課題　公開鍵暗号方式による暗号化・復号化プログラムを作成する

共通鍵暗号方式では暗号化する人と復号化する人が同じ鍵を持つ必要があるが，ネットワークを介してこの鍵を送るとするとその送信のための暗号化をどうするのかという問題が生じる．そこで考え出されたのが公開鍵暗号方式である．公開鍵暗号方式では，2 つの鍵を用意し一方を暗号化に用いる公開鍵，もう一方を復号化に用いる秘密鍵とする．自分に情報を送信して欲しい相手には公開鍵を用いて暗号化してもらうが，この暗号の解読は公開鍵では行えず，自分が持っている秘密鍵でしか行えない．したがって，公開鍵は誰に知られても良いことになる．このような公開鍵暗号方式としては RSA 暗号化が代表的である．この RSA 暗号化による暗号化・復号化のプログラムを作成せよ．

RSA 暗号化

まず，互いに異なる 2 つの素数を用意しそれぞれ p，q とし，$n = pq$ を法とする世界を考える (n 以上の数は n で割った余りとなる)．次に，e を $(p-1)(q-1)$ と互いに素となる $(p-1)(q-1)$ より小さな整数とし，この e を暗号化に用いる秘密鍵とする．公開鍵 e と法とする数 n は公開することになる．このとき，暗号化は以下の式で行われる (mode n は n で割った余りを表す)．

$$b = a^e \bmod n$$

一方，復号化は d を

$$d = \frac{m(p-1)(q-1)+1}{e} \qquad (m \text{ は任意の正の整数})$$

を満たす整数として，以下の式で行う．

$$a' = b^d \bmod n$$

これは，以下の関係式が成り立つことによる．

$$a^{(p-1)(q-1)} \bmod n = 1$$

実際，暗号化された情報 b の d 乗を考えると

$$b^d \bmod n = (a^e)^d \bmod n = a^{(p-1)(q-1)+1} \bmod n = a$$

である．n を公開しているので n を素因数分解できれば p，q がわかり秘密鍵 d を計算されてしまうが，p，q が非常に大きな数である場合の n の素因数分解の効率的な方法は現在のところ見出されていない (ことになっている)．

公開鍵暗号は電子署名としても使うことができ，秘密鍵で暗号化したデータを送信し，公開鍵で復号化することができれば本人であることが確認できる．

(実行例)

$p = 13$，$q = 19$，$e = 5$ としたときの暗号化の結果を以下に示す．簡単のため，各文字は対応するアスキーコードで数値化し，一文字ごとに暗号化を施した．

```
(例) This is a pen.  --> 曹 O^TO^T+^B2
```

実際には，1 文字ごとの暗号化では公開鍵を用いて使われているそれぞれの文字がどの文字に変換されるかの表を作ることで暗号を解読できてしまうが，非常に大きな単位でコード化されている場合にはその全てに対して表を作ることはできなくなる．