

SKILL 3

[CS601] – Cryptography and Blockchain

Date – 01/02/2023 | *By* Aishwarya Suryakant Waghmare, PRN – 2001106059

Title :

SHA256 Implementation using the python code.

Skills/Competencies to be acquired :

- Making use of python code to implement the code.
- Making use of the logic of the SHA256 algorithm.

Time taken to complete the activity :

One Hour

Purpose of the activity :

To implement the SHA256 implementation algorithm by making use of the python code.

Steps performed in this activity :

Code written for the SHA256 implementation is as follows :

```
# Python code to check for the available algorithms
import hashlib
```

```
# Print all the available algorithms
print("The available algorithms are : ", end = "")
print(hashlib.algorithms_guaranteed)
```

```
# Python code to demonstrate the SHA256 algorithms
import hashlib
```

```
# Initializing the string
str = "Blockchain and Cryptocurrency"
```

```
# Encode the string then send it to the SHA256
result = hashlib.sha256(str.encode())
```

```
# Printing the equivalent hexadecimal value
print("The hexadecimal equivalent of SHA256 is : ")
print(result.hexdigest())
print("\r")
```

```
# initializing string
str = "Skill Assignment"
```

```
# encoding GeeksforGeeks using encode()
# then sending to SHA384()
result = hashlib.sha384(str.encode())
```

```
# printing the equivalent hexadecimal value.
print("The hexadecimal equivalent of SHA384 is : ")
print(result.hexdigest())
```

```
print ("\r")
```

```
# initializing string
str = "SHA256 Implementation"
```

```
# encoding GeeksforGeeks using encode()
# then sending to SHA224()
result = hashlib.sha224(str.encode())
```

```
# printing the equivalent hexadecimal value.
print("The hexadecimal equivalent of SHA224 is : ")
print(result.hexdigest())
```

```
print ("\r")
```

```
# initializing string
str = "Aishwarya Waghmare"
```

```
# encoding GeeksforGeeks using encode()
# then sending to SHA512()
result = hashlib.sha512(str.encode())
```

```

# printing the equivalent hexadecimal value.
print("The hexadecimal equivalent of SHA512 is : ")
print(result.hexdigest())

print ("\r")

# initializing string
str = "CS601 - BlockChain and Cryptography - Skill 3"

# encoding GeeksforGeeks using encode()
# then sending to SHA1()
result = hashlib.sha1(str.encode())

# printing the equivalent hexadecimal value.
print("The hexadecimal equivalent of SHA1 is : ")
print(result.hexdigest())

```

Output/ Presentation prepared :

```

[1] # Python code to check for the available algorithms
import hashlib

# Print all the available algorithms
print("The available algorithms are : ", end = "")
print(hashlib.algorithms_guaranteed)

The available algorithms are : {'sha3_224', 'sha3_256', 'sha512', 'sha3_512', 'md5', 'sha224', 'sha384', 'shake_128', 'shake_256', 'sha1', 'blake2s', 'sha256', 'sha3_384', 'blake2b'}

# Python code to demonstrate the SHA256 algorithms
import hashlib

# Initializing the string
str = "Blockchain and Cryptocurrency"

# Encode the string then send it to the SHA256
result = hashlib.sha256(str.encode())

# Printing the equivalent hexadecimal value
print("The hexadecimal equivalent of SHA256 is : ")
print(result.hexdigest())

print("\r")

The hexadecimal equivalent of SHA256 is :
e1b53203c18c6ca8e1177efd77c7c636f8f27d9ed1c17b283b483291cf497c

```

completed at 11:03AM

```
# printing the equivalent hexadecimal value.
print("The hexadecimal equivalent of SHA512 is : ")
print(result.hexdigest())

print("\n")

# initializing string
str = "CS601 - BlockChain and Cryptography - Skill 3"

# encoding GeeksforGeeks using encode()
# then sending to SHA1()
result = hashlib.sha1(str.encode())

# printing the equivalent hexadecimal value.
print("The hexadecimal equivalent of SHA1 is : ")
print(result.hexdigest())
```

The hexadecimal equivalent of SHA384 is :
70bf7742df9928806a554916e88db52a7b7b9059675ab39f81fb0baf38fca31bfca5b7dad7f6f310a7ba895840096

The hexadecimal equivalent of SHA224 is :
b8ed1b598e7f7e95c7f2b3835bc309a8c21b154865ec389a3e6e4b90

The hexadecimal equivalent of SHA512 is :
722a9eb4b66f30b9be487d15294db5dd289b58e77a9a21613a16ba370279f975987f9281b1cee54a558a4ba4d81313a82020ada884dc944d14151fad61599d07

The hexadecimal equivalent of SHA1 is :
947cbf79c95564a8d0a37fe332b3143424d92354

0s completed at 11:22 AM

Resources/ tools used for the skill activity :

- Laptop
- Google Colab
- Lecture Notes
- E-References
- E-books.

Skills/ Competencies acquired and Result/ Conclusion :

Therefore, understood and implemented the SHA256 algorithm by making use of the python code.