教育課題演習　第 14 回　RSA 暗号

フェルマーの小定理

p を素数とする。a が p の倍数でないとき，$a^{p-1}\equiv 1 \pmod{p}$

証明

2 項定理の展開式

$(a+b)^p=a^p+{}_pC_1a^{p-1}b+{}_pC_2a^{p-2}b^2+\cdots\cdots+{}_pC_{p-2}a^{p-2}b^2+{}_pC_{p-1}ab^{p-1}+b^p$

において，$a=b=1$ とおくと，

$2^p=1+{}_pC_1+{}_pC_2+\cdots\cdots+{}_pC_{p-2}+{}_pC_{p-1}+1$

${}_pC_k=\dfrac{p!}{k!(p-k)!}$ なので，

p が素数のとき，${}_pC_1, {}_pC_2$，…，${}_pC_{p-2}$，${}_pC_{p-1}$ は p の倍数。

∴　$2^p\equiv 2 \pmod{p}$

2 項定理の展開式で $a=2$，$b=1$ とおくと，

$3^p=2^p+{}_pC_1\cdot 2^{p-1}+2^{p-2}{}_p\cdot C_2+\cdots\cdots+2^2\cdot{}_pC_{p-2}+2\cdot{}_pC_{p-1}+1$

∴　$3^p\equiv 2+1=3 \pmod{p}$

以下同様に，$a=1, 2, 3, \cdots, p-1$ に対し

$a^p\equiv a \pmod{p}$

p は素数なので，$a=1, 2, 3, \cdots, p-1$ に対し，a と p は互いに素であり，

$a^{p-1}\equiv 1 \pmod{p}$　$(a=1, 2, 3, \cdots, p-1)$

合同式の性質

m, n が互いに素のとき，　$a\equiv b \pmod{m}$，$a\equiv b \pmod{n} \Leftrightarrow a\equiv b \pmod{mn}$

証明

次の性質を用いる。

$a\equiv b \pmod{m} \Leftrightarrow a-b$ は m の倍数

RSA 暗号による通信の原理

受信者は，公開鍵 k, m を公開する。

送信者は，平文(plain text)P に対し，$C=P^k \bmod m$ によって暗号文(cipher text) C を作成し，受信者に送る。ただし，$P<m$ とする。

受信者は，秘密鍵 u を用いて $C^u \bmod m$ を計算して，平文 P を得る。

公開鍵と秘密鍵の条件

（1）　$P^{ku}\equiv P \pmod{m}$　　（復号できること）

（2）　k, m から u を容易に推測できないこと。　　（暗号の安全性）

公開鍵と秘密鍵をどう作るか。

大きい素数 2 個 p, q を用意し，$m=pq$ とする。

$\phi(m)=(p-1)(q-1)$と互いに素な正の整数を選び，公開鍵 k とする。

$ku \equiv 1 \pmod{\phi(m)}$ となる正の整数 u を秘密鍵とする。

復号できる理由

概要　$P^{ku} \equiv P \pmod{p}$と $P^{ku} \equiv P \pmod{q}$を示して，$P^{ku} \equiv P \pmod{m}$を導く。

$ku=\phi(m)v+1$　(v は正の整数) とする。

$P^{ku} \equiv P \pmod{p}$となる理由（$P^{ku} \equiv P \pmod{q}$となる理由も同様)。

(i) P が p の倍数でもないとき，

フェルマーの小定理から，　$P^{p-1} \equiv 1 \pmod{p}$

両辺を$(q-1)v$ 乗し，さらに両辺に P を乗じると，

$ku=(p-1)(q-1)v+1$ より，　$P^{ku} \equiv P \pmod{p}$

(ii) P が p の倍数であるとき

$P^{ku} \equiv P \pmod{p}$が成立することは明らか。

$P^{ku} \equiv P \pmod{p}$と $P^{ku} \equiv P \pmod{q}$から $P^{ku}-P$ は p の倍数でも，q の倍数でもある。

p, q は異なる素数なので，$P^{ku}-P$ は $m=pq$ の倍数。すなわち，$P^{ku} \equiv P \pmod{m}$。

文章の数値化

インターネットでは，バイト（＝8 ビット）を単位として通信する。

英数字と, !%&".,?+*`{}()などの記号は, バイトの範囲で符号化できる (7 ビット ASCII)。

漢字やハングルなど各国固有の文字はユニコードで定義され，先頭バイトの 8 ビット目を 1 とする複数バイトで表される(UTF-8)。

平文の数値化

平文がバイト列 $abcde\cdots$で表されるとき，

$P=a+b\times256+c\times256^2+d\times256^3+e\times256^4+\cdots$

とする。

暗号の破り方と対策

１．受信した C と一致するまで，$P=1,2,3,4,\cdots$に対し $P^k \bmod m$ を計算する。

対策　P が小さい数のときは，公開鍵 k, m から簡単に解読されてしまうので，

短い文のときにはダミーを追加して長くする。

対策　通信のたびごとに異なる k, m を用いる。

２．m を素因数分解して p, q を求める。

$\phi(m)=(p-1)(q-1)$が分かれば秘密鍵 u は簡単に求まる。

対策　p,q を大きい素数に選ぶ。$\sqrt{m}$ に近い素数を避ける。