

Ques) SHA-1 is a popular heuristic hash function that is currently in trend. In this experiment, we shall familiarize ourselves with SHA-1 as well as look at one important application of hashing, namely, the HMAC algorithm which is currently used in the Internet to achieve data integrity.

Code:

```
#Using hashlib and hmac modules
import hashlib
import hmac
def make_digest(message, key):
# converting into bytes
    key = bytes(key, 'UTF-8')
    message = bytes(message, 'UTF-8')
# creating signature from the digest using sha1
    digester = hmac.new(key, message, hashlib.sha1)
    signature1 = digester.hexdigest()
    print("Hexdigest: ",signature1)
# other functions to display details
    print ("Digest size is(in bytes): " + str(digester.digest_size))
    print ("Block size is(in bytes): " + str(digester.block_size))
    print ("Canonical name(encryption Algorithm used): " + digester.name)
# main function
message=input("Enter the message(used in SHA1): ")
key=input("Enter the key(used in MAC): ")
make_digest(message,key)
```

Output:

```
1 #Using hashlib and hmac modules
2 import hashlib
3 import hmac
4 def make_digest(message, key):
5 # converting into bytes
6     key = bytes(key, 'UTF-8')
7     message = bytes(message, 'UTF-8')
8 # creating signature from the digest using sha1
9     digester = hmac.new(key, message, hashlib.sha1)
10    signature1 = digester.hexdigest()
11    print("Hexdigest: ",signature1)
12    # other functions to display details
13    print ("Digest size is(in bytes): " + str(digester.digest_size))
14    print ("Block size is(in bytes): " + str(digester.block_size))
15    print ("Canonical name(encryption Algorithm used): " + digester.name)
16 # main function
17 message=input("Enter the message(used in SHA1): ")
18 key=input("Enter the key(used in MAC): ")
19 make_digest(message,key)
```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell <https://aka.ms/pscore6>
PS C:\Users\Rishabh\documents\cp> python -u "c:\Users\Rishabh\documents\cp\assessment6.py"
Enter the message(used in SHA1): rishabh
Enter the key(used in MAC): rishabh
Hexdigest: e3aae8dc5a95df4ef5acff017a0588a1e9ea2f85a
Digest size is(in bytes): 20
Block size is(in bytes): 64
Canonical name(encryption Algorithm used): hmac-sha1
PS C:\Users\Rishabh\documents\cp>