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

* Coding Phase: Pseudo Code / Flow Chart / Algorithm

ALGORITHM:

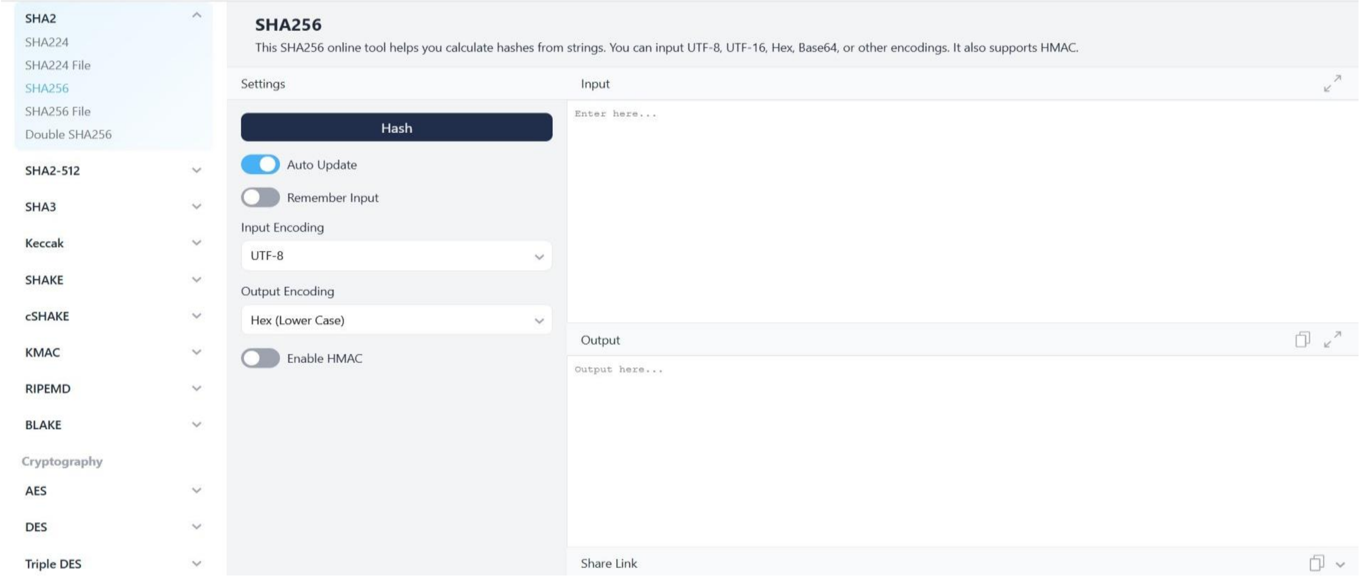
1. Go to the provided SHA-256 online tool link.
2. Enter any input text or message in the given text box.
3. The tool automatically converts the input into a SHA-256 hash.
4. Observe the generated 256-bit (64-character) hexadecimal hash.
5. Modify the input slightly and notice the significant change in the hash.
6. Understand that the hash is irreversible and unique to the input.

* Software used

1. Web Browser – Brave
2. Online Tool – SHA-256 Hash Generator
   URL: https://emn178.github.io/online-tools/sha256.html
3. Operating System – Windows 11

* Implementation Phase: Final Output (no error)

Go to the SHA-256 online tool,Open the link https://emn178.github.io/online-tools/sha256.html in a web browser. This tool helps generate SHA-256 hashes instantly.



SHA256

This SHA256 online tool helps you calculate hashes from strings. You can input UTF-8, UTF-16, Hex, Base64, or other encodings. It also supports HMAC.

Settings

● Auto Update

○ Remember Input

Input Encoding: UTF-8

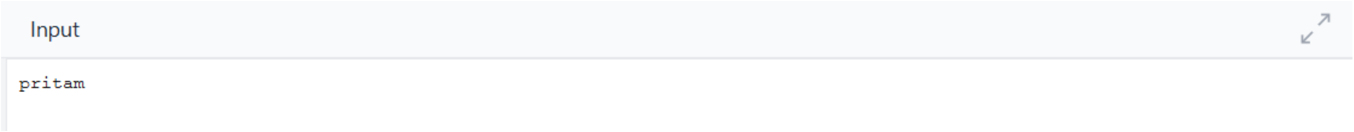
Output Encoding: Hex (Lower Case)

○ Enable HMAC

Input: Enter here...

Output: output here...

Enter the input text ,Type any message, word, or sentence in the input box provided on the webpage.

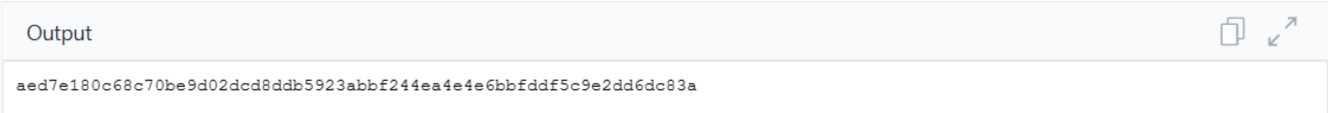


Input

```
pritam
```

Tool processes the input ,As soon as you type, the tool automatically applies the SHA-256 hashing algorithm to your input.

The tool displays the SHA-256 hash — a fixed-length 64-character hexadecimal string — just below the input box.



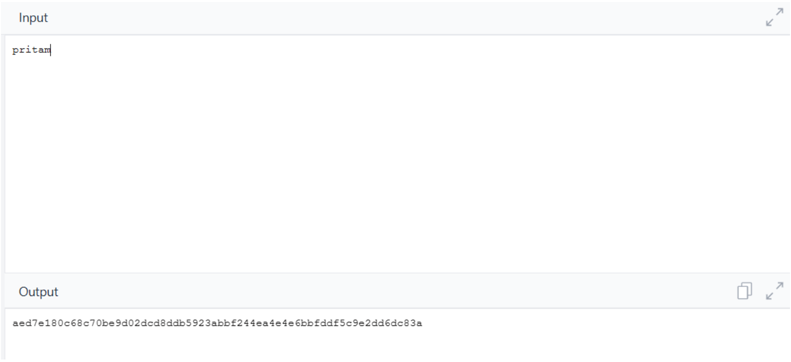
Output

```
aed7e180c68c70be9d02dcd8ddb5923abbf244ea4e4e6bbfddf5c9e2dd6dc83a
```

Even a small change in the input, such as modifying one letter or adding a space, causes the entire SHA-256 hash to change drastically—this is known as the avalanche effect. It occurs because SHA-256 performs multiple rounds of complex mathematical operations, where every bit of the input affects the final output. As a result, even the slightest modification leads to a completely different hash, ensuring high sensitivity and making it impossible to guess patterns or reverse the output. This property is essential in cryptography to maintain data integrity and prevent tampering.

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

* Implementation Phase: Final Output (no error)



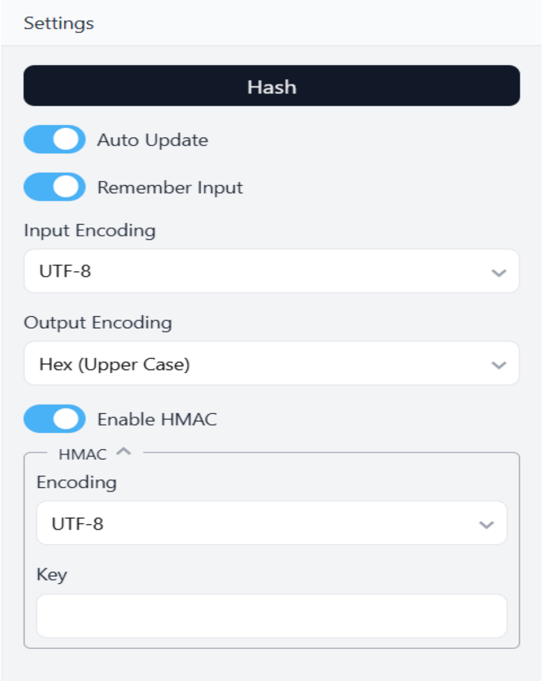
Input

```
pritam
```

Output

```
aed7e180c68c70be9d02dcd8ddb5923abbf244ea4e4e6bbfddf5c9e2dd6dc83a
```

This is the changes you can do for better output



Settings

- Auto Update
- Remember Input

Input Encoding: UTF-8

Output Encoding: Hex (Upper Case)

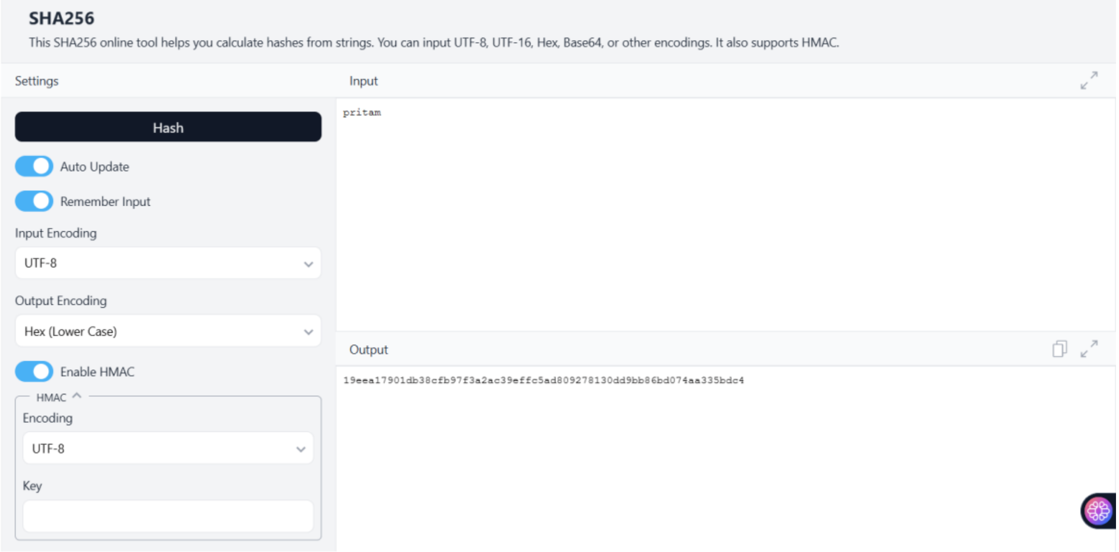
Enable HMAC

HMAC

Encoding: UTF-8

Key:

If we change the output encoding into hex uppercase then we saw a hash in upper case



SHA256

This SHA256 online tool helps you calculate hashes from strings. You can input UTF-8, UTF-16, Hex, Base64, or other encodings. It also supports HMAC.

Settings

- Auto Update
- Remember Input

Input Encoding: UTF-8

Output Encoding: Hex (Lower Case)

Enable HMAC

HMAC

Encoding: UTF-8

Key:

Input

```
pritam
```

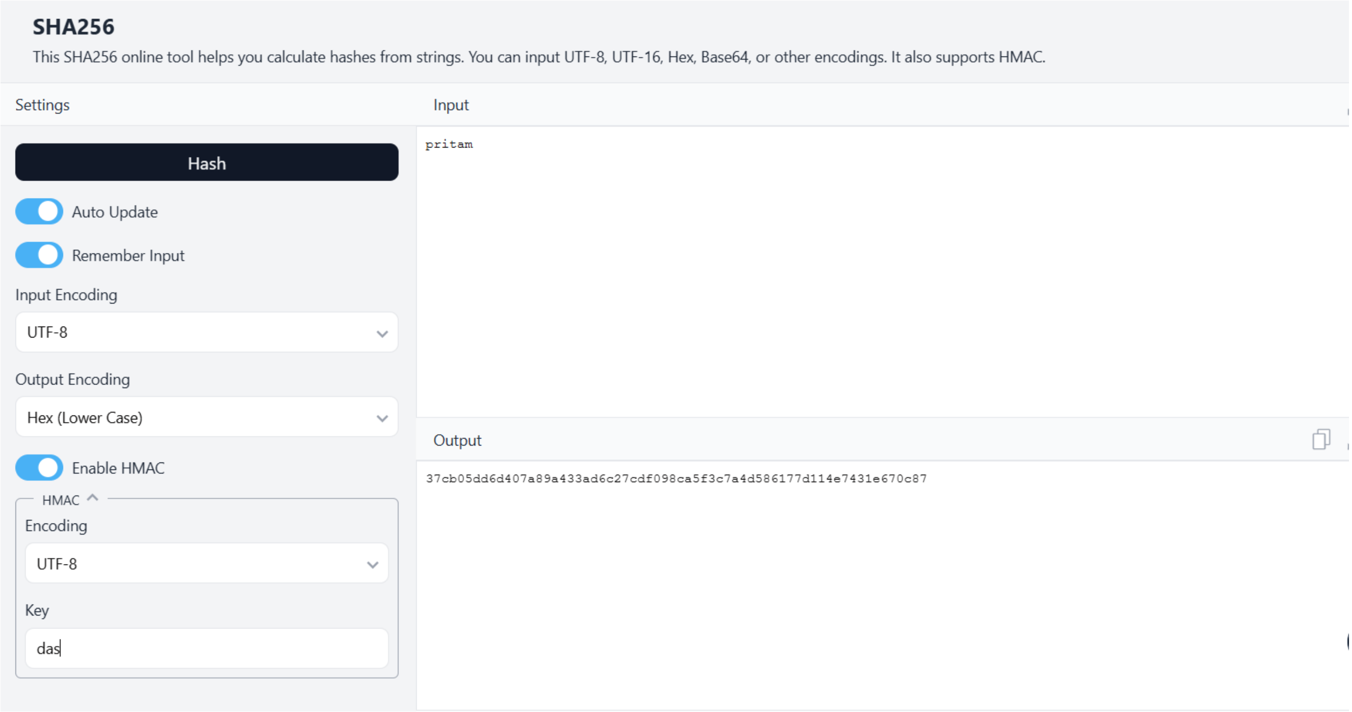
Output

```
19eea17901db38cfb97f3a2ac39effc5ad809278130dd9bb86bd074aa335bdc4
```

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

* Implementation Phase: Final Output (no error)

If we want more privacy then we have to on HMAC(hash-based message authentication code) ,in this you have to put some rivate key for more security



SHA256

This SHA256 online tool helps you calculate hashes from strings. You can input UTF-8, UTF-16, Hex, Base64, or other encodings. It also supports HMAC.

Settings

Hash

Auto Update

Remember Input

Input Encoding: UTF-8

Output Encoding: Hex (Lower Case)

Enable HMAC

HMAC

Encoding: UTF-8

Key: das

Input

```
pritam
```

Output

```
37cb05dd6d407a89a433ad6c27cdf098ca5f3c7a4d586177d114e7431e670c87
```

*Observations:

1. Each input generated a unique and fixed 64-character SHA-256 hash.
2. Slight changes in the input caused major changes in the hash (avalanche effect).
3. The tool supports various input/output encodings and optional HMAC functionality.

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 :

Regn. No. :

Signature of the Faculty:

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