なぜ，セアラの暗号は公開鍵暗号にならないのか

2 行 2 列の行列について考える。

補題　行列 A が単位行列 E の実数倍でないとき，$\vec{p}$ と $A\vec{p}$ が一次独立となる $\vec{p}$ が存在する。

証明　$\vec{p}$ と $A\vec{p}$ が一次独立である $\vec{p}$ が存在しないと仮定すると，任意の $\vec{p}$ に対して

$$A\vec{p} = k\vec{p}$$

したがって

$$A\begin{pmatrix}1\\0\end{pmatrix} = k_1\begin{pmatrix}1\\0\end{pmatrix},\quad A\begin{pmatrix}0\\1\end{pmatrix} = k_2\begin{pmatrix}0\\1\end{pmatrix}$$

と表される。よって $s \neq 0, t \neq 0$ として

$$A\begin{pmatrix}s\\t\end{pmatrix} = sA\begin{pmatrix}1\\0\end{pmatrix} + tA\begin{pmatrix}0\\1\end{pmatrix} = sk_1\begin{pmatrix}1\\0\end{pmatrix} + tk_2\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}k_1 s\\k_2 t\end{pmatrix}$$

一方　$A\begin{pmatrix}s\\t\end{pmatrix} = k\begin{pmatrix}s\\t\end{pmatrix}$　であるから

$$\begin{pmatrix}k_1 s\\k_2 t\end{pmatrix} = \begin{pmatrix}ks\\kt\end{pmatrix}$$

$s \neq 0, t \neq 0$ であるから，この等式より $k_1 = k_2$ である。したがって

$$A\begin{pmatrix}1\\0\end{pmatrix} = k\begin{pmatrix}1\\0\end{pmatrix},\quad A\begin{pmatrix}0\\1\end{pmatrix} = k\begin{pmatrix}0\\1\end{pmatrix}$$

この 2 式を合わせて

$$A\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = k\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\quad \text{すなわち}\quad A = kE$$

これは A が単位行列 E の実数倍でないことに矛盾する。

ゆえに，$\vec{p}$ と $A\vec{p}$ が一次独立となる $\vec{p}$ が存在する。

証明終り

命題 1　行列 A と B が交換可能で，A が単位行列 E の実数倍でないとき，実数 s, t を用いて $B = sA + tE$ と表される。

証明　A は単位行列 E の実数倍でないから，$\vec{p}$ と $A\vec{p}$ が一次独立である $\vec{p}$ が存在する。

これより，実数 s, t を用いて

$$B\vec{p} = sA\vec{p} + t\vec{p}$$

とおける。したがって，

$$B\vec{p} = sA\vec{p} + tE\vec{p} = (sA + tE)\vec{p} \quad \cdots①$$

また，$BA = AB$ であるから，①を用いると

$$B(A\vec{p}) = A(B\vec{p}) = A(sA + tE)\vec{p} = (sA + tE)A\vec{p} \quad \cdots②$$

$\vec{p}$ と $A\vec{p}$ を合わせた行列 $(\vec{p}, A\vec{p})$ を考えると，①，②より

$$B(\vec{p}, A\vec{p}) = (sA + tE)(\vec{p}, A\vec{p})$$

$\vec{p}$ と $A\vec{p}$ は一次独立であるから，行列 $(\vec{p}, A\vec{p})$ は逆行列を持つ。したがって

$$B = sA + tE$$

証明終り

命題 2　A が単位行列 E の実数倍でないとき，$XAX^{-1} = YAY^{-1}$ が成り立つ必要十分条件は，実数 s, t を用いて $Y = (sA + tE)X$ と表されることである。

証明　$XAX^{-1} = YAY^{-1}$ が成り立つとすると

$$A = X^{-1}YAY^{-1}X$$

$$A = (X^{-1}Y)A(X^{-1}Y)^{-1}$$

$$(X^{-1}Y)A = A(X^{-1}Y)$$

したがって，命題 1 により

$$X^{-1}Y = sA + tE$$

ゆえに

$$Y = X(sA + tE)$$

逆は明らかに成り立つ。

証明終り

命題 2 により，A, B が与えられたとき，X の方程式 $B = XAX^{-1}$ の解の 1 つを X_0 とすると，解 X は

$$X = X_0(sA + tE)$$

と表される。

これにより，A, B が既知であっても，等式 $B = XAX^{-1}$ からだけでは X を求めることはできない。

セアラの暗号の脆弱性

$GL(2, Z_n)$ で考える。Z_n は n を法とする整数 Z の剰余類環であり，$GL(2, Z_n)$ は Z_n の元を成分とする 2 行 2 列の行列で，逆行列を持つものである。

セアラの暗号では，$B = X^{-1}A^{-1}X$　と　$R = X^r \quad (r \in N)$ を計算し，A, B, R を公開鍵，X, r を秘密鍵としている。ただし，X と A は可換でないものとする。

公開鍵から秘密鍵 X が求まるかを考える。

命題 2 により， $B = X^{-1}A^{-1}X$ の解の 1 つを X_0 とすると $X = (sA + tE)X_0$ も解であるから，

$B = X^{-1}A^{-1}X$ だけでは X は求まらない。また， $R = X^r$ だけでも X は求まらない。これにより，X は秘密鍵になるはずであった。

ところが，ケーリー・ハミルトンの定理により， $s, t \in Z_n$ を用いて

$$X^r = sX + tE$$

と表されるから

$$R = sX + tE$$

したがって， $u, v \in Z_n$ を用いて

$$X = uR + vE \quad \cdots①$$

と表される。

ここで， $B = X^{-1}A^{-1}X$ より， $XB = A^{-1}X$ であるから，これに①を代入して

$$(uR + vE)B = A^{-1}(uR + vE)$$

v が 0 と合同でないとき，両辺に v^{-1} を掛けて変形すると

$$(uv^{-1}R + E)B = A^{-1}(uv^{-1}R + E)$$

$$uv^{-1}(RB - A^{-1}R) = A^{-1} - B$$

この等式から uv^{-1} の値が求まるが，①を変形すると

$$X = v(uv^{-1}R + E)$$

となるから， X が定数倍を除いて定まる。

セアラの暗号は復号するのに X の定数倍は無関係であるから， X は秘密鍵とはならない。