行列を用いた ElGamal 暗号

k 次正方行列 A の累乗を用いた ElGamal 暗号について考える。

受信者の初期設定

$$B = A^m \quad (\text{m は乱数})$$

を計算する。

m が秘匿される。

A, B を公開する。

送信者の作業

$$C = A^n$$

$$D = B^n \quad (\text{n は乱数})$$

を計算する。

ここで

$$D = (A^m)^n = A^{mn}$$

である。

D を鍵として，共通鍵暗号でメッセージ M を暗号化して M' を得る。

C と M' を受信者に送信する。

D, n が秘匿される。

復号処理

Y と Z は交換可能であるから

$$C^m = (A^n)^m = A^{mn} = D$$

により，D を得る。

D を鍵として，M' を復号して M を得る。

有限体上の ElGamal 暗号と同等性

この暗号が，有限体上の ElGamal 暗号と同等であることを示す。

行列 A の固有多項式を $f(x)$ とすると，ケーリー・ハミルトンの定理により

$$f(A) = O \quad \cdots①$$

多項式 x^n を $f(x)$ で割った商を $Q(x)$，余りを $R(x)$ とすると

$$x^n = f(x)Q(x) + R(x) \quad \cdots②$$

x に A を代入すると，①により

$$A^n = f(A)Q(A) + R(A) = R(A) \quad \cdots③$$

したがって，②の $R(x)$ が求まれば，A^n は求まる。

ここで，最高次の係数が 1 の多項式 $g(x)$ で，$g(A) = 0$ となるもののうち，次数が最小なものを考える。(最小多項式)

$f(x)$ を $g(x)$ で割った商を $Q_1(x)$，余りを $R_1(x)$ とすると

$$f(x) = g(x)Q_1(x) + R_1(x)$$

よって

$$f(A)=g(A)Q_1(A)+R_1(A)$$

$f(A)=O, g(A)=O$ であるから $R_1(A)=O$

ここで，$R_1(x)$ の次数は $g(x)$ の次数より低く，$g(x)$ は $g(A)=O$ となる次数が最小な多項式（最小多項式）であったから，$R_1(x)=0$ である。したがって

$$f(x)=g(x)Q_1(x)$$

すなわち，$f(x)$ は $g(x)$ で割り切れる。

（これより，固有方程式 $f(x)$ が既約多項式のときは，$g(x)=f(x)$ となり，固有多項式が最小多項式となる。）

$g(x)$ の次数を p（p≦k）とすると，$g(A)=0$ より A^p は

$$A^p=s_{p-1}A^{p-1}+s_{p-2}A^{p-2}+\cdots+s_0E$$

と表される。

ここで，$A^{p-1}, A^{p-2},\cdots, E$ が一次従属あると仮定すると，$g(x)$ より次数の低い多項式 $h(x)$ で $h(A)=O$ となるものが存在することとなり，$g(x)$ が最小多項式であることに矛盾するから，$A^{p-1}, A^{p-2},\cdots, E$ は一次独立である。

x^n を $g(x)$ で割った商を $Q_2(x)$，余りを $R(x)$ とおくと

$$x^n=g(x)Q_2(x)+R_2(x)$$

よって

$$A^n=g(A)Q_2(A)+R_2(A)$$

$g(A)=O$ であるから，

$$A^n=R_2(A)$$

このとき，

$$R_2(A)=t_{p-1}A^{p-1}+t_{p-2}A^{p-2}+\cdots+t_0E \qquad (\text{p}\leqq\text{k})$$

と表され，$A^{p-1}, A^{p-2},\cdots, E$ は一次独立であるから，係数 $t_{p-1}, t_{p-2},\cdots, t_0$ はただ一通りに定まる。

よって，行列 $B=A^n$ と，x^n を $g(x)$ で割った余り $R_2(x)=t_{p-1}x^{p-1}+t_{p-2}x^{p-2}+\cdots+t_0$ が 1 対 1 に対応する。

このとき，B から $t_{p-1}, t_{p-2},\cdots, t_0$ も，$t_{p-1}, t_{p-2},\cdots, t_0$ から B も求められるから，B から $R_2(x)$ も，$R_2(x)$ から B も求められる。

すなわち，行列による ElGamal 暗号は有限体上の ElGamal 暗号と完全に同等である。

したがって，有限体のビット数を i とすると，有限体上の k 次の正方行列による暗号強度は，高々 k×i ビットしかない。

なお，A^n を求めるとき，A の固有多項式 $f(x)$ を求めて，x^n を $f(x)$ で割った余り $R(x)$ を求め，これより $R(A)$ を求めれば高速である。

行列による ElGamal 暗号の解読法

まとめると，次のようになる。なお，最小多項式を求めるアルゴリズムは，種々のものがある。

1　A の固有多項式 $f(x)$ を求める。

2 固有多項式 $f(x)$ を因数分解する。

3 A の最小多項式 $g(x)$ を求める。

4 $B = A^n$ を $A^{p-1}, A^{p-2}, \cdots, E$ の一次結合で表し，$B = t_{p-1}A^{p-1} + t_{p-2}A^{p-2} + \cdots + t_0E$ となる $t_{p-1}, t_{p-2}, \cdots, t_0$ の値を求める。

5 離散対数問題 $x^n = t_{p-1}x^{p-1} + t_{p-2}x^{p-2} + \cdots + t_0 \mod g(x)$ を解き，n の値を求める。