

SHA-256 in Action – Cryptographic Hashing

School: ............................................................................................................. Campus: ....................................................... Academic Year: ...................... Subject Name: ........................................................... Subject Code: ..........................

Semester: ............... Program: ........................................ Branch: ......................... Specialization: .......................... Date: .....................................

(Learning by Doing and Discovery)

**\* Coding Phase: Pseudo Code / Flow Chart / Algorithm**

ALGORITHM:

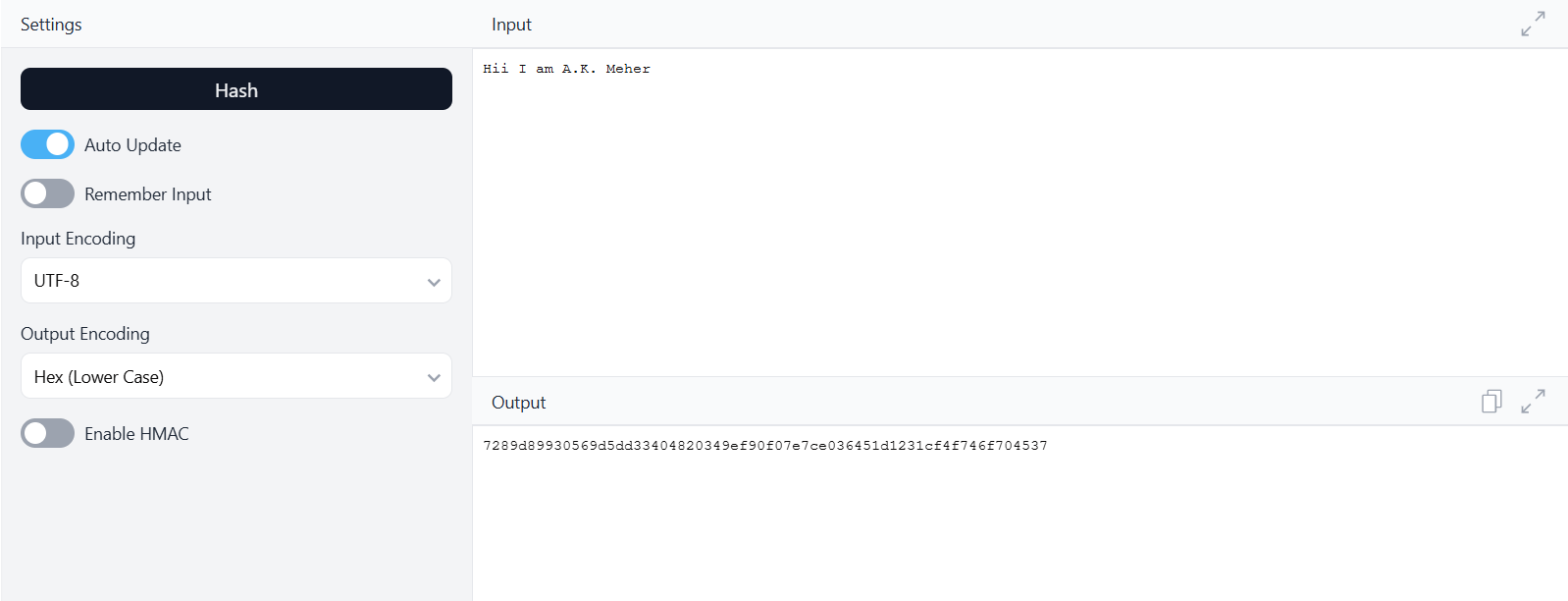
1. Start the program or open an online SHA-256 tool.
2. Enter an input string or message.
3. Apply the SHA-256 algorithm to convert the input into a hash value.
4. Display the resulting hash output.
5. Modify the input message slightly.
6. Apply the hash function again and compare with the previous hash.
7. End

# \* Software Used:

1. Online SHA-256 Tool (<https://emn178.github.io/online-tools/sha256.html>)
2. Brave Browser
3. Internet Connection

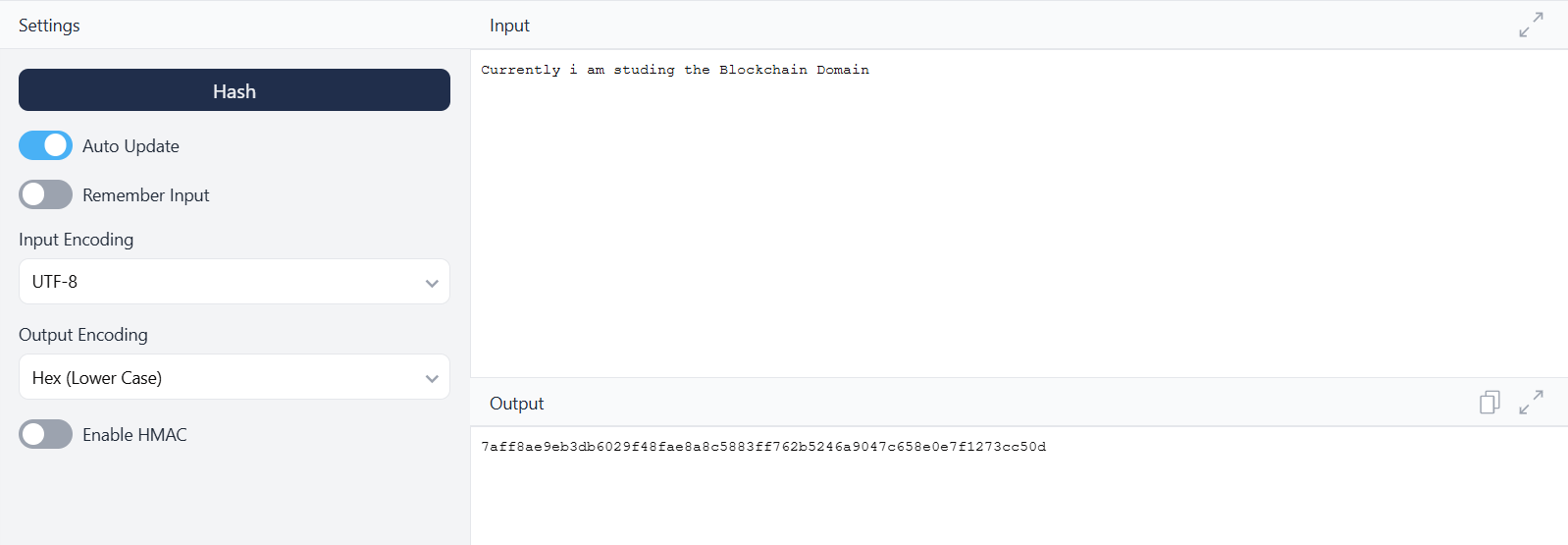
1. Open the online SHA-256 tool in a web browser.
2. Type the desired input message into the input box.
3. The tool will automatically generate a SHA-256 hash value.
4. Note down the hash output.
5. Slightly modify the input message and repeat the process.
6. Compare the newly generated hash with the previous one to observe changes.

**Test Case 1:**

* Input: Hii I am A.K. Meher
* Hash: 7aff8ae9eb3bd20383292facedfff72804651bsjs762jjgh03846c3bod

**Test Case 2:**

* Input: Currently I am studying in Blockchain Domain
* Hash: 099e9929306037759df60ab76d97762aabd28f3a7d3871557631837200fb2d44



## \* Implementation Phase: Final Output (no error)

Applied and Action Learning

The SHA-256 tool successfully generated a **64-character hash** for every input. A slight change in the input produced a completely different hash, proving the avalanche effect.

**Test Cases:**

* Input: Hii I am A.K. Meher  
  Hash: 588dfbad6bcdcbd75a6bd431dd216f688943a15b0ff683a5ff3211a5e6c15d80
* Input: Currently I am studying in Blockchain Domain  
  Hash: 099e9929306037759df60ab76d97762aabd28f3a7d3871557631837200fb2d44
* Input: Blockchain Technology   
  Hash: 9bc65d49c52c925e2ff5ffb947fa86a6d6af2f498fbcf988f3e8abf7e46f64b4

**Result:**

* Output length is always fixed (64 characters).
* Small input changes cause large output differences.
* Same input always gives the same hash.

# Observation:

1. SHA-256 always generates a fixed 64-character hash value irrespective of input size.
2. Even a small change in input results in a completely different hash output.
3. SHA-256 is a one-way function; the original message cannot be retrieved from the hash.
4. It is widely used in blockchains, digital signatures, password storage, and file verification.
5. The algorithm is fast, deterministic, and secure for cryptographic applications.



|  |  |  |  |
| --- | --- | --- | --- |
| **Rubrics** |  |  |  |
| Concept | 10 |  |  |
| Planning and Execution/  Practical Simulation/ Programming | 10 |  |  |
| Result and Interpretation | 10 |  |  |
| Record of Applied and Action Learning | 10 |  |  |
| Viva | 10 |  |  |
| **Total** | **50** |  |  |

***Signature of the Student:***



***Signature of the Faculty:***