公開鍵暗号の例: RSA 暗号

Rivest, Shamir, Adleman (1977)

- **大きな素数 p, q を選び、積 $\mathrm{N} = \mathrm{pq}$ を作る**
- **N を用いて、公開鍵 e・秘密鍵 d の対を作る**
- **暗号化の計算は N と公開鍵 e とから可能**
- **復号は秘密鍵 d を用いる**
- **N と公開鍵 e とから秘密鍵 d を求めるには、N の素因子分解 $\mathrm{N} = \mathrm{pq}$ が必要**
- **しかしそれは困難 (膨大な計算時間が掛かる)**

RSA 暗号 (Rivest-Shamir-Adleman)

p, q : 相異なる大きな素数 (実際には 1024 bit 以上)

$N := pq$: RSA 方式の**法 (modulus)**

$m := \mathrm{lcm}(p-1, q-1)$

$\gcd(e, m) = 1$ となる整数 e をランダムに選ぶ

$ed \equiv 1 \pmod{m}$ となる整数 d を求める

- (N, e) : **暗号化鍵 (encryption key)**
  $\longrightarrow$ **公開鍵 (public key)**
- d : **復号鍵 (decryption key)**
  $\longrightarrow$ **秘密鍵 (secret key, private key)**

RSA 暗号 (Rivest-Shamir-Adleman)

p, q：**相異なる大きな素数**

$$N = pq,\ \ m = \mathrm{lcm}(p-1, q-1),\ \ ed \equiv 1 \pmod{m}$$

- (N, e)：**公開鍵 (暗号化鍵)**
- d：**秘密鍵 (復号鍵)**

平文・暗号文は $0, 1, \ldots, N-1$ **に符号化**
(mod$N$ **で考える)**

平文 M **の暗号化：** $\boxed{C = E(M) \equiv M^e \pmod{N}}$

暗号文 C **の復号：** $\boxed{M = D(C) \equiv C^d \pmod{N}}$

RSA 暗号 (Rivest-Shamir-Adleman)

p, q : **相異なる大きな素数**

$$N = pq,\ \ m = \mathrm{lcm}(p-1, q-1),\ \ ed \equiv 1 \pmod{m}$$

平文 M **の暗号化 :** $\boxed{C = E(M) \equiv M^e \pmod{N}}$

暗号文 C **の復号 :** $\boxed{M = D(C) \equiv C^d \pmod{N}}$

元に戻るのか ($D(E(M)) = M$ **か) ?**

$\longrightarrow$ **以下、暫く板書で**

初等整数論の準備

- $(a, b) = 1$ **のとき、** $a|bc \Longrightarrow a|c$

- **特に** p **：素数のとき、**
  $$p|ab \Longrightarrow (p|a \text{ **または** } p|b)$$

- $(m, n) = 1$ **のとき、**
  $$a \equiv b \pmod{mn}$$
  $$\Longleftrightarrow a \equiv b \pmod{m}, a \equiv b \pmod{n}$$

Fermat の小定理

p : **素数のとき、**

- $(a, p) = 1$ **なる** $a \in \mathbb{Z}$ **に対し、**

$$a^{p-1} \equiv 1 \pmod{p}$$

- **同じことだが、任意の** $a \in \mathbb{Z}$ **に対し、**

$$a^{p} \equiv a \pmod{p}$$

冪乗の高速計算

p, q：**相異なる大きな素数 (実際には** 1024 **bit 以上)**

$$N = pq,\ \ m = \mathrm{lcm}(p-1, q-1),\ \ ed \equiv 1 \pmod{m}$$

- **平文** M **の暗号化：** $C = E(M) \equiv M^e \pmod{N}$
- **暗号文** C **の復号：** $M = D(C) \equiv C^d \pmod{N}$

暗号化して復号すると元に戻ることは判った。

しかし、高速に計算できるのか？ (e, d **は巨大)**

$\longrightarrow$ **冪乗の高速計算法が必要**

RSA 暗号 (Rivest-Shamir-Adleman)

公開鍵 (N, e) から秘密鍵 d が計算できるか ？

- **N の素因数分解 $\mathrm{N} = \mathrm{pq}$ を知っていれば容易**
- **事実上 N の素因数分解と同程度の困難さ**

「困難さ」 $\cdots$ 計算時間が掛かる

RSA 暗号の安全性 $\Longleftrightarrow$ 素因数分解の困難さ

“計算量的安全性 (computational secrecy)”