最強うだれぽ

c0¡gakuseki¿ 菅野路哉

2016 年 06 月 17 日

1 平文

自分の学籍番号を用いて平文を求める。

初めに、十分に大きい素数である p と q を自由に決定する。今回、p と q は 19, 31 を用いる。

次に、p と q を掛けた値を n とし、学籍番号 (¡gakuseki¿) を n - 2 で割った余りに 2 を足したものを平文とする。また、n は公開鍵の 1 つである。

$$
\begin{aligned}
p &= 19 \\
q &= 31 \\
n &= p \times q = 19 \times 31 =< n > \\
\text{平文} &= (115114 \bmod (n-2)) + 2 = (< gakuseki > \bmod < n >) + 2 =< m >
\end{aligned}
$$

n: ¡n¿

平文: ¡m¿

2 秘密鍵生成

p - 1 と q - 1 の最小公倍数を求める。求めた最小公倍数を λ(n) とする。導いた λ(n) を用いて公開鍵の 1 つである e を求める。e が 0 以上 λ(n) 未満かつ、λ(n) と e の最小公約数が 1 となるように e を定める。導いた λ(n) を用いて秘密鍵 d を求める。d を求める式を以下に示す。

$$
d = \frac{1}{e} \bmod \{\lambda(n)\}
$$

式を変形して、$(d \times e - 1) \bmod \lambda(n) = 0$ となるように d を決定する。

$$
\begin{aligned}
\lambda(n) &= LCM(p-1, q-1) \\
\lambda(n) &= 90
\end{aligned}
$$

3 暗号化

暗号文 c を求める。暗号文は $c = m^e \bmod n$ で求める。

公開鍵 e: ¡e¿, n: ¡n¿

平文 m: ¡m¿

m^e

<hsk>

$< me > \bmod n < hsd >$

暗号: ¡c¿

よって、暗号文¡c¿が導かれた。また、復号の確認も行う。復号は、$m = c^d \bmod n$ によって確認できる。

$<ruizyo>$ 復号: ¡hukugo¿

初めに求めた平文と同じ結果が得られたため、復号が正しく行われた。