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
http://www2c.comm.eng.osaka-u.ac.jp/~prog1/

例：アフィン暗号

※ユークリッドの互除法については、
ウェブなどで調べよ。

文字集合$C = \{c_0, c_1, \cdots, c_{N-1}\}$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$\mathrm{keyA} = a$、$\mathrm{keyB} = b$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。

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）。

例：アフィン暗号

- 課題11-7: あるテキストが与えられたとき、文中に含まれる英単語の割合を算出する関数を作成せよ。
  ただし英単語のリストはenglish_wordlist.txtから得てよい。
  また、できるだけ正しく英単語の割合が算出できるよう、テキストに対してはアルファベットのみから構成される単語を抽出するといった前処理を施すこと。

- 課題11-8: 暗号文のみが与えられたとき、有り得るすべての鍵a、bを用いて課題11-6と同様に暗号文を解読する。
  各鍵対に対して出力される解読文に対し、課題11-7で作成した関数を用いて、含まれる英単語の割合を算出し、それに基づき、暗号化の際に用いられたと推定される鍵a、b、及び解読結果を出力するプログラムを作成せよ。

例：アフィン暗号

※ 一般的な英文での文字の頻度は
暗号文に対する平文以外から求めること

課題11-9: c_iは$j = a \times i + b \pmod N$で算出される$c_j$で置き換えられる
ため、c_iとc_jの対が2対あれば、a、bが求められる。
そこで、英文における文字の頻度の偏りを利用して
c_iとc_jの対を2対推測する。例えば、一般的に英文で
最も使われる文字は'e'、最も使われない文字は'z'とする。
このとき、暗号文において最も使われている文字、
使われていない文字をそれぞれ'e'、'z'に対するc_jと推測する。
このように頻度に基づき、a、bの候補を限定した上で、
課題10-8と同様に、暗号化の際に用いられたと推定される
鍵a、b、及び解読結果を出力するプログラムを作成せよ。
ただし、一般的な英文での文字の頻度（※）と暗号文における
文字の頻度に基づき、2対のc_iとc_jの候補を決定する関数、
及び、2対のc_iとc_jからa、bを求める関数を作成して用いよ。

例：アフィン暗号

課題11-10: enc_wa.txtを読み込み、課題11-8、課題11-9で作成したプログラムにより、鍵及び元の平文を推定せよ。
候補となった鍵対の数、及び解読にかかった時間を比較せよ。

※ timeモジュールを用いて
import time
time.time()で現在時刻（ある起点からの経過時間）が取得できる。

課題11-11: 適当な平文を$(a, b) = (1,0)$、$a \geq N$、$b \geq N$、Nと互いに素でないaなどの鍵で暗号化した後、必要であれば、課題11-6で作成したプログラムを用いて、鍵を用いて暗号文を解読したり、課題11-10で作成したプログラムを用いて鍵及び元の平文を推定し、どのような問題が生じるか考察せよ。

レポートの提出

- 課題11-1～11-11に取り組む。
- 各課題に対し、プログラム作成時の考え方、
  ソースプログラム、実行結果、考察を
  レポートに記載する。
- レポートとソースコードを入れたフォルダを圧縮し
  下記アドレスに提出する。
  prog2@nanase.comm.eng.osaka-u.ac.jp
- 読みやすいレポートとするよう心がけること。
- Subjectは「【Report5】学籍番号 氏名」とする。
- 提出期限：7月18日（木）