School: .....Campus: .....

Academic Year: ..... Subject Name: ..... Subject Code: .....

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

Date: .....

Applied and Action Learning

(Learning by Doing and Discovery)

Name of the Experiment: SHA-256 in Action – Cryptographic Hashing

*Objectives/Aim

The aim of this activity is to gain a clear understanding of the SHA-256 cryptographic hash function, its fundamental principles, and its practical applications. This includes demonstrating how SHA-256 generates a unique fixed-size hash from any given input, exploring key properties such as collision resistance and the avalanche effect, and using software tools to produce and verify hash values. Through this, the objective is to highlight the importance of SHA-256 in ensuring data integrity and security in various digital systems.

*Apparatus/Software Used

- Laptop
- Online SHA-256 hash generators

* Theory/Concept

SHA-256 is a cryptographic hash function that takes an input of any size and produces a fixed 256-bit (32-byte) hash value, which acts like a digital fingerprint of the data. It is designed to be fast, deterministic, and secure, making it nearly impossible to reverse or find two different inputs with the same hash. This makes SHA-256 widely used for data integrity verification, digital signatures, and security applications, where even a tiny change in input drastically changes the output hash.

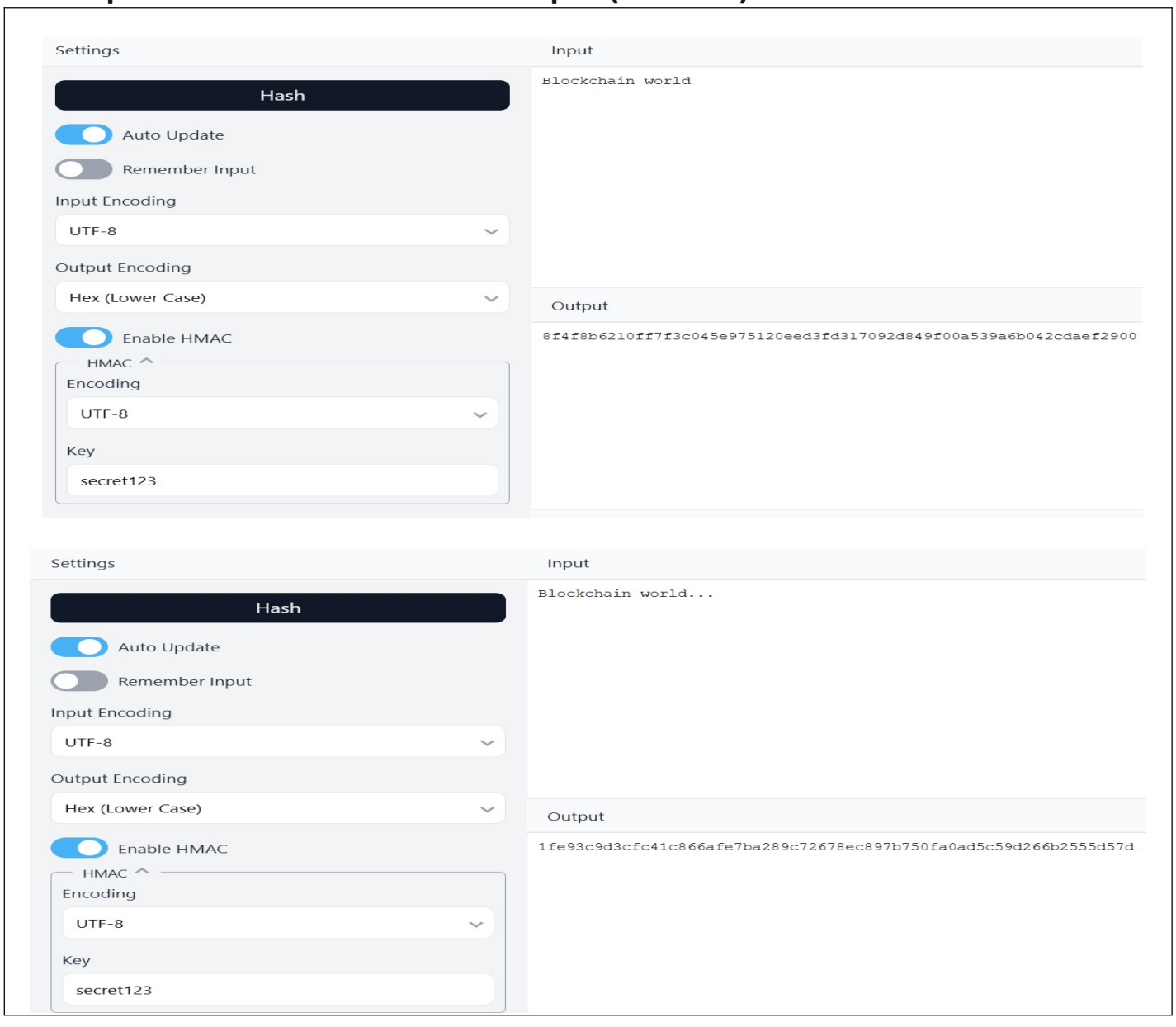
**** As applicable according to the experiment.***

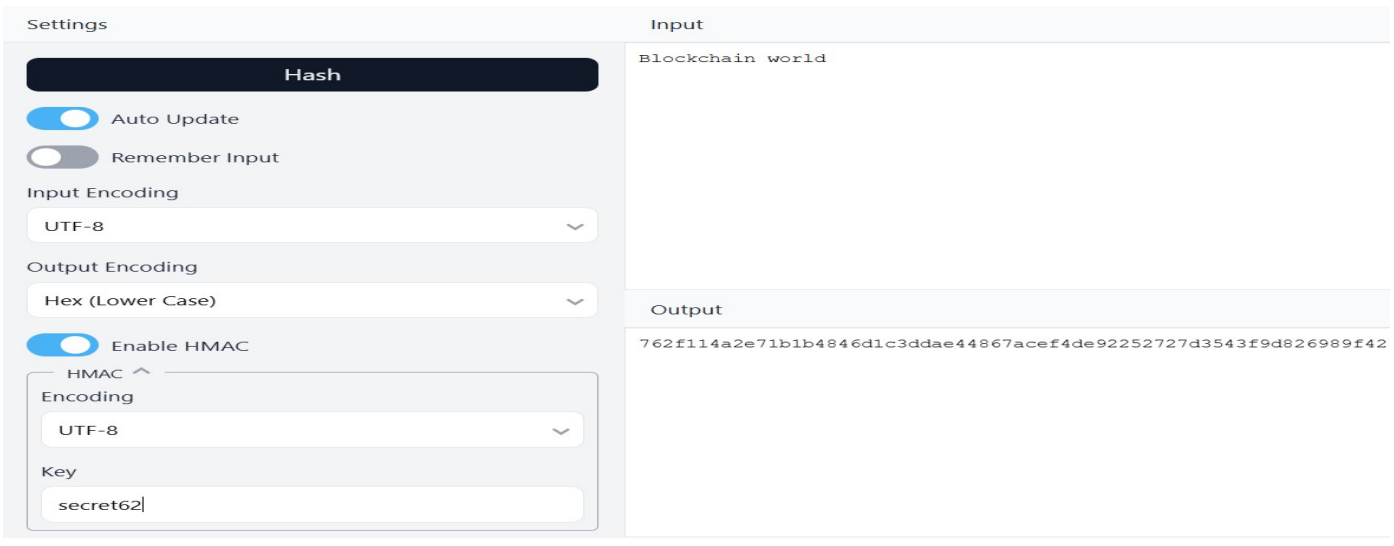
Two sheets per experiment (10-20) to be used.

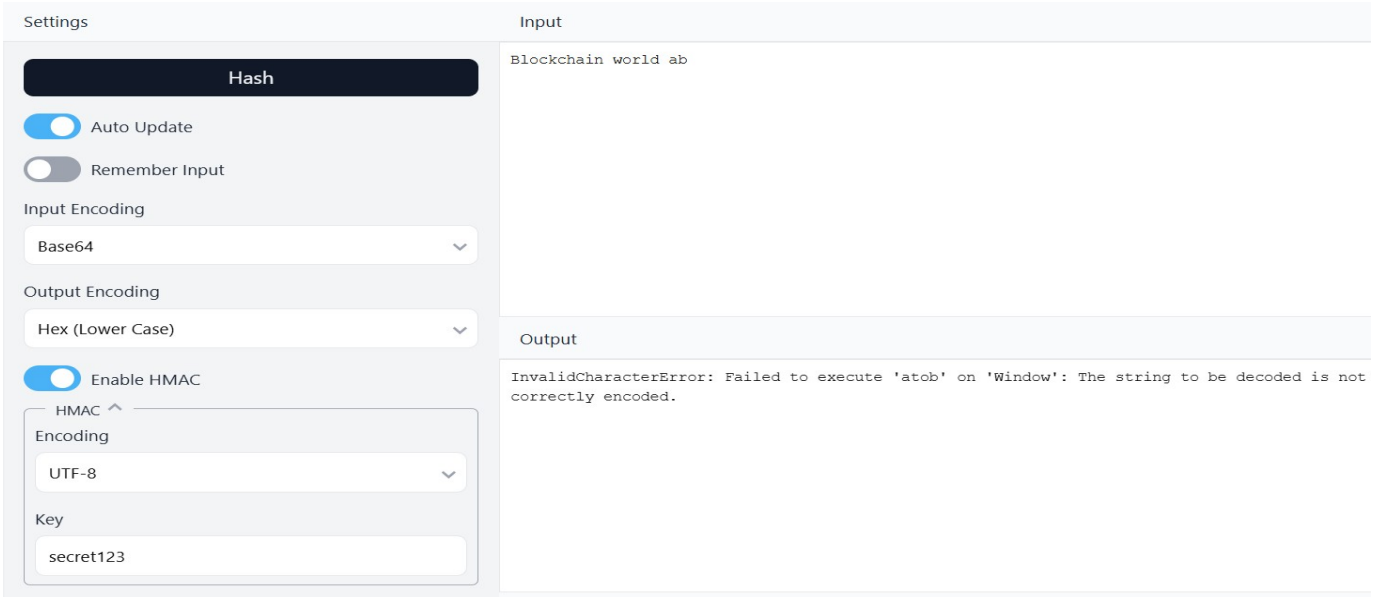
* Procedure

- First we need to navigate to an online SHA-256 hashing tool that offers an easy-to-use interface for entering text and adjusting different options to generate hash values.
- Keep the input encoding and output encoding by default i.e UTF-8 and Hex(Lower Case) respectively.
- Now in the input text area we need to input any text as we desire
  In the configure setting we can enable HMAC and provide a secret key for our text input.
- Now we will see a SHA-256 Hash being generated for our initial text input and note it.
- If we slightly change our input text it will completely change our output hash (i.e showing avalanche effect)
- Even if we keep the text unchanged and change the secret key it will also show the avalanche effect.
- Also if we change the input encoding setting from UTF-8 to Base-64 it will show an invalid character error.

* Implementation Phase: Final Output (no error)







* Observations

It was noted that the SHA-256 hash function reliably generates a 64-character hexadecimal output, no matter how long or short the input is. The output is consistent—meaning the same input always produces the same hash. Most importantly, even a slight change, such as modifying just one character in the input, led to a completely different and unpredictable hash. This clearly illustrates the avalanche effect in action.

**** As applicable according to the experiment.***
Two sheets per experiment (10-20) to be used.

ASSESSMENT

Rubrics	Full Mark	Marks Obtained	Remarks
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 :

Name :

Signature of the Faculty :

Regn. No. :

**** As applicable according to the experiment.***
Two sheets per experiment (10-20) to be used