2011.06.13(第 9 回)

p, q を素数とする ($p \neq q$). $n = pq$, $n' = (p-1)(q-1)$ とおく.

$$ed = 1 \mod n'$$

となる数の組 (e, d) を見つける.
公開: n と e (公開鍵)
秘密: p, q および d (秘密鍵)
m の暗号化: $m' = (m^e) \,\%\, n$
m' の復号化: $(m')^d \,\%\, n$.

練習 1　1. $p = 5$, $q = 7$, $e = 5$ の時, gcd アルゴリズム (互除法) を用いて秘密鍵 d を生成せよ.

2. 数字 m を公開鍵で暗号化したら 33 であった. m を求めよ.

練習 2　1. $p = 7$, $q = 13$, $e = 5$ の時, gcd アルゴリズムを用いて秘密鍵 d を生成せよ.

2. 数字 m を公開鍵で暗号化したら 81 であった. m を求めよ.

練習 3 "RSA 暗号系では n が公開されているのだから, n を素因数分解すれば, 秘密の p, q が分かり, 公開された e から gcd アルゴリズムで秘密鍵の d もわかってしまう. 一体これのどこが暗号なのですか?"
この疑問に対する答えは?

Risa/Asir ドリルは `http://www.math.kobe-u.ac.jp/Asir` の日本語ページにあり. 17 章を参照. ここにより本格的な解説がある.
サンプルプログラムは `http://www.math.kobe-u.ac.jp/HOME/taka/2011/c1` よりダウンロードできる.