公開鍵暗号における暗号化・復号の計算について

ー大きな数の剰余演算をいかに行うかー

$$C = M^{e} \bmod n \qquad M = C^{d} \bmod n$$

n の桁数とRSA暗号の安全性
1990年代：512ビット（10進数155桁）
⇒ 現在：1024ビット（10進数309桁）

剰余演算の性質

$$(x \times y) \bmod p = ((x \bmod p) \times (y \bmod p)) \bmod p$$

練習問題

[a] $(27 \times 30) \bmod 25 = ?$　　[b] $(200^{100}) \bmod 15 = ?$

公開鍵暗号における暗号化・復号の計算

$$C = P^{E} \bmod M$$

$$= \underbrace{(\cdots((P \bmod M) \times (P \bmod M) \bmod M) \times \cdots)}_{\text{回の乗算}} \bmod M$$

$$C_1 = P \bmod M = P \quad (P < M)$$

$$C_n = (C_{n-1} \times P) \bmod M \quad (n = 2, 3, \cdots, E), \quad C_E = C$$

公開鍵暗号　暗号化・復号の計算（2進数展開）（1）

$$E=(a_k a_{k-1}\cdots a_1 a_0)_2 \quad a_i\in\{0,1\},i=0,1,\cdots,k$$

$$E=a_k\times 2^k+a_{k-1}\times 2^{k-1}+\cdots+a_1\times 2^1+a_0\times 2^0$$

$$=\sum_{i=0}^{k}a_i 2^i$$

$$P^E=P^{(a_k a_{k-1}\cdots a_1 a_0)_2}=P^{\sum_{i=0}^{k}a_i 2^i}$$

$$=P^{a_k 2^k}\times P^{a_{k-1}2^{k-1}}\times\cdots\times P^{a_1 2^1}\times P^{a_0 2^0}$$

公開鍵暗号　暗号化・復号の計算（2進数展開）（2）

$$P^E \bmod M=$$

$$(\cdots((P^{a_0 2^0}\bmod M)\times(P^{a_1 2^1}\bmod M)\bmod M)\cdots)\bmod M$$

$$P^{a_i 2^i}=\begin{cases}1 & a_i=0\ \text{のとき}\\ P^{2^i} & a_i=1\ \text{のとき}\end{cases}\quad(i=0,1,\cdots,k)$$

$$P^{a_i 2^i}\bmod M=\underbrace{(\cdots((P^2\bmod M)^2\bmod M)^2\bmod M\cdots)^2}_{i\text{回2乗する}}\bmod M$$

公開鍵暗号　暗号化・復号の計算（2進数展開）（3）

$P_i = P^{a_i 2^i}$ とおく（ただし，$a_i = 0$ のとき $P_i = 1$）

$a_i = 1$ のとき

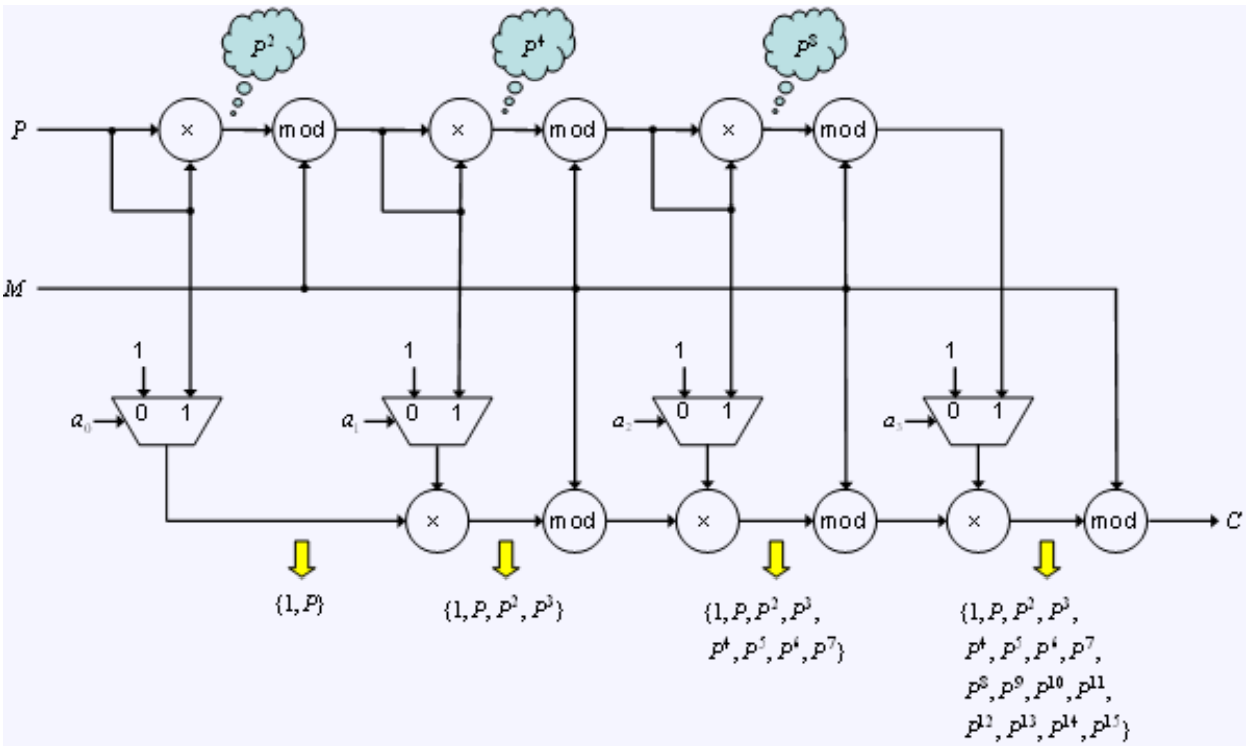
$$P_{i,1} = P^2 \bmod M$$

$$P_{i,n} = (P_{i,n-1})^2 \bmod M \quad (n = 2,3,\cdots,i)\ ,\ P_i = P_{i,i}$$

$$C_0 = P_0 \bmod M$$

$$C_n = (C_{n-1} \times P_n) \bmod M \quad (n = 2,3,\cdots,k)$$

$$C = C_k$$



暗号器・復号器のブロック図

$E = (a_3\, a_2\, a_1\, a_0)_2$（4ビット）の場合