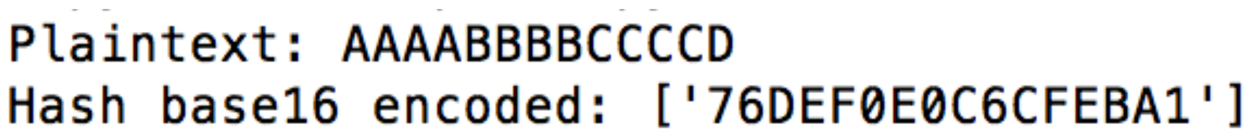
Kennan Lyle Seno
D14123582
Lab 7

Question 1

To run the python script, type ‘python lab7-part1.py’ in the terminal.

Output:



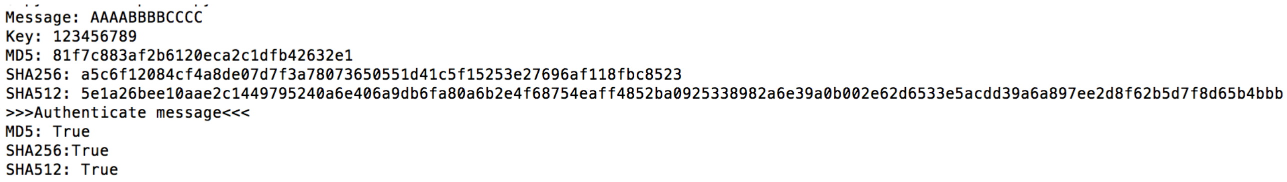
```
Plaintext: AAAABBBBCCCCD
Hash base16 encoded: ['76DEF0E0C6CFEBA1']
```

The screenshot above shows that output when a before and after the plaintext is hashed using hash function using compression function DES-ECB in Davies-Meyer mode and follows the approach of Merkle-Damgard Construction.

Questions 2

To run the python script, type ‘python lab7-part2.py’ in the terminal.

Output:



```
Message: AAAABBBBCCCC
Key: 123456789
MD5: 81f7c883af2b6120eca2c1dfb42632e1
SHA256: a5c6f12084cf4a8de07d7f3a78073650551d41c5f15253e27696af118fbc8523
SHA512: 5e1a26bee10aae2c1449795240a6e406a9db6fa80a6b2e4f68754eaff4852ba0925338982a6e39a0b002e62d6533e5acdd39a6a897ee2d8f62b5d7f8d65b4bbb
>>>Authenticate message<<<
MD5: True
SHA256:True
SHA512: True
```

The screenshot above shows the MAC using different algorithm and authentication on each to check that if came from the correct sender