ＲＳＡ暗号

ファルマーの小定理 pを素数，aをpと互いに素な数とすると，$a^{p-1} \equiv 1 \mod p$ が成り立つ．

（証明） $1 \cdot 2 \cdots (p-1) \equiv a \cdot 2a \cdots (p-1)a \equiv a^{p-1}\big(1 \cdot 2 \cdots (p-1)\big) \mod p$　よって，$a^{p-1} \equiv 1 \mod p$

RSA 暗号

ボブは，２つの素数 $p = 7, q = 19$を考え，$pq = 133,\ (p-1)(q-1) = 108$ を作ります．

次に，$(p-1)(q-1) = 108$と互いに素である素数$r = 5$を考えます．そしてアリスに

公開暗号鍵　$\boldsymbol{n = 133,\ r = 5}$

を示します．ボブとアリスは以下の表で文字を数字に変えることを約束しています．

a	b	c	d	e	f	g	h	i	j
1	2	3	4	5	6	7	8	9	0

アリスはボブに，fb というワードを暗号で送ります．fb を数で表すと 62 です．そして，

$$62^5 \equiv 120^2 \cdot 62 \equiv 36 \cdot 62 \equiv 104 \mod 133$$

と計算し，104を暗号文として，ボブに送ります．

ボブは解読作業として，$(p-1)(q-1) = 108, r = 5$から，方程式

$$\boldsymbol{5s \equiv 1 \mod 108}$$

を解いて，**解読鍵** $s = 65$を得ます．そして，解読鍵 $s = 65$から送られてきた暗号104の解読を$\mod 133$で行うと

$$x = 104^s = 104^{65} \equiv (104^2)^{32} \cdot 104 \equiv (43)^{32} \cdot 104 \equiv (120)^{16} \cdot 104 \equiv 36^8 \cdot 104$$
$$\equiv 99^4 \cdot 104 \equiv 92^2 \cdot 104 \equiv 85 \cdot 104 \equiv 62$$

つまり，$x = 62$よりアリスから送られたワードは fb であることがわかるのです．

（RSA 暗号解読の証明）aを送るべきワードとすると暗号は，$a^r \mod pq$である．

$rs \equiv 1 \ mod.(p-1)(q-1)$より，$rs = (p-1)(q-1)t + 1$と書ける．

したがって，フェルマーの小定理より，$(a^r)^s \equiv a^{(p-1)(q-1)t+1} \equiv 1^{(q-1)t} \cdot a \equiv a$である．

問題１．公開暗号鍵 $n = 77, r = 53$を見て，ボブはアリスから 15 という暗号を受け取った．

(1) 解読鍵sを求めよ．

(2) 15 を解読せよ．

問題２．ボブの公開暗号鍵は $n = 323, r = 281$で，ボブはアリスから 7 という暗号を受け取った．

(1) 解読鍵sを求めよ．

(2) 7 を解読せよ．