

RSA 公開鍵暗号について

この公開鍵暗号方式は大きな数の素因数分解が非常に困難であるということを根拠としているものである。

ここでは A 君が B 君にメッセージを暗号文 m にして送ることを考える。このとき A 君は B 君が公開している鍵 (n, e) を用いてメッセージを暗号化する。鍵は公開している（公開鍵）ので誰でも暗号化できることになる。したがって A 君は暗号化できるわけである。しかし暗号化したものは B さんだけが持っている秘密鍵 d でしか復号化できない。

以下ではこの仕組みを簡単な例で理解しよう。

まず B 君の公開鍵 (n, e) を作る。

1. 公開鍵の 1 つの数 n の作り方

B 君は比較的大きな（100 桁程度の）異なる素数 p, q を 2 つ選び、その積 $n = pq$ を計算する。

ここでは簡単のため、 $p = 7, q = 11$ としよう。このとき $n = pq = 77$ となる。

2. メッセージ m の作り方

メッセージ m としては $m \in \{0, 1, 2, \dots, n-1\}$ を利用することができる。したがって今の場合は $m \in \{0, 1, 2, \dots, 76\}$ を利用することができる。

ここでは $m = 50$ としよう。

3. 公開鍵のもう 1 つの数 e の作り方

φ をオイラーの関数とする。このとき e は $\varphi(m) = \varphi(p)\varphi(q) = (p-1)(q-1)$ と互いに素となる自然数 e ($1 < e < (p-1)(q-1)$) を任意に選ぶとする。このことは最大公約数

$$\gcd(p-1, e) = \gcd(q-1, e) = 1$$

を満たすように e を決めると言ってもよい。

今の場合、 $\varphi(m) = (p-1)(q-1) = (7-1)(11-1) = 60$ と互いに素である自然数 e として $e = 47$ がとれる。

以上で準備は完成した。

メッセージは $m = 50$ 、公開鍵は $(n, e) = (77, 47)$ である。この公開鍵は暗号を作成するユーザーのコンピュータに入れておく。暗号を作成したい人は誰でも、公開された公開鍵を使って暗号を作成することができるのである。

（以上のまとめ）

p, q は異なる 2 つの素数とする。

公開鍵は $(n, e) = (pq, e)$ メッセージ m は $1 \leq m \leq pq-1$ なる自然数

4. 暗号化の仕方

A 君はメッセージ m を公開鍵 $(n, e) = (pq, e) = (77, 47)$ を用いて次のように m を暗号化して c を得る。

$$c = m^e \pmod{n} = m^e \pmod{pq}$$

したがって、今の場合

$$c = m^e = 50^{47} \equiv 8 \pmod{77}$$

5. 秘密鍵 d の定め方

復号化のためには、次に示すような秘密鍵 d が必要になる。 d は次のように求める。

d は e の $\text{mod } (p-1)(q-1)$ に関する乗法的逆元である。すなわち d は

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

となるものである。

求め方はユークリッドの互除法によればよい。これは行列の基本変形を用いて、次のように計算できる。

今の場合は、 $47d \equiv 1 \pmod{60}$ となる d を求めることになるので

$$\begin{aligned} \left(\begin{array}{ccc|ccc} 47 & 1 & 0 & & & \\ 60 & 0 & 1 & & & \end{array} \right) &\sim \left(\begin{array}{ccc|ccc} 47 & 1 & 0 & & & \\ 13 & -1 & 1 & & & \end{array} \right) &\sim \left(\begin{array}{ccc|ccc} 8 & 4 & -3 & & & \\ 13 & -1 & 1 & & & \end{array} \right) &\sim \left(\begin{array}{ccc|ccc} 8 & 4 & -3 & & & \\ 5 & -5 & 4 & & & \end{array} \right) &\sim \left(\begin{array}{ccc|ccc} 3 & 9 & -7 & & & \\ 5 & -5 & 4 & & & \end{array} \right) &\sim \\ \left(\begin{array}{ccc|ccc} 3 & 9 & -7 & & & \\ 2 & -14 & 11 & & & \end{array} \right) &\sim \left(\begin{array}{ccc|ccc} 1 & 23 & -18 & & & \\ 2 & -14 & 11 & & & \end{array} \right) &\sim \left(\begin{array}{ccc|ccc} 1 & 23 & -18 & & & \\ 0 & -60 & 47 & & & \end{array} \right) \end{aligned}$$

したがってこの変形より

$$\begin{pmatrix} 23 & -18 \\ -60 & 47 \end{pmatrix} \begin{pmatrix} 47 \\ 60 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

となるので1行目を比較して $23 \cdot 47 - 18 \cdot 60 = 1$ よって $23 \cdot 47 \equiv 1 \pmod{60}$ となるので、 $d = 23$ (秘密鍵) である。

(まとめ)

秘密鍵 d は e の $\text{mod } (p-1)(q-1)$ に関する乗法的逆元、すなわち

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

である。

次に、復号化の手順を説明する。

6. 復号化の仕方

暗号 c からメッセージ m を復号化するには、暗号 c を秘密鍵 d 乗したものの $\text{mod } n$ を計算すればよい。すなわち

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

が成り立つのである。この理由は次の通りである。

(証明) $ed \equiv 1 \pmod{(p-1)(q-1)}$ であるから、 $ed = 1 + k(p-1)(q-1)$ である。(k はある整数) したがって

$$c^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot m^{k(p-1)(q-1)} = m \cdot (m^{k(q-1)})^{p-1}$$

ここで $m \not\equiv 0 \pmod{p}$ ならばフェルマーの小定理より $(m^{k(q-1)})^{p-1} \equiv 1 \pmod{p}$

したがって $m^{ed} = m(m^{k(q-1)})^{p-1} \equiv m \pmod{p}$

$m \equiv 0 \pmod{p}$ ならば $m^{ed} \equiv 0 \pmod{p}$, $m \equiv 0 \pmod{p}$ だから $m^{ed} \equiv m \pmod{p}$

同様にして $m^{ed} \equiv m \pmod{q}$ が成り立つ。

よって $m^{ed} \equiv m \pmod{pq} \equiv m \pmod{n}$ が成り立つ。(証明終)

したがって B 君は $c = 8$ を受け取ると

$$c^d = 8^{23} \equiv 50 \pmod{77}$$

と復号化する。

p, q が小さいと e の逆元 d が自分自身 e になってしまうことが起こりうるので、大きな数の例を挙げる。計算は Maxima を用いた。参考までに計算式を挙げる。

(例) $p = 5717, q = 271$ とする。 $n = pq = 1549307$

$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = 1543320$

メッセージ m として、 $m = 10$ を選ぶ。 $e = 719$ とする。

公開鍵は $(n, e) = (1549307, 719)$ である。 m を暗号化すると、暗号 c は

$$c = m^e \pmod{n} \equiv 532488$$

となる。(Maxima では $\text{mod}(10^{719}, 1549307)$ とすればよい。)

秘密鍵 g を求める。これは e の $\text{mod}(p-1)(q-1)$ に関する乗法的逆元 d であったから、ユークリッドの互除法で求められて、 $d = 628919$ を得る。

暗号 c を復号化して、メッセージ m を得よう。

$$m = c^d \pmod{n} = 532488^{628919} \pmod{1549307} \equiv 10$$

となる。

最後に RSA 暗号の安全性について述べる。

上のことから $c \equiv m^e \pmod{pq}$ であったが、 e が大きいとき直接 c から m を決めるのには大量の計算が必要になる。だから c から m を知るのは困難である。

また、上のように復号化すればよいとわかって、 d が分からなければそれはできないのであるが、 d を求めるためには $p-1, q-1$ すなわち p, q が必要である。そのためには $n=pq$ を素因数分解しなければならない。これがまた非常に困難なのである。

現在は $n=pq$ として 300 桁くらいの数が使われる。