REPORT 7

学籍番号：08D18151

氏名：山下慎太郎

- 課題 11-1

  <考え方>

  ユークリッドの互除法の公式通りに実装した。

  <結果>

```
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_1.py
x =  63 y =  99
gcd =  9
```

```
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_1.py
x =  120 y =  38
gcd =  2
```

  <ソースコード>

```
while(store_x != 0):
    store_x = y % x
    store_y = x
    x = store_x
    y = store_y
    gcd = store_y
```

- 課題 11-2

  <考え方>

  keyA を random で生成し、11-1 の関数に N と keyA を引数にし、gcd が 1 になるまで生成させる。

  <結果>

```
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_2.py
keyA =  47 keyB =  68
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_2.py
keyA =  9 keyB =  70
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_2.py
keyA =  27 keyB =  2
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_2.py
keyA =  89 keyB =  1
```

  <ソースコード>

```
N = 100
while(1): #gcd が 1 になるまで繰り返す
    keyA = random.randint(2, N-1)
    if euclid(keyA, N) == 1:
        break
keyB = random.randint(1, N-1)
```

- 課題 11-3

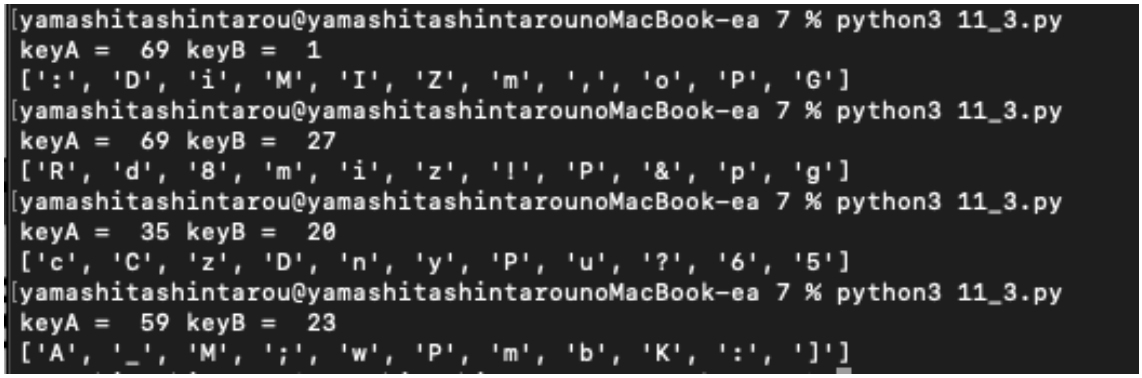
<考え方>

encode する部分は前回の部分の関数を利用した。

アフィン暗号を afin.append(str_list[(keyA*i+keyB) % N])として生成した。

<結果>

与えるテキストは"asdlfkj!?　)"



<ソースコード>

```
while(1):
    keyA = random.randint(2, N-1)
    if euclid(keyA, N) == 1:
        break
keyB = random.randint(1, N)

for i in range(int(len(str_list)/2)):
    afin.append(str_list[(keyA*i+keyB) % N])
```

```
encoded = encode(text, afin, str_list)
```

- 課題 11-4

  <考え方>

  decode する関数を生成した。

  前回の課題の decode 関数を使用した。

  <結果>

```
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_4.py
keyA =  3 keyB =  22
encoded =  ['S', '.', 'b', 'z', 'h', 'w', 't', 'y', 'N', 's', '"']
decoded =  ['a', 's', 'd', 'l', 'f', 'k', 'j', '!', '?', ' ', ')']
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_4.py
keyA =  71 keyB =  30
encoded =  ['.', 'm', 'n', 'h', 'R', 's', '3', '!', '-', 'E', 'J']
decoded =  ['a', 's', 'd', 'l', 'f', 'k', 'j', '!', '?', ' ', ')']
[yamashitashintarou@yamashitashintarounoMacBook-ea 7 % python3 11_4.py
keyA =  49 keyB =  33
encoded =  ['_', '5', '8', 'q', ']', '[', 'a', '1', 'y', 'l', '0']
decoded =  ['a', 's', 'd', 'l', 'f', 'k', 'j', '!', '?', ' ', ')']
```

  <ソースコード>

```
f = open("encoded.txt", "w") #encoded.txt 生成
for i in range(len(encoded)):
    f.write(encoded[i])
f.close()

with open('encoded.txt') as f: #encoded.txt に書かれているテキストを読み込む
    text = f.read()

decoded = decode(encoded, afin, str_list)
print("decoded = ",decoded)

f = open("decoded.txt", "w") #decoded.txt に decode した内容を書き込む
for i in range(len(decoded)):
    f.write(decoded[i])
```

```
f.close()
```