2004 年 **10** 月 **5** 日

おまけ

素数を n 個用意する。
その素数を $p_1, p_2, p_3, \cdots\cdots\cdots\cdots, p_{(n-1)}, p_n$ とする。
$P = p_1 * p_2 * p_3 * \cdots\cdots\cdots\cdots\cdots * p_{(n-1)} * p_n$ とする。
$L = lcm(p_1 - 1, p_2 - 1, p_3 - 1, \cdots\cdots\cdots\cdots, p_{(n-1)} - 1, p_n - 1)$ とする。

Alice は $gcd(a, L) = 1$ を満たす a を選ぶ。
そして、 $a * A = 1 (mod\ L)$ を満たす A を計算する。
Bob も同様にして b , B を用意する。
(a, A) (b, B) は他人に知られないように秘密にする。

Alice は平文 M を Bob に伝えたい。
そこで、 $M^a\ mod\ P$ を Bob に送る。
Bob は送ってもらった暗号文を b 乗して Alice に渡す。
($(M^a)^b\ mod\ P$ を Alice に送る。)
Alice は今度は A 乗して Bob に返す。
($((M^a)^b)^A = (M^{aA})^b = M^b\ mod\ P$)
Bob は最後に B 乗してみる。すると・・・
($(M^b)^B = M^{bB} = M\ mod\ P$)
∴Bob は平文 M を盗聴者に知られることなく得ることができた。

執筆者 梅どぶろく ◆21Da3ggG3M

2004 年 **10** 月 **7** 日

竹暗号

Alice と Bob は P,L を知っていて、
それぞれ秘密の $(a, A)(b, B)$ をつくっている。
Alice が Bob にある平文 M を送りたいとする。
Bob に y^B を教えてもらう。(y は秘密)
(mod P は省略しています。)

Alice 側　　Bob 側

M に y^B を掛ける
↓
My^B
↓
a 乗する
↓
$(My^B)^a$ →→→→→→→→→→→→→→→→→→→→→→→→ $(M^a)(y^{aB})$
↓
b 乗する
↓
$(M^b\ y)^a$ ←←←←←←←←←←←←←←←←←←←←←←←← $M^{ab}\ y^a$
↓
A 乗する
↓
$M^b\ y$ →→→→→→→→→→→→→→→→→→→→→→→→ $M^b\ y$
↓
y^{-1} を掛ける
↓
M^b
↓
B 乗する
↓
M を得る

執筆者　梅どぶろく ◆21Da3ggG3M