現代における暗号への要請

現在の情報化社会では
様々な場面で暗号が使われている

例：インターネット取引 (ネットショッピングなど)

- **不特定多数の人と暗号通信をしたい**
- **事前に鍵を共有できない**

$\longrightarrow$ 共通鍵暗号では実現が困難

$\longrightarrow$ 公開鍵暗号・鍵共有方式のアイデア
(1976〜77)

公開鍵暗号

暗号化鍵 (公開鍵)・復号鍵 (秘密鍵) が別

- 事前の鍵共有の必要無し
  $\longrightarrow$ 見ず知らずの人からも送ってもらえる

- 認証・署名機能がある
  $\longrightarrow$ 改竄・なり済ましの対策
  $\longrightarrow$ 否認防止の機能も持つ

公開鍵暗号

但し、一般には、
暗号化・復号が共通鍵暗号に比べて低速

そこで、

- 始めに公開鍵暗号方式で鍵を送付・共有
- その鍵を用いて秘密鍵暗号方式で通信

というように、組合わせて用いることが多い

公開鍵暗号の特徴

- 暗号化は誰でも出来る
- 復号は秘密鍵を知らないと出来ない
  (もの凄く時間が掛かる)

そんな都合の良い仕組みが本当にあるのか ？

$\longrightarrow$ ある!! (多分大丈夫)

計算困難な問題 を利用 (素因数分解・離散対数問題)

代表的な公開鍵暗号方式

- **RSA 暗号 (Rivest-Shamir-Adleman)**
- **Diffie-Hellman 鍵共有**
- **ElGamal 暗号**

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、**

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