情報システム工学科
伊達 章



# インターネットのセキュリティ：公開鍵暗号

- 暗号化：平文 ($M$) から暗号文 ($C$) への変換
- 復号化（解読）：暗号文から平文への変換

$M$: メッセージ（Message）
$C$: 暗号文 (Cipher)

- 共有鍵暗号

  暗号化と復号化で用いる鍵が同一.
  例： DES (data encryption standard)
  暗号化：平文を 64 ビットのブロックに区切り，置換と転置を複雑に繰り返す.
  置換処理：文字とコードの対応を変える処理. 例： MIYAZAKI → NJZB[BLJ
  転置処理：出現の順番を入れ替える処理. 例：MIYAZAKI → ZYIJAAKM

  問題点：

  - どのように鍵を安全に配送するか.
  - 通信相手ごとに異なる鍵が必要. → たくさんの鍵を管理する必要がある.

- 公開鍵暗号

  公開鍵 (Public key) と秘密鍵 (Private key) という二つの鍵を使用する暗号方式

  例： RSA 方式 （2000 年 9 月に特許切れ）

  R.L. Rivest, A. Shamir and L. Adleman: "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120–126, Feb 1978.

  特徴：

  - 2 つの鍵がペアになって，はじめて機能する．
  - 片方の鍵で暗号化すれば，もう一方の鍵で復号化できる．
  - 使い方は「暗号文の送付」と「電子署名の認証」の 2 通り．
  - 事前に公開鍵を相手に渡しておくだけでよく，秘密に鍵を交換する必要がない．
  - 自分の秘密鍵だけを秘密に持っていればよく，管理すべき鍵の個数が少なくてすむ．
  - 大きな数の素因数分解が困難である性質を利用．

  数学的基盤：

  - 記号：以下で $e, d, n, M, C$ はすべて正の整数．
    $\bmod n$ というのは $n$ で割った余り．　　例： $7 \bmod 3 = 1$.
  - $M = (M^e)^d \bmod n$, $\quad {}^\forall M \in \{1, \cdots, n-1\}$ が成り立つ数の組 $(e, d, n)$ を使う．
    例： $M = (M^{11})^{23} \bmod 377 = M^{253} \bmod 377$ （$e = 11, d = 23, n = 377$）
    実は，どんな $M(= 1, \cdots, 376)$ の値に対しても，この式は成立している!!
  - 上式を満たす $e, d, n$ の組を，どのように決めるかについては少し難しいので省略．

  使い方 1：暗号文の送付．　例：ヒデからリエに秘密にメッセージ「$M$」を伝えたい場合

  - 問題設定：「$M$」は 1 から 376 までの，ある整数．
    リエの公開鍵は $(e, n)$，秘密鍵は $(d, n)$，　$e = 11, d = 23, n = 377$.
    公開鍵は誰でも知ることができるが，秘密鍵はリエしか知らない．
  - 1. 暗号化：ヒデはリエの公開鍵 $(e, n)$ を使い，メッセージ $M$ を $C = M^e \bmod n$ と暗号化して送る．
  - 2. 復号化：リエは自分の秘密鍵 $(d, n)$ を使い，暗号文 $C$ を $M = C^d \bmod n$ として，もとのメッセージを復元する．

  使い方 2： 電子署名の認証．　　例：ヒデが，このメッセージ（署名）が確かにヒデ本人からのものであることをリエに伝えたい場合．

  - 1. 暗号化： ヒデは自分の秘密鍵で署名を暗号化して送る．
  - 2. 復号化： リエはヒデの公開鍵を使い復号化し，署名を確認する．

  RSA 方式の安全性の根拠

  - 通常 $n$ は 1024 ビット程度の数で，2 つの素数 $p, q$ の積．
  - 大きな正数の素因数分解は困難．→ この事実がくずれると危ない．

その数学的しくみ：

- $M = (M^e)^d \bmod n, \quad {}^\forall M \in \{1, \cdots, n-1\}$ が成り立っていた.
  $\underline{M = (M^e)^d \bmod n = (M^e \bmod n)^d \bmod n = C^d \bmod n}$ も成り立つ.
  これが，もとのメッセージを復元できる理由.
- 「大きくなる前に適宜割っていっても，最終的な余りは変わらない」
  例： $26 \bmod 3 = (13 \times 2) \bmod 3 = (13 \bmod 3) \times (2 \bmod 3) = 1 \times 2 = 2$
- 実際の数値を使った例：
  - 「97」を公開鍵 $(11, 377)$ を使って暗号化：$C = 97^{11} \pmod{377}$
    $97^{11} = 97^{(1+2+8)} = 97 \times 97^2 \times 97^8$
    → それぞれの $(\text{mod } 377)$ を計算
    $97^2 \pmod{377} = 9409 \pmod{377} = 361 \pmod{377}$
    $97^4 \pmod{377} = 361^2 \pmod{377} = 130321 \pmod{377} = 256 \pmod{377}$
    $97^8 \pmod{377} = 256^2 \pmod{377} = 65536 \pmod{377} = 315 \pmod{377}$
    $C = 97^{11} \pmod{377} = 97 \times 361 \times 315 \pmod{377}$
    $= 11030355 \pmod{377} \rightarrow 89$

  - 「89」を秘密鍵 $(23, 377)$ を使って復号化：$M = 89^{23} (\text{mod } 377)$
    $89^{23} = 89^{(1+2+4+16)} = 89 \times 89^2 \times 89^4 \times 89^{16}$
    → それぞれの $(\text{mod } 377)$ を計算
    $89^2 = 7921 = 4 \pmod{377}$
    $89^4 \pmod{377} = 89^{2^2} \pmod{377} = 4^2 \pmod{377} = 16 \pmod{377}$
    $89^8 \pmod{377} = 89^{4^2} \pmod{377} = 16^2 \pmod{377} = 256 \pmod{377}$
    $89^{16} \pmod{377} = 89^{8^2} \pmod{377} = 65536 \pmod{377} = 315 \pmod{377}$
    $M = 89^{23} \pmod{377} = 89 \times 4 \times 16 \times 315 \pmod{377} = 89 \times 4 \times 5040$
    $(\text{mod } 377) = 89 \times 4 \times 139 \pmod{377} = 49484 \pmod{377} \rightarrow 97$