Kennan Lyle Seno
D14123582
Lab 3

NOTE:

I have created an encrypt and decrypt function to be used for questions 1-3 by passing different values as arguments.

- encrypt(key, plainText, mode, iv, padding)
  - key (String) - key used to encrypt the plaintext
  - plainText (String) - plaintext to be encrypted
  - mode (MODE_ECB, MODE_CBC) - mode of operation that will be used
  - iv (String) - Initial value that will be used if mode == MODE_CBC
  - padding (Boolean) - specify if padding should be used or not
- decrypt(key, cipherText, mode, iv)
  - key (String) - key used to encrypt the plaintext
  - cipherText (String) - ciphertext to be decrypted
  - mode (MODE_ECB, MODE_CBC) - mode of operation that will be used
  - iv (String) - Initial value that will be used if mode == MODE_CBC

Output Code:

```
key = '12345678'
iv = '00000000'

print "------------------------Q1----------------------------------"
text = 'AAAABBBBAAAABBBB'
cipherText = encrypt(key, text, DES.MODE_ECB, '', False)
print "Encrypted text: " + cipherText
print "Decrypted text: " + decrypt(key, cipherText, DES.MODE_ECB, '')

print "------------------------Q2----------------------------------"
text = 'AAAABBBBAAAABBBB'
cipherText = encrypt(key, text, DES.MODE_CBC, iv, False)
print "Encrypted text: " + cipherText
print "Decrypted text: " + decrypt(key, cipherText, DES.MODE_CBC, iv)

print "------------------------Q3----------------------------------"
text = 'AAAABBBBCCCC'
cipherText = encrypt(key, text, DES.MODE_ECB, '', True)
print cipherText
decryptedText = decrypt(key, cipherText, DES.MODE_ECB, '')
print "Decrypted text: ", decryptedText, " length: ", len(decryptedText)
```

Output:

```
------------------------Q1----------------------------------
Encrypted text: 19ff4637bb2fe77c19ff4637bb2fe77c
Decrypted text: AAAABBBBAAAABBBB
------------------------Q2----------------------------------
Encrypted text: aac823f6bbe58f9eaf1fe0eb9ca7eb08
Decrypted text: AAAABBBBAAAABBBB
------------------------Q3----------------------------------
19ff4637bb2fe77cc57e62a6316c0676
Decrypted text:  AAAABBBBCCCC  length:  16
```