Information Security & Cryptography

Nehal Jhajharia

Lab Assignment 7

Use any crypto library (available in Java, Python/ C++/ .net) to implement AES and SHA.

```
from hashlib import sha256

plain_text = input("Enter plain text: ")

sha_digest = sha256(plain_text.encode()).hexdigest()

print("SHA: %s" % sha_digest)

from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes

key = get_random_bytes(16)
cipher = AES.new(key, AES.MODE_EAX)
ciphertext, tag = cipher.encrypt_and_digest(plain_text.encode())
print("AES digest: %s" % ciphertext)



d_cipher = AES.new(key, AES.MODE_EAX, nonce=cipher.nonce)
decrypted = d_cipher.decrypt(ciphertext)
print("AES decrypted: %s" % decrypted.decode())
```

```
jhajharia@Nehals-MacBook-Air Asmt7 % source venv/bin/activate
(venv) jhajharia@Nehals-MacBook-Air Asmt7 % python main.py
Enter plain text: nehaljhajharia
SHA: b92fa82cc0301fac7076876d9e8729e70cbecbdb0f9b8e498a481c083fc79351
AES digest: b'"\x12F)\xb9\xa9\x85.\xd8\xfe\xfc\x02\xe4Y'
AES decrypted: nehaljhajharia
(venv) jhajharia@Nehals-MacBook-Air Asmt7 %
```