Centurion University
Shaping Lives Empowering Communities...

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 Experiement :

* Coding Phase: Pseudo Code / Flow Chart / Algorithm

SHA-256 (Secure Hash Algorithm, FIPS 182-2)

- Definition: SHA-256 is a cryptographic, keyless hash function — specifically a Manipulation Detection Code (MDC) — that produces a 256-bit (32-byte) fixed-length digest.
- History: Released in 2001 through a collaboration between NSA and NIST as a stronger alternative to the SHA-1 family, which was becoming vulnerable to brute-force and collision attacks.
- Processing: It processes data in 512-bit blocks (16 × 32-bit words) with 64 computational rounds per block.
- Core Function: Converts any input into a unique, fixed-length 256-bit output, ensuring integrity, authenticity, and tamper resistance.
- Deterministic Output: The same input always produces the same hash output.
- One-Way Function: It's computationally infeasible to reverse the hash to find the original data.
- Avalanche Effect: Even a single-bit change in input drastically changes the entire hash output.
- Collision Resistance: The probability of two different inputs producing the same hash is extremely low.
- Preimage Resistance: Given a hash output, it's practically impossible to find any input that generates it.
- Second Preimage Resistance: It's infeasible to find another input with the same hash as a given message.

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

Coding Phase: Pseudo Code / Flow Chart / Algorithm

Features of SHA-256

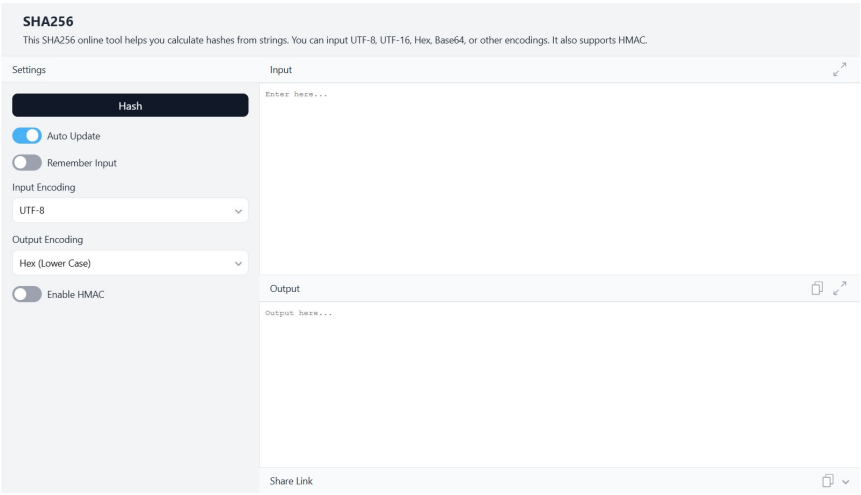
1. Fixed Output Size – Always produces a 256-bit (32-byte) hash regardless of input size.
2. Deterministic – Same input always gives the same output hash.
3. One-Way Function – Impossible to reconstruct the original input from its hash.
4. Avalanche Effect – Small input changes cause a completely different hash.
5. Collision Resistance – Extremely rare for two different inputs to generate the same hash.
6. Preimage Resistance – Hard to find an input that hashes to a specific value.
7. Second Preimage Resistance – Difficult to find a different input with the same hash as another input.
8. High Security – Resistant to current known cryptographic attacks.
9. Efficient Processing – Works well on both hardware and software platforms.
10. Standardized Algorithm – Defined by NIST and widely used globally.

* Softwares used

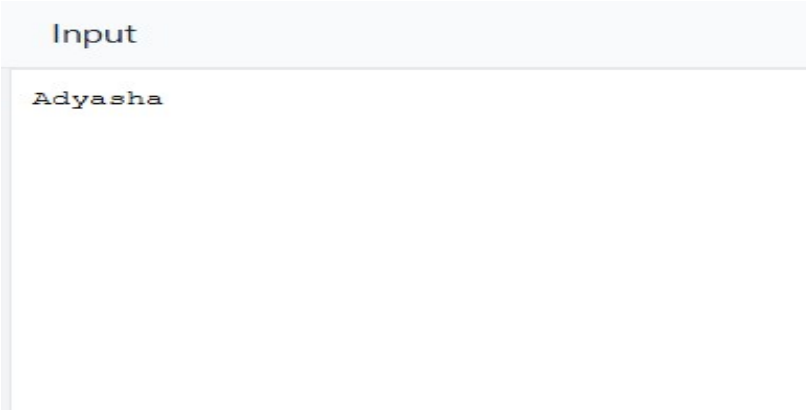
Brave Browser
SHA-256 Online tool

* Testing Phase: Compilation of Code (error detection)

Initial Phase



Inserted the data

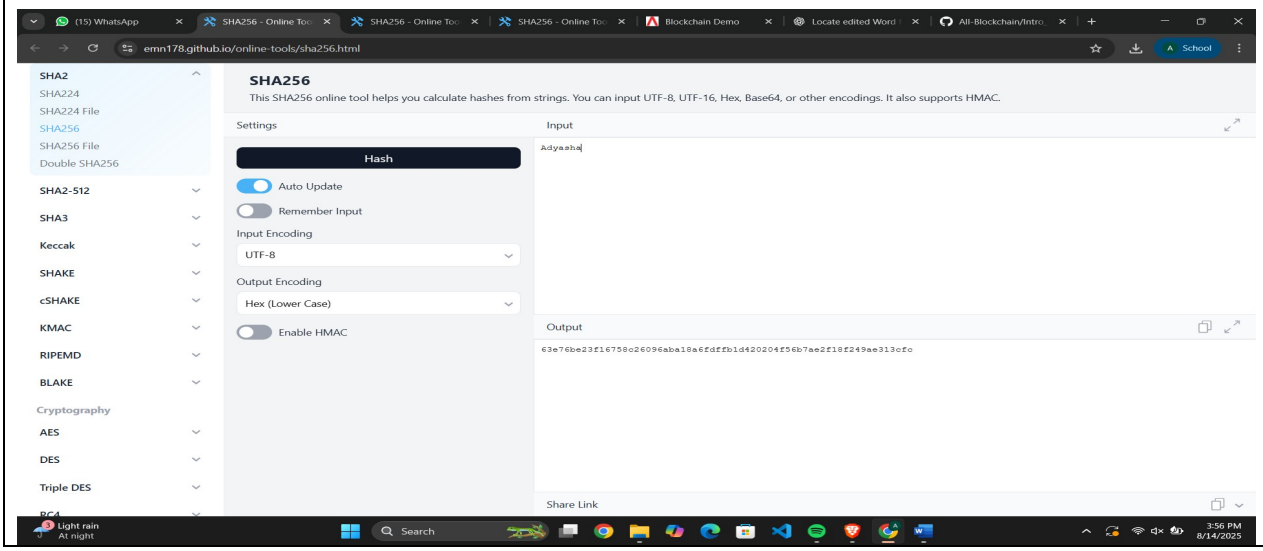


Hash generated automatically

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

* Implementation Phase: Final Output (no error)

Final Output



* Observations

SHA-256 is a secure cryptographic hash function that produces a fixed 256-bit output. It is deterministic, one-way, and highly resistant to collisions, with a strong avalanche effect. These features make it ideal for ensuring data integrity and security in applications like blockchain, digital signatures, and password protection.

ASSESMENT

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 :

Regn. No. :

Signature of the Faculty:

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