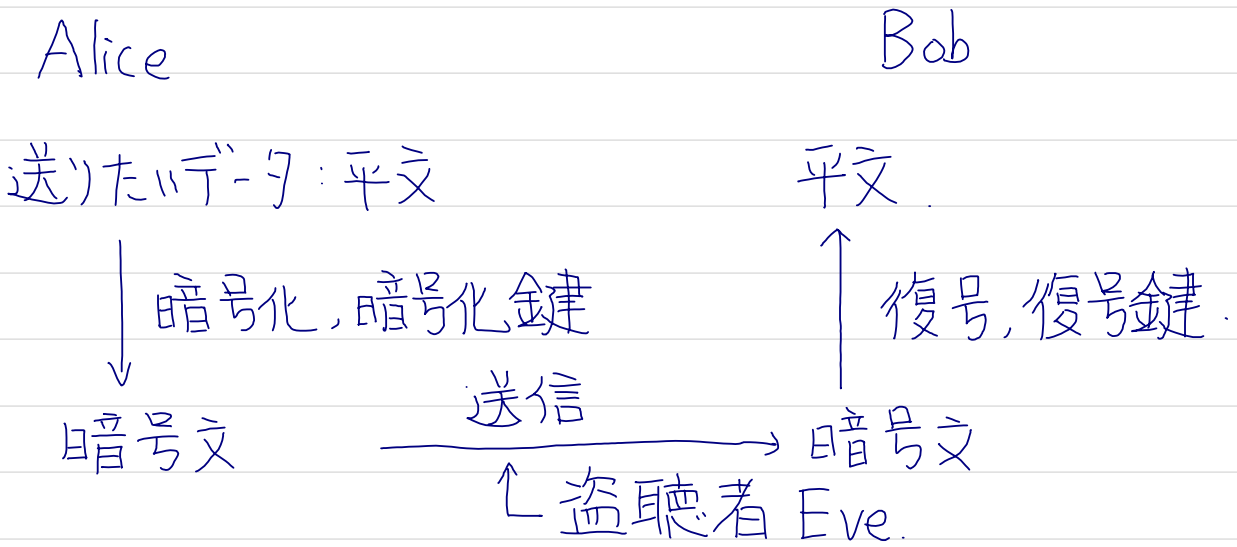
§5. 暗号



暗号化キーと復号キーが

一致している：対称暗号 → 秘密鍵暗号

一致していない：非対称暗号 → 公開鍵暗号

例 (1) アルファベットの文章に対し

暗号化キー：

a b c d e …	x y z	と2つずつずらす
↓ ↓ ↓	↓ ↓ ↓	
c d e f g …	z a b	

復号キー：もとにもどす

とすると，これは対称暗号

(2) ヒル暗号

アルファベットを $\{0,1,\cdots,25\}$ と同一視する.

M を $d\times d$ の (mod 26 での) 正則行列とする.

(0,…,25 を成分とする)

平文 p の長さは d の倍数とし, これを d 文字ずつに区切り暗号化する

今 p は長さ d とし. $p=p_1p_2\cdots p_d$ とし.

$p=\begin{bmatrix}p_1\\ \vdots\\ p_d\end{bmatrix}$ ともかくことにする. この暗号化を Mp とすると.

復号は $M^{-1}(Mp)$ によって行われる.

例えば $d=2$ $M=\begin{bmatrix}3&3\\2&5\end{bmatrix}$ とすると $M^{-1}=\begin{bmatrix}15&17\\20&9\end{bmatrix}$ であり,

平文: CODE = 2,14.3.4 は.

$$M\begin{bmatrix}2\\14\end{bmatrix}=\begin{bmatrix}3&3\\2&5\end{bmatrix}\begin{bmatrix}2\\14\end{bmatrix}=\begin{bmatrix}22\\22\end{bmatrix}=\begin{bmatrix}W\\W\end{bmatrix}$$

$$M\begin{bmatrix}3\\4\end{bmatrix}=\begin{bmatrix}3&3\\2&5\end{bmatrix}\begin{bmatrix}3\\4\end{bmatrix}=\begin{bmatrix}21\\0\end{bmatrix}=\begin{bmatrix}V\\A\end{bmatrix}$$

これを復号すると.

$M^{-1}\begin{bmatrix}22\\22\end{bmatrix}=\begin{bmatrix}2\\14\end{bmatrix}$　$M^{-1}\begin{bmatrix}21\\0\end{bmatrix}=\begin{bmatrix}3\\4\end{bmatrix}$　となる.

RSA暗号

鍵の生成

1. p,q を異なる素数, $n=pq$ とする
2. $\varphi(n)=(p-1)(q-1)$ と素な自然数 e をとる.
3. $ed\equiv 1 \pmod{\varphi(n)}$ をみたす d をとる.
4. n と e を公開, d,p,q は非公開.

暗号化

平文 x に対し $y\equiv x^e \pmod n$ を暗号文とする.

復号

$z\equiv y^d \pmod n$ とすると, $x=z$ となる.

定理5.1. このアルゴリズムで $z=x$ が成り立つ.

☺ $x \leq n$ とする.

$z \equiv y^d \equiv x^{ed}$ となるが. 命題4.14より

$z \equiv x^{ed} \equiv x$ である //.

注意5.2.

(1) 大きな素数をえる効力率のよいアルゴリズムがある.

(2) $\varphi(n)$ と素な整数 e は. $lcm(p-1, q-1)$ と素な数を選べばよい. なお. $gcd(a,b) \cdot lcm(a,b) = a \cdot b$ である.

(3) d は1次合同方程式の解.

(4) x^k は. $x^k = \begin{cases} (x^{\frac{k}{2}})^2 & k: 偶数 \\ (x^{\frac{k-1}{2}})^2 \cdot x & k: 奇数 \end{cases}$ となるので.

およそ $\log_2 k$ 回の計算で求められる.

(5) 復号キーは d であるが. n と e から d を求めるには

$\varphi(n)$ が必要 ∴ p と q が必要になる.

→ 因数分解の難しさが RSA 暗号の根拠

今だと $e^{c(\log n \cdot \log(\log n))^{\frac{1}{2}}}$ くらいかかる.

→ 100ケタ, 1ステップ 1μs で 数十億年.

例. $p=7$, $q=11$ とすると. $n=pq=77$.

$\varphi(n)=(p-1)(q-1)=60$ である. $e=7$ としてみる.

ここで $7d \equiv 1 \pmod{60}$ を求めると.

$60 = 7\times 8 + 4$

$7 = 4\times 1 + 3$ より

$4 = 3\times 1 + 1$

∴ $d \equiv -17 \equiv 43$

$1 = 4 - 3\times 1 = 4 - (7-4\times 1)$

$= -7 + 4\times 2 = -7 + 2(60 - 7\times 8)$

$= 2\times 60 - 17\times 7$.

さて $x=3$ とすると.

$y = 3^7 = 2187 \equiv 31 \pmod{77}$ より $y=31$

順号すると.

$31^{43} = 31 \cdot (31^{21})^2$

$31^{21} = 31 \cdot (31^{10})^2$

$31^{10} = (31^5)^2$

$31^5 = 31 \cdot (31^2)^2$ と計算して. $x = 31^{43} \equiv 3$ となる.