of data. This is a one-way process, so the hash value cannot be used to recreate the original data.

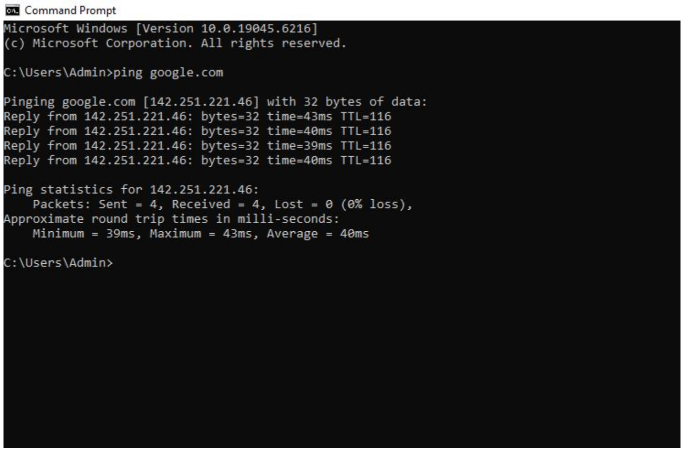
    If even a single character in the data is changed, the new hash value will be completely different. By comparing the hash value of data at two different points in time, you can instantly tell if the data has been altered or corrupted. This guarantees the data's authenticity and reliability.

- How can hashing detect unauthorized modifications?
  - Hashing provides a **unique digital fingerprint** for data. Any modification, no matter how small, will create a completely different hash value.

    By comparing a file's current hash value to its original, stored hash, you can instantly tell if the data has been altered. A mismatch indicates that the data has been corrupted or tampered with. This is known as the **avalanche effect**, which makes it practically impossible to modify data without also changing its hash.

📡 C. Availability Test – Network Ping

Tool: Command Prompt (Windows) or Terminal (Mac/Linux)



```
Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping google.com

Pinging google.com [142.251.221.46] with 32 bytes of data:
Reply from 142.251.221.46: bytes=32 time=43ms TTL=116
Reply from 142.251.221.46: bytes=32 time=40ms TTL=116
Reply from 142.251.221.46: bytes=32 time=39ms TTL=116
Reply from 142.251.221.46: bytes=32 time=40ms TTL=116

Ping statistics for 142.251.221.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 43ms, Average = 40ms

C:\Users\Admin>
```

Guide Questions:

- What does the ping result indicate about network **availability**?

  - A successful ping result confirms that a **network connection exists** between your device and the destination.

It indicates two things about network availability:

1. **Reachability**: The destination host is online and reachable.
2. **Latency**: The time it takes for a packet to travel to the destination and back (measured in milliseconds), which shows the speed and quality of the connection.

   If the ping fails, it indicates that the destination is unreachable, a firewall is blocking the connection, or there's an issue with the network path.

- How could a **DDoS attack** affect this result?

  - A **DDoS (Distributed Denial-of-Service) attack** could affect the ping result by overwhelming the network or server with a flood of traffic, causing severe **latency** (high ping times) or complete **packet loss**.

    - **Ping Flood**: A type of DDoS attack that specifically uses ICMP packets (the same ones used by the `ping` command) to saturate the target's bandwidth. The target becomes so busy responding to the fake requests that it can't handle legitimate ones, including your ping.

    - **Resource Exhaustion**: The attack consumes the target's system resources (like CPU, memory, and bandwidth), making it slow to respond or completely unresponsive.

    - **Result**: Your ping would show a very high latency (e.g., hundreds or thousands of milliseconds) or a "Request timed out" error, indicating that the network is so congested that the packets can't get through.

- Why is availability important in information systems?

  - **Availability** is a core component of information security, ensuring that authorized users can access information and systems when they need them. Without it, the other two pillars of the **CIA triad**—confidentiality and integrity—are meaningless because the data cannot be used.