




プログラミング技法II

担当： 新田 直子

大学院工学研究科 電気電子情報工学専攻

naoko@comm.eng.osaka-u.ac.jp



出席確認のため、
チャットに**学籍番号＋氏名と共に**
出席した旨書いて下さい！！



これまでの課題に対するコメント

例：回文

- **課題9**: english_wordlist.txtを読み込み、回文（前から読んでも後ろから読んでも同じ語句）となる単語の個数を調べ、単語をリストアップせよ。

```
word = 'Hello World!'
```

```
flag = 0
```

```
for i in range(len(word)//2):
```

```
    if word[i]!=word[len(word)-i-1]:
```

```
        flag = 1
```

```
word[::-1]            '!dlroW olleH'
```

```
if word==word[::-1]
```

例:シーザー暗号

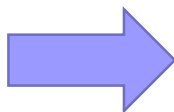
文字集合 $C = \{c_0, c_1, \dots, c_{N-1}\}$ に属する文字により構成されるテキスト(文字列)を暗号化することを考える。文字 $c_i \in C$ は整数値 i に置き換えられるものとし、 c_i を $j = i + b \pmod{N}$ で算出される c_j で置き換える暗号法をシーザー暗号という。
ただし、 b は鍵であり、 $1 \leq b < N$ とする。

```
if (i+b)>N:
```

```
    j = (i+b)-N
```

```
else:
```

```
    j = i+b
```

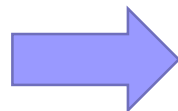


```
j = (i+b) % N
```

```
for i in range(len(LETTERS)):
```

```
    if LETTERS[i]=='X':
```

```
        idx = i
```



```
LETTERS.index('X')
```

```
for l, x in enumerate(LETTERS):
```

```
    if x=='X':
```

```
        idx = i
```



今週の課題

※ユークリッドの互除法については、ウェブなどで調べよ。

例：アフィン暗号

文字集合 $C = \{c_0, c_1, \dots, c_{N-1}\}$ に属する文字により構成されるテキストを暗号化することを考える。文字 $c_i \in C$ は整数値 i に置き換えられるものとし、 c_i を $j = a \times i + b \pmod{N}$ で算出される c_j で置き換える暗号法をアフィン暗号という。ただし、 a 、 b は鍵であり、 $2 \leq a < N$ 、 $1 \leq b < N$ 、 a と N は互いに素 (a と N の最大公約数 $\gcd(a, N)$ が 1) であるものとする。

- **課題11-1**: ユークリッドの互除法(※)を利用して、 x と y の最大公約数 $\gcd(x, y)$ を求める関数を作成せよ。
- **課題11-2**: 課題11-1で作成した関数とモジュール `random` を用いて、アフィン暗号の条件を満たすような2つの鍵 $\text{keyA} = a$ 、 $\text{keyB} = b$ を生成する関数を作成せよ。

例：アフィン暗号

文字集合 C を、アルファベット大文字小文字、数字、記号(スペース、-、!、"、&、'、(、)、*、,、.、:、;、[、]、_、`、?、改行の19種類)とする。

- **課題11-3:** 2つの鍵とテキストが与えられたとき、アフィン暗号による暗号文を返す関数を作成せよ。
- **課題11-4:** 文字集合 C に属する文字に構成される任意のテキストをテキストファイル(例: plaintext.txt)に保存せよ。このテキストファイルを読み込み、課題11-2で作成した2つの鍵を用いて暗号化し、暗号文を別のテキストファイルに保存するプログラムを作成せよ。

レポートの提出

- 課題11-1～11-4に取り組む。
- 各課題に対し、プログラム作成時の方針、工夫点など、**ソースコード**(**考え方の説明**に使う。
重要な部分のみでよい)、**実行結果**
(適切なテストケースに対する動作確認)を
レポートに記載する。
- レポートとソースコード(.pyの形式)を**CLEから**提出する。
- **zip圧縮はしないこと！**
- 読みやすいレポートとするよう心がけること。
- 提出期限：6月18日(木)



来週の課題

例：アフィン暗号

※拡張ユークリッドの互除法については、ウェブなどで調べよ。

$ax = 1 \pmod{N}$ となる x は、 N を法とする a の乗法の逆元($x = a^{-1}$)である。アフィン暗号による暗号文は、暗号化した際の鍵 a 、 b が既知であれば、 c_j を $i = a^{-1} \times (j - b) \pmod{N}$ で算出される c_i で置き換えることにより解読できる。


- **課題11-5:** 拡張ユークリッドの互除法(※)を利用して、 a と N が与えられたとき、 $ax = 1 \pmod{N}$ となる x を求める関数を作成せよ。
- **課題11-6:** 課題11-4で作成した暗号文と暗号化に用いた2つの鍵が与えられたとき、課題11-5で作成した関数を用いて、暗号文を解読した結果を出力するプログラムを作成せよ(課題11-4で暗号文を保存した後に追記し、解読文が平文と等しいか確認すればよい)。

レポートの提出

- 課題11-5～11-6に取り組む。
- 各課題に対し、プログラム作成時の方針、工夫点など、**ソースコード**(**考え方の説明**に使う。
重要な部分のみでよい)、**実行結果**
(適切なテストケースに対する動作確認)を
レポートに記載する。
- レポートとソースコード(.pyの形式)を**CLEから**提出する。
- **zip圧縮はしないこと！**
- 読みやすいレポートとするよう心がけること。
- 提出期限：6月25日(木)

提出物に関する注意点

- レポートのないもの、ソースプログラム、実行結果を張り付けただけのレポート（説明のないもの）は採点しません。
- レポートは必ず1つのファイルにまとめること（基本的に参照されている別ファイルは見ません。貼り付けが困難な程、長さのあるテキストファイルなどは除く）。
- ソースコードが添付されていないものは動作確認困難なため減点します。
- 他人のソースコード、レポートの**コピーは厳禁**。
発見した場合は、採点できません。
参考にした場合などは、出典（誰の何を参考にしたか）を明記すること。
※変数名を変更したのみの場合などはコピーに含みます。



出席確認のため、
チャットに**学籍番号＋氏名と共に**
出席した旨書いて下さい！！