

# RSA 暗号鍵作成シート

東京電機大学工学部  
情報通信工学科  
ワークショップ

## 1 鍵の作成

1. 素数を二つ思いつき、積を求めましょう

$p =$

$q =$

$n(= pq) =$

2. オイラー関数  $\varphi(n) = (p - 1)(q - 1)$  を計算しましょう

$\varphi(n) =$

3. オイラー関数の値と互いに素な数  $e$ (暗号鍵) を思いつきましょう

$e =$

4. オイラー関数の値  $\varphi(n)$  と暗号鍵  $e$  でユークリッドの互除法を行いましょう (過程をすべて記述すること)

5. ユークリッドの互除法を逆にたどり、値を代入していくことで  $a\varphi(n) + de = 1$  となる  $a, d$  を求めましょう。この  $d$  が復号鍵になります。

$a =$

$d =$

6. 公開鍵

$e =$

$n =$

7. 秘密鍵

$d =$

$n =$

## 2 試してみよう

$p, q$  と互いに素な数は暗号化することができます。

1. 暗号化したい数  $x$ (これが平文) を選びます。

$x =$

2.  $y = x^e \bmod n$  を計算します。これが暗号文になります。

$y =$

3.  $y^d \bmod n$  を計算します。これで暗号文を復号したことになります。