RSA暗号

RSA暗号のしくみ

1. 計算するもの

- 2つのランダムな大きな素数p_1, p_2
- $n = p_1 p_2$
- $\phi(n) = \phi(p_1)\phi(p_2)$
- $\phi(n)$ と互いに素であるランダムな数pub
- $\phi(n)$ を法とするpub の逆元prv

2つの大きな素数$_{p_1, p_2}$

- ランダムに値を生成して, 素数なら採用する
- 素数の判定は,ミラー・ラビンテストによって可能
- 1回のテストに$O(\log p)$
- k回テストすると,$O(k \log p)$で素数である確率$\geq 1/4^k$

オイラー関数$\phi(n)$

- $\phi(n) :=$ 1以上$n-1$以下で,n と互いに素な数の個数
- $\phi(p) = p - 1$ (p: 素数)
- $\phi(n) = \phi(p_1p_2) = \phi(p_1)\phi(p_2) = (p_1 - 1)(p_2 - 1)$

$\phi(n)$と互いに素な数$_{pub}$

- ランダムに値pubを生成して,$\gcd(n, pub) = 1$なら採用する

$_{\phi(n)}$を法とする$_{pub}$の逆元$_{prv}$

- 拡張GCDを用いて, $x \cdot pub + y \cdot \phi(n) = 1$ なるx, yを計算
- $prv = (x \bmod \phi(n))$ とおくと, $prv \cdot pub \equiv 1 \pmod{\phi(n)}$

2. 暗号化・復号

- 平文m を,$m^{pub} \bmod n$ で暗号化
- 暗号化したものを, $(m^{pub})^{prv} \bmod n$ で復号
- 平文m は$m < n$ である必要がある
- ASCII(1文字8bit)を128文字送るには,$n \geq 2^{1024}$が必要
- もっと長い文を送りたいときは,128文字ごとにブロック化など

復号できるのか？

$$(m^{pub})^{prv} = m^{pub \cdot prv} = m^{1+q \cdot \phi(n)} = m(m^{\phi(n)})^q$$

(a) m と n が互いに素のとき

$m^{\phi(n)} \equiv 1 \bmod n$ より, $(m^{pub})^{prv} \equiv m \cdot 1^q = m \bmod n$

復号できるのか？

$$(m^{pub})^{prv} = m(m^{\phi(n)})^q = m((m^{p_2-1})^{p_1-1})^q$$

(b) m と n が互いに素でないとき

$m < n = p_1 p_2$ より,$\gcd(m,n) = p_1$として良い

- mはp_1の倍数より,$(m^{pub})^{prv} \equiv m \equiv 0 \bmod p_1$
- mはp_2と互いに素だから,$(m^{pub})^{prv} \equiv m(1^{p_1-1})^q \bmod p_2 = m$

よって$(m^{pub})^{prv} \equiv m \bmod n$

実装

bit.ly/2tk7E0T