RSA暗号
Riverst-Shamir-Adleman

情報科学の世界II

2019年度

只木　進一（理工学部）

RSA暗号概要

- 整数論という数学の応用
- 因数分解が困難であることに基づく
- 公開鍵暗号に利用される
- James H. Ellis (1969)及びClifford Cocks(1973)が理論的基礎を発見したが、長く秘密にされていた
- 1977年にRSAが公表。

整数の合同
Congruence

- 二つの整数aとb。ある整数mで除した余りが等しい
  - aとbは法mについて合同：$a \equiv b \pmod{m}$
- $a \equiv a' \pmod{m}$かつ$b \equiv b' \pmod{m}$ならば
  - $ab \equiv a'b' \pmod{m}$

$$a = n_a m + a'$$

$$b = n_b m + b'$$

$$ab = (n_a m + a')(n_b m + b') = (n_a n_b m + n_a + n_b)m + a'b'$$

Fermatの小定理

- pを素数、$a \not\equiv 0 \pmod{p}$
- このとき、$a^{p-1} \equiv 1 \pmod{p}$
- 例示：$p = 11, a = 3$

$$3^2 \equiv 9 \pmod{p}$$

$$3^4 \equiv 81 \pmod{p} \equiv 4 \pmod{p}$$

$$3^8 \equiv 16 \pmod{p} \equiv 5 \pmod{p}$$

$$3^{10} \equiv \left(3^2 \times 3^8\right) \pmod{p} \equiv 45 \pmod{p} \equiv 1 \pmod{p}$$

Fermatの小定理
応用

- pとqを素数、$\gcd(a, pq) = 1$
- このとき、$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$
- 例示：$p = 5, q = 7, a = 11$

$$11^2 \equiv 121 \pmod{35} \equiv 16 \pmod{35}$$

$$11^4 \equiv 256 \pmod{35} \equiv 11 \pmod{35}$$

$$11^8 \equiv 16 \pmod{35}$$

$$11^{16} \equiv 11 \pmod{35}$$

$$11^{4\times 6} \equiv 11^{(16+8)} \pmod{35} \equiv (11\times 16) \pmod{35} \equiv 1 \pmod{35}$$

秘密鍵と公開鍵

- メッセージを受信する者
  - 二つの大きな素数pとqを生成し、秘密鍵とする。
  - $m = pq$
  - $\phi(m)$：mと互いに素である1以上m以下の自然数の数。今は$(p-1)(q-1)$
  - k：$\phi(m)$と互いに素である適当な自然数
- mとkを公開鍵とする

メッセージ暗号化
送信側

- mはLビットであるとする
- メッセージMを$L-1$ビット毎の語に区切る
  - $M = a_0 a_1 \cdots a_n$
- 各語を変換
  - $b_i = a_i^k \pmod m$
  - $M' = b_0 b_1 \cdots b_n$
- M'を送信

復号

- $kv - \phi(m)u = 1$の適当な解(u, v)を得る

$$
\begin{aligned}
b_i^{\,v} &\equiv a_i^{\,kv} \pmod{m} \equiv a_i^{\,1+\phi(m)u} \pmod{m} \\
&\equiv \left(a_i \pmod{m}\right)\left(a_i^{\phi(m)} \pmod{m}\right)^u \\
&\equiv \left(a_i \pmod{m}\right)\left(1 \pmod{m}\right)^u \\
&\equiv a_i \pmod{m}
\end{aligned}
$$

例

- 秘密鍵$p = 13, q = 11, \phi(m) = 120$
- 公開鍵$m = 143, k = 7$
- mは8ビット
  - 7ビット毎の語に分離
- $kv - \phi(m)u = 1$の解$v = 103$

数学的裏付けのある暗号

- 確実に符号化・復号化ができる
  - 数学的に保証されている
- 方式は公開／鍵は非公開
- 素数への因数分解が困難
  - 今のところ有効なアルゴリズムなし
- コンピュータの高速化によって、長い鍵が必要になっている