

 SHA-256 in Action – Cryptographic Hashing  
  
**Objective/Aim:**  
  
 To understand and demonstrate the working of the SHA-256 cryptographic hashing algorithm using a sample input

and observe the properties of hash functions

**Apparatus/Software Used:**

* Laptop
* Word for documentation,
* SHA-256 online
* Internet for research

**Theory/Concept:**

**What is a Hash Algorithm?**

A hash algorithm (or hash function) is a mathematical function that takes any input data (text, file, password, etc.) and produces a fixed-size string of characters, which is usually a hexadecimal number. This output is called a hash value or digest.

**What is SHA-256?**

SHA-256 stands for Secure Hash Algorithm - 256 bit. It’s one of the most commonly used hash functions today and is part of the SHA-2 family, developed by the NSA and published by NIST.

**How it works (in simple terms):**

* Takes any input (a file, a message, a password, etc.)
* Outputs a 256-bit hash (which is a 64-character hexadecimal string)

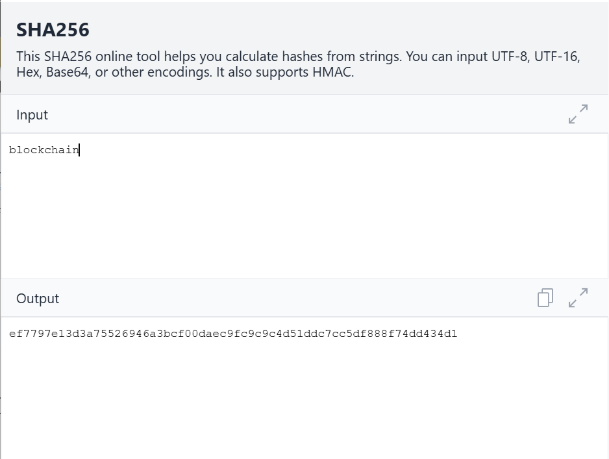
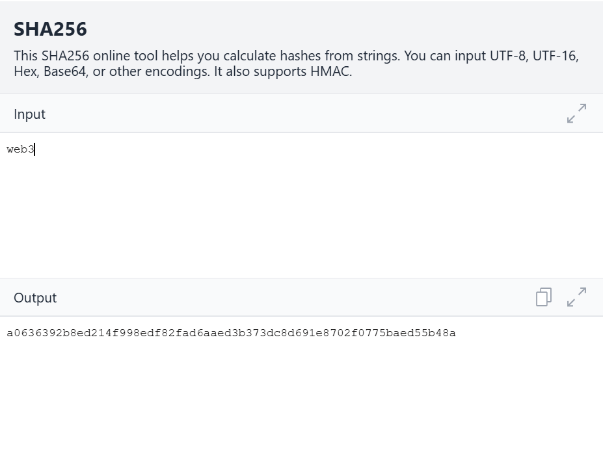


**Procedure:**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Step 1:** Go to online SHA-256 online tool <https://emn178.github.io/online-tools/sha256.html>.

**Step 2:** give a string as an input

**Step 3:** get the hash as an output if a single alphabet changes then the hash also changes   
  
  
  
  
  
  
**Observation:**

* For the same input it will generate the same hash but if single alphabet or

Number or space changes then it changes the hash even if the change a .

* The SHA-256 algorithm provides a one-way hash—it is not possible to retrieve the original input from the hash, ensuring data confidentiality.



