2. 公開鍵暗号

Def (素因数分解)

2つの素数 p, q に対して、その積 $n=pq$ が与えられたとき p, q を求める問題を素因数分解問題という。

2.1 RSA暗号

Def (公開鍵暗号)

公開鍵暗号は3つの関数 鍵生成, 暗号化, 復号の3つの関数から構成される。

鍵生成: セキュリティパラメータ (key のビット長) に対して 公開鍵と秘密鍵を出力する関数

暗号化: 平文 (plaintext) と公開鍵の入力に対して 暗号文 を出力する関数

復号: 暗号文と 秘密鍵 の入力に対して平文を出力する関数

RSA暗号

鍵生成 ① 2つの素数 p, q を生成する。 $n=pq$ とする。
(大きな)

② $\lambda(n) = \mathrm{LCM}(p-1, q-1)$ (最小公倍数)

$\lambda(n)$ と互いに素な整数 $1 \le e \le \lambda(n)$ を生成

③ 公開鍵 : n, e

秘密鍵 : d $\quad e \cdot d \equiv 1 \pmod{\lambda(n)}$

暗号化 : 平文 $m \in [0, n-1]$

① $c \equiv m^e \pmod n$ (注) m^e を n で割った余り

c が暗号文

復号 : 暗号文 $c \in [0, n-1]$

$c^d \equiv m^{ed} \equiv m \pmod n$

復号できる理由

- 位数 ℓ とは $\mathbb{Z}/n\mathbb{Z} \ni a$ で $a^\ell \equiv 1 \pmod n$ となる元である。
- $a^{\ell+1} \equiv a^\ell \cdot a \equiv a$ (平文)
- $U(\mathbb{Z}/n\mathbb{Z}) = \{\mathbb{Z}/n\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/n\mathbb{Z}\}$
  $= \{\mathbb{Z}/n\mathbb{Z} \ni a \mid \gcd(a, n) = 1\}$

$\#U(\mathbb{Z}/n\mathbb{Z}) = \varphi(n) = (p-1)(q-1) = \ell$

$\Rightarrow$ Lagrange の定理 : $U(\mathbb{Z}/n\mathbb{Z}) \ni \forall a \quad a^{\varphi(n)} \equiv 1$

$\Rightarrow a^{\lambda(n)} \equiv 1$ となる $\quad a^{\lambda(n)+1} \equiv a \pmod n$

つまり $e \cdot d \equiv 1 \pmod{\lambda(n)} \to ed = \lambda(n)k + 1$ ($k \in \mathbb{N}$)

$$C^d \equiv m^{ed} \equiv m^{\lambda(n)k+1} \equiv m^{\lambda(n)k} \cdot m \equiv m \pmod{n}$$

RSA暗号の性質

1. 確定的暗号
   同じ平文に対する暗号文は同一. (RSA暗号)

2. 確率的暗号
   同じ平文に対する暗号文が毎回確率的にかわる (ElGamal暗号)

3. 準同型性をもつ：関数により演算が保たれる.
   暗号関数：{平文} → {暗号文}

   Enc : $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

   $m \mapsto m^e \pmod{n}$

   $Enc(m_1) \cdot Enc(m_2) = m_1^e \cdot m_2^e = (m_1 \cdot m_2)^e = Enc(m_1 \cdot m_2)$

   暗号文の積　　平文の積

(Example)：同じ平文(m)の暗号文 $Enc(m)$

このとき，暗号文は異なるが同じ平文の暗号文を作るには？

$Enc(m) \neq Enc(m') \Rightarrow Dec(Enc(m)) = Dec(Enc(m'))$
を作るのに準同型性が使える

2.2 暗号の安全性

安全性 = 攻撃レベル × 解読レベル

攻撃レベル = 攻撃者が入手する情報，入手方法

弱 受動的攻撃　　RSA暗号 {n, e}

- 直接攻撃：公開情報のみ　　{n, e}
- 既知平文攻撃：平文の集合 $\{m_i\}$ に対し対応する暗号文 $\{C_i\}$ を利用
  但し平文 $\{m_i\}$ は えらべない　　$\{m_i, m_i^e\}$

注 公開鍵暗号の場合は誰でも暗号化可能より情報量は同じ

能動的攻撃　　Chosen Cipher Attack (CCA)

強
- 選択的暗号文攻撃：暗号文の集合 $\{C_i\}$ に対して，対応する平文 $\{C_i, C_i^d\}$ を利用 $\{C_i, C_i^d\}$

コツ

解読レベル　　　　RSA

(ア)・全面的攻撃 : ユーザの秘密鍵がわかる　d

・完全解読 : 任意の暗号文が解読できる　$^{\forall}C \to m$

(復号と等価なアルゴリズムが作れる)

(イ)・部分解読 : 暗号文から平文のある情報が…もれる

↓

識別不可能性 (indistinguishability, IND)

2つの平文 m_1, m_2 (大きさは同じ) に対して

どちらかの暗号文 $C^* = E(m_1)$ or $E(m_2)$ が

与えられたときに、どちらの暗号文かを識別する。

安全性 = 攻撃レベル × 解読レベル

攻撃レベル		解読レベル
・直接攻撃	×	全面的解読
・既知平文攻撃		完全解読
・CCA		部分解読

Def (IND-CCA)

適応的選択暗号文攻撃の下で識別不可能性をもつ暗号を IND-CCA 安全な暗号という。

2.3 整数の性質

(位数)・ $n = p \cdot q$　$\# U(\mathbb{Z}/n\mathbb{Z}) = \varphi(n) = (p-1)(q-1)$

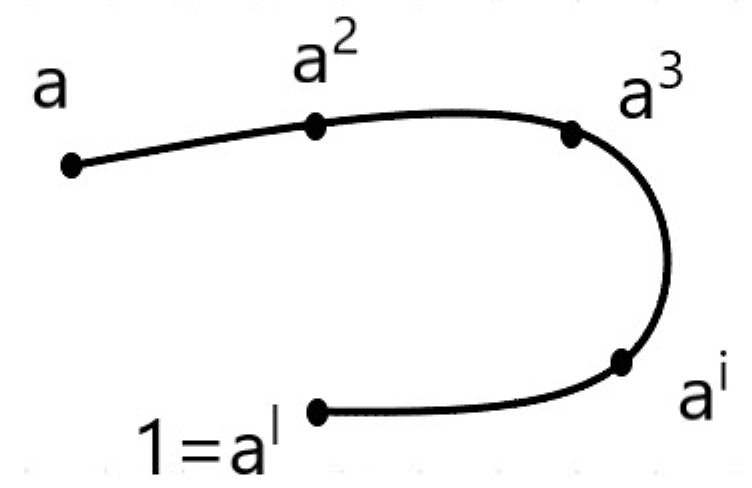
・ $n = p$ 素数

$\# U(\mathbb{Z}/p\mathbb{Z}) = \#\{\mathbb{Z}/p\mathbb{Z} \ni a \mid \gcd(a,p)=1\}$

$= p-1$

Lagrange: G: 有限群,　$|G| = l$ (元の個数)

このとき $G \ni {}^{\forall}a$ に対して $a^l = 1$



$U(\mathbb{Z}/p\mathbb{Z}) \ni {}^{\forall}x$　$x^{p-1} \equiv 1 \pmod p$

pは素数 ⇒ $^{\forall}x$ に対して $x^{p-1} \equiv 1 \pmod p$

対偶　pは素数でない ⇐ $^{\exists}x$ に対して $x^{p-1} \not\equiv 1$

逆　pは素数 ⇐ $^{\forall}x$ に対して $x^{p-1} \equiv 1 \pmod p$
とは限らない