情報数理：暗号理論入門

高畑　弘

2006年4月14日

目 次

第1章　初等整数論のまとめ

1.1　ユークリッドの互助法と合同式

定義 1.1 2 つの整数 $a,\ b$ の正の公約数の最大値を $a,\ b$ の最大公約数といい、(a,b) で表す。$(a,b)=1$ のとき、a と b は互いに素であるという。

定理 1.1 2 つの整数 $a,\ b\ (a^2+b^2\neq 0)$ について、$(a,b)=d$ ならば $au+bv=d$ を満たす整数 $u,\ v$ が存在する。$b\neq 0$ ならば、u として $0\leqq u<|b|$ なるようなものを選ぶことができる。

定理 1.2 互いに素な 2 つの整数 $a,\ b$ について

$$ax\equiv 1 \pmod{b} \quad (0<x<|b|)$$

を満たす整数 x が存在し、ただ一つである。

系 1.1 p を素数とする。$p\nmid a$ ならば

$$ax\equiv 1 \pmod{p} \quad (0<x<p)$$

を満たす整数 x が存在し、ただ一つである。

定理 1.3 (中国人の剰余定理) r 個の正の整数 $p_1,p_2,\ldots,p_r$ は互いに素であるとする。また、r 個の整数 $a_1,a_2,\ldots,a_r$ は任意の $i\ (1\leqq i\leqq r)$ について $(a_i,p_i)=1$ であるとする。このとき、任意の整数の組 $b_1,b_2,\ldots,b_r$ に対して合同連立方程式

$$\begin{aligned}
a_1x &\equiv b_1 \pmod{p_1}\\
a_2x &\equiv b_2 \pmod{p_2}\\
&\vdots\\
a_rx &\equiv b_r \pmod{p_r}
\end{aligned}$$

は解をもち、その解は法 $M=p_1p_2\cdots p_r$ に関して一意である。

定義 1.2 正の自然数 n に対して、n 以下の正の自然数のうち、n と互いに素であるものの個数を $\varphi(n)$ で表し、この関数 $\varphi(n)$ をオイラー関数という。

定理 1.4 n の素因数分解を $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ とすると、

$$\begin{aligned}\varphi(n) &= (p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdots(p_k^{\alpha_k}-p_k^{\alpha_k-1}) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\end{aligned}$$

が成り立つ。とくに、n が素数の場合は $\varphi(n)=n-1$ であり、$\varphi(n^a)=n^a-n^{a-1}$ となる。

系 1.2 2 つの正の整数 $a,\ b$ が互いに素ならば $\varphi(ab)=\varphi(a)\varphi(b)$ である。

定理 1.5 正の自然数 n について

$$n=\sum_{d|n}\varphi(d)$$

が成り立つ。

証明　右辺を $f(n)$ で表す。まず、$(n,m)=1$ ならば $f(mn)=f(m)f(n)$ であることを示す。$d\mid mn$ ならば $d=d_1d_2$ $(d_1\mid m,\ d_2\mid n)$ と書ける。従って、系 1.2 を考慮して

$$\begin{aligned}f(mn) &= \sum_{d_1|m}\sum_{d_2|n}\varphi(d_1d_2) \\ &= \sum_{d_1|m}\sum_{d_2|n}\varphi(d_1)\varphi(d_2) \\ &= \left(\sum_{d_1|m}\varphi(d_1)\right)\left(\sum_{d_2|n}\varphi(d_2)\right) \\ &= f(m)f(n)\end{aligned}$$

ところで、素数 p に対して

$$\begin{aligned}f(p^k) &= \sum_{i=0}^{k}\varphi(p^i) \\ &= 1+\sum_{i=1}^{k}(p^i-p^{i-1}) \\ &= p^k\end{aligned}$$

であるから、自然数の素因数分解を考慮するならば、証明は終わる。　□

1.2　フェルマーの定理とオイラーの定理

定理 1.6 (フェルマーの定理) 正の整数 p を素数とする。整数 a が $p \nmid a$ であるとき

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ。

系 1.3 素数 p と任意の整数 a に対して

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

が成り立つ。

定理 1.7 (オイラーの定理) n を正の整数、a を n と互いに素である整数とする。このとき

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つ。

証明　$M = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$ を n 以下の n と互いに素である正の整数の集合とすると、あきらかに $M = \{\mathrm{Mod}(ar_1, n), \mathrm{Mod}(ar_2, n), \ldots, \mathrm{Mod}(ar_{\varphi(n)}, n)\}$ である。よって

$$a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$$

従って、$a^{\varphi(n)} \equiv 1 \pmod{n}$ を得る。　□

系 1.4 n を平方自由な（任意の素数の 2 以上のベキを因数としない）整数とする。d と e を正の整数とし、$de - 1$ は n のすべての素因数 p に対して、$p - 1$ の倍数であるとする（例えば、$de \equiv 1 \pmod{\varphi(n)}$ ）。このとき、任意の整数 a について、$a^{de} \equiv a \pmod{n}$ が成り立つ。

証明　証明すべきことは任意の n の素因数 p に対して $a^{de} \equiv a \pmod{p}$ であることである。素数 p を固定する。もし、$p \mid a$ ならば $a^{de} \equiv a \pmod{p}$ は明らかである。$p \nmid a$ とすると、$de - 1 = k(p-1)$ であるから、定理 1.6 より、$a^{de} = \{a^{p-1}\}^k a \equiv a \pmod{p}$ が得られる。よって、証明が終わる。　□

系 1.5 異なる二つの素数 $p,\ q$ について、$n = pq$ とおく。正の整数 $d,\ e$ について、$de \equiv 1 \pmod{\varphi(n)}$ ならば、任意の整数 a に対して $a^{de} \equiv a \pmod{n}$ が成り立つ。

1.3 有限体

大雑把に言って**体**とは四則演算が自由にできる代数系である。また**有限体**とは、元の個数が有限個である体である。そんなものがあるのか？という疑問がおきるだろう。これからその重要な例を説明していく。時間があまりないので、よっく聴いてくださいよ。$\mathbb{Z}$ 上の関係 $a \equiv b \bmod m$ は**同値関係**であるから、2 以上の整数 m について、この関係による $\mathbb{Z}$ の類別ができる．各類は m で割ったときの余りによって特徴付けられので、それらそれぞれの類を**法** m による**剰余類**と呼ぶ．この剰余類の集合を

$$\mathbb{Z}/m\mathbb{Z} \qquad \text{または} \qquad \mathbb{Z}_m$$

で表す．明らかに、$\mathbb{Z}_m$ の元の個数は m 個である．それぞれの類の代表元として $\{0, 1, 2, 3, \ldots, m-1\}$ がとれる．従って、$\mathbb{Z}_m$ を

$$\{[k] \mid 0 \leqq k \leqq m-1\}$$

と表すことができる．

さて、$\mathbb{Z}_m$ の元の間に加算、乗算を定義しよう．まず、加算はつぎのように定義する．

$$[k] + [j] \stackrel{\text{def}}{=} [\mathrm{Mod}(k+j, m)] \qquad (0 \leqq k, j \leqq m-1).$$

乗算はつぎのように定義する．

$$[k] \times [j] \ ([k][j]) \stackrel{\text{def}}{=} [\mathrm{Mod}(kj, m)] \qquad (0 \leqq k, j \leqq m-1).$$

加算に関して、簡略のためつぎのような記法を用いる

$$\overbrace{[k] + [k] + \cdots + [k]}^{n \text{ 個}} = n[k], \qquad [k] = 1 \cdot [k], \qquad 0[k] = [0]$$

同様に乗算に関してもつぎのような記法を用いる．

$$\overbrace{[k] \times [k] \times \cdots \times [k]}^{n \text{ 個}} = [k]^n, \qquad [k] = [k]^1, \qquad [k]^0 = [1].$$

最後の記法 $[k]^0 = [1]$ は $k > 0$ の場合について使用する．

定理 1.8 $\mathbb{Z}_m$ は上で定義した加算乗算に関して可換環 (commutative ring) をなす．すなわち

(1) 加算乗算に関して可換である

(2) 加算に関して群 (group) をなす

(3) 加算乗算に関して結合法則が成り立つ

(4) 分配法則が成り立つ

定理 1.9 $0 < k \leqq m-1$ である k について $[j][k] = [1]$ を満たす $0 < j \leqq m-1$ が存在するための必要充分条件は $(k, m) = 1$ である.

証明 （充分性） 定理 1.2 より、$1 \leqq j < m$ で $kj \equiv 1 \pmod{m}$ が存在する.
（必要性） $[j][k] = [1]$ を満たすということは、$jk + \ell m = 1$ を満たす $j,\ \ell$ が存在するということであるから、$(k, m) = 1$ となる. □

定義 1.3 $[1] \in \mathbb{Z}_m$ を**単位元**といい、少々紛らわしいが 1 で表す. また、$\alpha \in \mathbb{Z}_m$ に対して、$\beta\alpha = 1$ を満たす β を α の**（乗法に関する）逆元**といい、α^{-1} で表す.

定理 1.10 $\mathbb{Z}_m^* = \{[k] \mid 1 \leqq k < m,\ (k, m) = 1\}$ とおくとき、$\mathbb{Z}_m^*$ は乗算に関して群 (group) をなす.

証明 $(k, m) = (j, m) = 1$ とする。$\ell = \mathrm{Mod}(kj, m)$ とおき、$(\ell, m) = 1$ を示せばよい。$(\ell, m) = d > 1$ とする。このとき、$kj = tm + \ell = k'd$ となるので、$(k, m) = (j, m) = 1$ に矛盾する。 □

定義 1.4 一般に、可換群 G の元 a について $a^n = e$ (G の単位元) を満たす自然数が存在するとき、そのうち最小の n を a の位数 (order) という.

定理 1.11 可換群 G の元 a の位数を n とする。$a^r = e$ ならば $n \mid r$ である。

証明 $r = qn + i$ $(0 \leqq i < n)$ とすると、$a^n = e$ より、$a^i = e$ となるが、n が a の位数であることから、$i = 0$ でなければならない。 □

定理 1.12 可換群 G の二つの元 $a,\ b$ のそれぞれの位数 $m,\ n$ が互いに素ならば、ab の位数は mn である。

証明　ab の位数を d とすると、定理 1.11 より $d \mid mn$ である．$d < mn$ とする。このとき $mn = kd$ となる。$d = d_1 d_2$ $(d_1 \mid m,\ d_2 \mid n)$,　$k = k_1 k_2$ $(m = d_1 k_1,\ n = d_2 k_2)$ と書ける。まず、$d_2 = n$ であることを示す。

$$e = (ab)^{dk_1} = (ab)^{d_1 d_2 k_1} = \left(a^{d_1 k_1}\right)^{d_2} b^{d_1 d_2 k_1} = b^{d_1 d_2 k_1}$$

であるから、前定理 1.11 より、$n \mid d_1 d_2 k_1$ であるから $n \mid d_2$ となり、$n = d_2$ を得る。

次に、$d_1 = m$ であることを示す。

$$e = (ab)^{dk_2} = (ab)^{d_1 d_2 k_2} = a^{d_1 d_2 k_2} \left(b^{d_2 k_2}\right)^{d_1} = a^{d_1 d_2 k_2}$$

であるから、前定理 1.11 より、$m \mid d_1 d_2 k_2$ であるから $m \mid d_1$ となり、$m = d_1$ を得る。したがって、$d = mn$ となる。

定理 1.13 可換群 G の元の位数の最大値を M とする．任意の元の位数は M の約数である。

証明　$a \in G$ の位数を g とし、位数 M をもつ元を b とする。いま、$g \nmid M$ としよう。$K = \{g, M\}$ とおく。もちろん $K > M$ となる。

$$K = d_1 d_2, \quad d_1 \mid g,\ d_2 \mid M, \quad (d_1, d_2) = 1$$

を満たす $d_1,\ d_2$ が存在する。このとき、$h_1 = a^{g/d_1},\ h_2 = b^{M/d_2}$ とおくと、$h_1,\ h_2$ のそれぞれの位数は $d_1,\ d_2$ であり、仮定によって、$(d_1, d_2) = 1$ であるから、前定理 1.12 によって、$h_1 h_2 \in G$ の位数は $d_1 d_2 = \{g, M\} = K =$ に等しい。これは M が最大位数であることに矛盾する。　□

定義 1.5 p を素数とす。$\mathbb{Z}_p$ を F_p で、$\mathbb{Z}_p^*$ を F_p^* で表す。

定理 1.14 p を素数とすると、F_p は 0 以外の元はすべて逆元をもつ可換環つまり**可換体** (commutative field) である。F_p^* は $p-1$ 個の元からなる。F_p^* には $p-1$ のすべての約数それぞれを位数とする元が存在する。さらに位数 d の元は $\varphi(d)$ 個ある。（この定理以降は体といえば可換体を意味することにする）

証明　定理の前半は明らか。後半を証明する。フェルマーの定理 1.6 によって、任意の $a \in F_p^*$ に対して $a^{p-1} = 1$ であるから、定理 1.11 によって F_p^* の任意の元の位数は $p-1$ の約数である。$a \in F_p^*$ の位数を d とする．このとき、$A = \{a^j \mid 1 \leqq j \leqq d\}$

はすべて異なる．F_p^* の中で位数 d をもつのは $B = \{a^j \mid 1 \leqq j \leqq d,\ (j,d) = 1\}$ の $\varphi(d)$ 個のみである．なぜならば、位数 d を持つ元は方程式 $X^d - 1 = 0$ の解であるが

$$X^d - 1 = \prod_{i=1}^{d} (X - a^i)$$

であるから、位数 d の元の集合は A の部分集合である。しかし、a^j $(j,d) = k > 1$ については $j = kj_1$ と書けて、$\{a^j\}^{d/k} = \{a^d\}^{j_1} = 1$ となるので、位数は d/k 以下となる。一方、$(j,d) = 1$ とすると、$ju + dv = 1$ を満たす整数 u, v が存在する。a^j の位数を $d' < d$ と仮定してみよう。このとき、$a^{d'} = a^{d'(ju+dv)} = a^{d'ju} a^{d'dv} = (a^{jd'})^u (a^d)^{d'v} = 1$ となり、a の位数が d 未満になってしまい、矛盾である。上述のことから、$d \mid p-1$ なる d に対して次の二つの場合が可能である：

(a) 位数 d の元が存在し、その個数は $\varphi(d)$

(b) 位数 d の元は存在しない。

ところで、F_p^* の元はすべて位数をもつ。$d \mid p-1$ なる d に対して $A_d = \{$ 位数 d を持つ元の全体 $\}$ とすると、$A_d \cap A_{d'} = \phi$ iff $d \neq d'$ であり、

$$F_p^* = \bigcup_{d \mid p-1} A_d.$$

ところで、もし、d を位数とする元が存在するならば $\sharp(A_d) = \varphi(d)$ であり、定理 1.5 によって $p - 1 = \sharp(F_p^*) = \sum_{d \mid p-1} \varphi(d)$ であるから、すべての $d \mid p-1$ に対して $\sharp(A_d) = \varphi(d)$ でなければならない．すなわち、任意の $d \mid p-1$ に対して $A_d \neq \phi$．□

系 1.6 F_p^* には位数 $p-1$ の元が存在して、その個数は $\varphi(p-1)$ である。

定義 1.6 F_p^* の位数 $p-1$ の元を F_p^* の**原始元**という。

系 1.7 F_p^* の原始元を g とすると g^j がまた原始元であるための必要十分条件は $(j, p-1) = 1$ である。

定理 1.15 異なる素数 $p,\ q$ に対して $n = pq$ と置くとき、

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$$

が成り立つ。

証明　$\mathbb{Z}_n$ の各元 m に $\mathbb{Z}_p \times \mathbb{Z}_q$ の元 $(\mathrm{Mod}(m,p), \mathrm{Mod}(m,q))$ を対応させればよい。$\mathbb{Z}_p \times \mathbb{Z}_q$ における演算の定義は各成分ごとの演算である。この対応を $f(m)$ で表すとき、次の事柄を証明すればよい。詳細は演習問題とする。

1. f は $\mathbb{Z}_n$ からに $\mathbb{Z}_p \times \mathbb{Z}_q$ への全単射である。全射の証明には Chinese Remainder Theorem を用いる。
2. 写像 f が環 $\mathbb{Z}_n$ から環 $\mathbb{Z}_p \times \mathbb{Z}_q$ への準同型である。

□

定理 1.16 異なる素数 $p,\ q$ に対して $n = pq$ と置くとき、乗法群 $\mathbb{Z}_n^*$ の最大位数は $g = \mathrm{LCM}(p-1, q-1)$ に等しい。

証明　$\mathbb{Z}_p$ と $\mathbb{Z}_q$ のそれぞれの任意の元を $a,\ b$ とすると、$(a,b)^g = (1_p, 1_q)$ であることは明らかであるから、前定理によって、$\mathbb{Z}_n^*$ の最大位数 g' は g の約数である。$g' < g$ としよう。a_p, a_q をそれぞれ $\mathbb{Z}_p, \mathbb{Z}_q$ の原始元とする。g' の定義によって、

$$(a_p, a_q)^{g'} = (1_p, 1_q) = (a_p^{g'}, a_q^{g'})$$

が成立していなければならないのだが、$a_p,\ a_q$ の定義によって、$p-1 \mid g',\ q-1 \mid g'$ が成立している筈である。しかし、これは $g \leqq g'$ を意味するので矛盾になる。ゆえに $g' = g$ である。□

注意 1.1 これらの定理を複数個の異なる素数 $p_1, p_1, \ldots, p_k$ とその積 $n = p_1 p_2 \cdots p_k$ の場合に拡張するのは容易である。即ち、まず

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$$

である。また、乗法群 $\mathbb{Z}_n^*$ の最大位数は $g = \mathrm{LCM}(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$ に等しい。

1.4　演習問題

第2章　現代暗号の基礎

2.1　暗号入門

誰でも知っているように、暗号は、文を作成するのに利用する文字（日本語ならば漢字、ひらがな、カタカナ、英語ならば普通の意味でのアルファベット）または単語などをそれぞれ別の文字あるいは文字列に変更して、当事者以外の者にはその文の内容が理解できないようにする技術である。

一般に、通信に利用する文の構成要素の全体を**アルファベット**といい、Ω で表す。文はアルファベットの列である。コンピュータで処理しやすいように、Ω のそれぞれに自然数を対応させる関数 $f : \Omega \longrightarrow N$ を**符号化**という。各 $\omega \in \Omega$ に対する $f(\omega)$ を ω の符号という。もちろん、符号化関数 $f : \Omega \longrightarrow N$ は単射でなければならない。

例題 2.1 普通のアルファベット $\Omega_1 = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots, \mathrm{Z}\}$ を考える。文字は大文字のみ使用。空白、コンマ、ピリオド、疑問符、感嘆符などは用いないことにする。このとき、もっとも単純な符号化関数は $f_1(\mathrm{A}) = 0, f_1(\mathrm{B}) = 1, f_1(\mathrm{C}) = 2, f_1(\mathrm{D}) = 3, \ldots, f_1(\mathrm{Z}) = 25$ である。

例題 2.2 前例題のアルファベット Ω_1 を用いて、その n 個の直積として新しいアルファベット

$$\Omega_2 = \overbrace{\Omega_1 \times \Omega_1 \times \cdots \times \Omega_1}^{n\text{ 個}}$$

が定義される。これは Ω_1 の元の文字を n 個連ねた文字列の集合であり、$\sharp(\Omega_2) = 26^n$ である。このアルファベットに対する符号化関数はさまざまなものが考えられる。たとえば、体系的な符号化関数として次に述べるようなものがある。$\tilde{\omega} = \omega_1\omega_2\omega_3\cdots\omega_n$ にたいして符号化 $f_2(\tilde{\omega})$ をつぎのように定める

$$f_2(\tilde{\omega}) = f_1(\omega_1) + f_1(\omega_2)26 + f_1(\omega_3)26^2 + f_1(\omega_4)26^3 + \cdots + f_1(\omega_n)26^{n-1}$$

上に述べたことで、アルファベットおよびその符号化については理解されたであろう。今後、アルファベットとその符号化とは同じものと考える場合もある。

それでは、簡単な古典的暗号をいくつか紹介する。

例題 2.3 (シーザー暗号) アルファベットは Ω_1 で、符号化関数は f_1 とする。文 $P = a_1a_2\cdots a_m$ に対する暗号文 $C = b_1b_2\cdots b_m$ を次のように定義する。

$$b_i = a_i + 3 \bmod 26 \qquad (1 \leqq i \leqq m)$$

例題 2.4 (ヴィジュネール暗号) アルファベットは Ω_1 で、符号化関数は f_1 とする。ひとつの単語 $v = v_1v_2\cdots v_d$ を決める。文 $P = a_1a_2\cdots a_m$ を d 文字ごとのブロックに分けて、i 番目のブロックを $P_i = a_{i1}a_{i2}\cdots a_{id}$ とする。これについての暗号化 $C_i = b_{i1}b_{i2}\cdots b_{id}$ を

$$b_{ij} = a_{ij} + v_j \bmod 26 \qquad (1 \leqq j \leqq d)$$

によって定義し、平文 P の暗号文として、$C = C_1C_2\cdots$ を作ればよい。

例題 2.5 (アフィン変換暗号) アルファベットと符号化関数は前例題と同様とする。自然数 a を 26 未満で $(a, 26) = 1$ なるものとし、b は 26 未満の任意の自然数とする。このとき、各文字 $\omega \in \Omega_1$ に対する暗号化関数を

$$c = a\omega + b \bmod 26$$

で定義する。この暗号化関数が単射であることは仮定 $(a, 26) = 1$ から明らか。アフィン変換暗号をブロック暗号に拡張することは容易である。

例題 2.6 (転置暗号) 例題 2.4 のヴィジュネール暗号と同じように、文字の d 個づつのブロックを考え、それを列ベクトル $\boldsymbol{a}_i$ として考える。行列 K をつぎのようなものとする。(1) 要素は 0 かまたは 1 である。(2) 各列に 1 が存在して、一つだけである。(3) 各行に 1 が存在して、一つだけである。暗号化は

$$\boldsymbol{b}_i = K\boldsymbol{a}_i$$

によって行われる。

定義 2.1 アルファベット Ω の有限列の集合 $\mathcal{P}$, $\mathcal{C}$ と、或る暗号化機能（K をパラメタとする $\mathcal{P}$ から $\mathcal{C}$ への単射 f_K ）の組 $(f_K, \mathcal{P}, \mathcal{C})$ を K を暗号化鍵とする暗号システムという。$\mathcal{P}$ の元を平文、$f_K(\mathcal{P}) \subseteq \mathcal{C}$ の元を暗号文という。

また、各 $P \in \mathcal{P}$ に対して $f_K(P) \in \mathcal{C}$ を計算することを暗号化 (encryption) といい、暗号文 $f_K(P)$ から平文 P を復元することを復号化 (decryption) という。（ホントは復号でよいのですが、慣習に従います）

定義 2.2 K を暗号化鍵とする暗号システム $(f_K, \mathcal{P}, \mathcal{C})$ において、各平文 $P \in \mathcal{P}$ に対する暗号文 $f_K(P)$ から平文 P を復元する或る機能（D をパラメタとする $f_K(\mathcal{P})$ から $\mathcal{P}$ への単射 f_D ）が存在するとき、そのパラメタ D を復号化鍵という。これを数式で表すと次のようになる。

$$f_D(f_K(P)) = P \qquad P \in \mathcal{P}$$

以上の定義また以下の定義において、$K,\ D$ が与えられれば、$f_K(P),\ f_D(C)$ を計算することは、カンタンであることが暗黙のうちに了解されているものとする、ことを確認しておきたい。

定義 2.3 暗号化鍵 K と復号化鍵 D について、一方が分かれば他方がカンタンに（多項式時間で）求められるとき、その暗号システムは対称であるという。

上の例題 2.3〜 2.6 はすべて対称暗号システムである。対称暗号システムにおいては、暗号化鍵または復号化鍵のいずれかが第三者にしられてしまうと、その暗号システムが完全に知られることになり、盗聴や成り済ましが可能になる。したがって、暗号鍵および復号化鍵ともに秘匿されなければならない。このようなシステムでは、暗号を利用するグループの構成員が n 人いれば、$n(n-1)/2$ の異なる (K, D) が必要であり、それらはすべて秘匿されなければならない。これが対称暗号システムの最大の欠点である。この欠点を克服するのが、次節以降に解説される、非対称暗号システムまたは公開鍵暗号システムである。

2.2 RSA 暗号システム

この節で説明する **RSA 暗号システム**は Rivest, Shamir, Adleman の 3 名によって開発された暗号システムである。

以降、暗号システムの仕組みは周知のことと仮定する。

定義 2.4 暗号化鍵あるいは復号化鍵いずれか一方から他方を導くことが著しく困難である暗号システムを非対称暗号システムという。

以下に説明する RSA 暗号システムは、最初に実用化された非対称暗号システムである。非対称暗号システムはその特性によって、暗号化鍵を**公開**することができる。従って、非対称暗号システムは別名、**公開鍵暗号システム**とも呼ばれる。むしろ、この名称の方が一般的である。

まず、RSA 暗号システムの大雑把な内容を述べる。細かいが重要な諸注意は後ほど加えることにする。平文の集合 $\mathcal{P}$ は自然数のある集合とする。その最大値を N_P で表しておく。

暗号理論では情報をやりとりする人間として、アリス (Alice)、ボブ (Bob) 等の名前がよく使用されるので、この講義でもそれを踏襲することにする。

それでは、早速、アリスの暗号化鍵と復号化鍵を作るアルゴリズムを示す。

(A1) アリスは異なる 2 つの巨大な素数 $p_A,\ q_A$ を選ぶ。少なくとも 10 進法で 300 桁ぐらいで選ぶ。そして、$n_A = p_A q_A$ を計算する。

(A2) アリスは n_A に対するオイラー数 $\varphi(n_A) = (p_A - 1)(q_A - 1)$ を計算する。

(A3) アリスは $\varphi(n_A)$ 以下で、$(e_A, \varphi(n_A)) = 1$ となる自然数 e_A を探す。e_A はある程度大きい方がよい。

(A4) アリスは $\varphi(n_A)$ 以下で、$e_A d_A \equiv 1 \pmod{\varphi(n_A)}$ を満たす自然数 d_A を求める。(ユークリッドの互除法)

(A5) アリスは $p_A,\ q_A,\ \varphi(n_A),\ d_A$ を秘匿して、n_A と e_A のみを**公開する。**

この作業を、秘密の通信を行うグループの構成員すべてが行い、電話帳ならぬ暗号帳が出来上がる。そこにはアリスの $\{n_A, e_A\}$ が登載されている。

それでは、ボブがアリスに暗号を用いて通信を行うにはどうすればよいかを説明しよう。

(B1) ボブは暗号帳を開いて、アリスの公開鍵 $\{n_A, e_A\}$ をみつける。

(B2) ボブがアリスに送りたい平文を P とする。ボブは $C = P^{e_A} \bmod n_A$ を計算して、C をアリスへ送る。

暗号文 C を受信したアリスは

$$D = C^{d_A} \bmod n_A$$

を計算する。すると、定理 1.7 の系 1.4 によって、$D = P$ であるから、アリスはボブからの平文 P を入手したことになる。

さて、e_A と n_A から d_A を導くことが難しい理由を説明しよう。e_A から d_A を導くためには $\varphi(n_A)$ を知らなければならない。ところが $\varphi(n_A)$ を知ることと n_A の素因数分解 $p_A q_A$ を知ることとは同等なのである。なぜならば、$\varphi(n_A) = (p_A - 1)(q_A - 1) = p_A q_A - p_A - q_A + 1 = n_A + 1 - (p_A + q_A)$ であるから、$\varphi(n_A)$ がわかれば、$p_A + q_A$ がわかり、これと公開されている $n_A\ (= p_A q_A)$ から、2 次方程式の根の公式によって $p_A,\ q_A$ が分かってしまう。ところが、n_A の素因数分解 $p_A q_A$ は極めて困難であることが知られている。原理的には素因数分解は可能なのであるが、$p_A,\ q_A$ が 10 進

法で 300 桁ぐらいである場合は実際に n_A を、$p_A,\ q_A$ を知らずに素因数分解するには天文学的時間が必要なのである。

この暗号システムでは各構成員の数だけ暗号化鍵と復号化鍵の組 $\{e, d\}$ があればよい。ここが対称暗号システムと大きく異なるところである（前節の終わりの部分を参照のこと）

RSA 暗号の内容を小さな素数を用いて解説しよう。

例題 2.7 $p = 19,\ q = 31$ とすると、$n = pq = 589$ となる。$n = 589$ に対するオイラー数 $\varphi(n)$ は $eu = 540$ である。ここで、暗号化鍵として $e = 37$ とすると、$d = 73$ が $ed \equiv 1 \pmod{eu}$ となり、$d = 73$ が復号化鍵となる。これらがアリスの暗号のパラメタとして、アリスは $n = 589$ と暗号化鍵 $e = 37$ を公開する。ボブはアリスに文 $PL = 375$ を送るために、アリスの公開パラメタを使用する。まず、ボブは

$$CY = 375^e \bmod 589$$

を計算する。$CY = 451$ である。そして、暗号文 CY をアリスへおくる。暗号文 CY を受け取ったアリスは

$$451^d \bmod n = 375$$

を得ることになる。

注意 2.1 二つの素数 $p,\ q$ を選ぶとき、$|p - q|$ が小さいものを選んではいけないのである。

注意 2.2 二つの素数 $p,\ q$ を選ぶとき、一方の素数、例えば p 、について $p - 1$ が平方自由でその素因数がすべて小さいと $n = pq$ が因数分解されて、暗号が破られる恐れがある。

注意 2.3 ボブがアリスへ送る平文をコード化して得られる自然数は n_A より小さくなくてはいけない。

2.3 ディジタル署名

重要な文書に責任者が署名をすることは日常的なことである。この署名で重要なことは、署名がその文書上に行われ、その文書と切り離せないこと、もうひとつは、その署名が真実、その署名者本人によって行われたことを確認できることである。

最近、インターネットを利用した商取引が盛んに行われている。取引が行われる場合、署名は欠かせない。ネット通信での商取引において、物理的文書での署名と

同じ役割を担うのがディジタル署名である。ここではRSA暗号システムを用いてその原理を説明することにする。

Case1. アリス(A)が、アリスのフルネーム付きの平文 P をボブ(B)へ送るものとする。アリスは P のフルネームの部分 fn を復号化鍵 d_A を用いて暗号化する。そしてできる文書を P' とする。P' の中にはこれがアリスが作成した文書であることが明記されているものとする。次に

$$C = P'^{e_B} \bmod n_B$$

を計算し、これをボブへ送る。これを受信したボブは

$$D = C^{d_B} \bmod n_B$$

を計算すると、P' が得られる。ここには、判読不可能な部分 sig がある。この部分に対して、公開されているアリスの暗号パラメタ $\{e_A,\ n_A\}$ を用いて

$$sig^{e_A} \bmod n_A \quad = [fn^{d_A} \bmod n_A]^{e_A} \bmod n_A = fn$$

を計算すると、アリスのフルネームが得られることになる。これによって、ボブはこの文書がアリスから発信されたものであることを信じることができる。しかし、これには、問題がある。その問題点とは？

問題点は二つある。一つは、この署名方式では、アリスのフルネームの暗号化が知られて、ボブあるいは第三者によって悪用される可能性がある。この難点を避けるためには、フルネームだけではなく、年月日やその他の冗長文を含めて、暗号化することが必要である。もう一つの難点は、本文と署名部分が分離していることである。普通の署名は本文と切り離せないようになっているが、上のような署名方式では、本文と署名が分離可能であるから、署名の部分だけ、他の文書に利用される危険性がある。そのため、署名は隠されていなければならない。

Case 2 ボブはアリスへ、文書 P をディジタル署名付きで送りたいとする。ボブのRSA暗号システムの鍵パラメタを $K = (n, p, q, a, b) \quad ab \equiv 1 \pmod{\varphi(n)}$ とする。ボブは (n, a) を公開している。ボブは

$$sig_B(P) = P^b \bmod n$$

を計算して、アリスへ $(P, sig_B(P))$ をおくる。アリスはボブの公開パラメタ (n, a) を使って

$$P = \{sig_B(P)\}^a \bmod n$$

を確認する。

ここに、署名方式の形式的な定義を与える。

定義 2.5 署名方式 ($signature\ scheme$) は、以下の条件を満たす5つの組 ($\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V}$) から構成される。

1 $\mathcal{P}$ は可能性ある文書 ($message$) の有限集合

2 $\mathcal{A}$ は可能性ある署名 ($signature$) の有限集合

3 $\mathcal{K}$ は可能性ある鍵 (key) の有限集合

4 各 $K \in \mathcal{K}$ に対して、$sig_K \in \mathcal{S}$ となる署名アルゴリズム ($signature\ algorithm$) と、対応する確認アルゴリズム ($verification\ algorithm$) $ver_K \in \mathcal{V}$ が存在する。各 $sig_K : \mathcal{P} \to \mathcal{A}$ と $ver_K : \mathcal{P} \times \mathcal{A} \to \{\text{true}, \text{false}\}$ はすべての文書 $P \in \mathcal{P}$ とすべての署名 $Y \in \mathcal{A}$ に対して、つぎの等式を満たすような関数である。

$$ver(P, Y) = \begin{cases} \text{true} & \text{if } Y = sig(P) \\ \text{false} & \text{if } Y \neq sig(P) \end{cases}$$

このように、定義するとき、Case 2 の場合には

$$Y = sig_B(P)\ (= P^b \bmod n) \quad \Leftrightarrow \quad P = Y^a \bmod n$$

であることを証明しなければならない。($\Rightarrow$) はオイラーの定理の系 1.4 から明らか。($\Leftarrow$) も同様である。

2.4 エルガマル暗号システム

RSA 暗号システムは巨大整数の素因数分解の難しさにその基礎を置く。この節ではそれとは異なる整数に関する難しさに基礎を置く暗号システムを紹介する。

現在のところ、楕円曲線まで話しを広げなければ、いずれの対称暗号システムも、上記二つの整数論の計算困難さにその基礎を置いているといっても過言ではない。楕円曲線まで取り込んでも、原理的はこの節で述べるものと同じである。

§1.3 の系 1.6 で述べたように、素数 p に対して、乗法群 F_p^* には原始元（位数 $p-1$ の元）が存在する。

例題 2.8 $p = 17$ とすると F_{17}^* の原始元として、$3, 5, 6, 7$ など $\varphi(16) = 8$ 個がある。ここで、$g = 3$ として、$g^i \quad (1 \leqq i \leqq 16)$ を計算してみると、次のような結果が得られる。

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
g^i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

もちろん、原始元 g と i が与えられたとき、g^i を計算するのは g, i が巨大でもそんなに時間はかからない。ところが、p が巨大であるとき、原始元 g があたえられ、$1 < y < p$ を勝手にとり、

$$y = g^i$$

を満たす i を求めよとやられると、これは難しいのですよ。たとえば、

$$\begin{aligned} p &= 374628092193991 \\ g &= 465746509 \end{aligned}$$

としたとき、

$$g^i = 210141791579293$$

を満たす i を求めよ、とやられたら、皆さんはドーしますか？正解をだしましょう。

$$i = 46272790174016$$

デース。

定義 2.6 乗法群 F_p^* とその原始元 g が与えられたとき、$1 < y < p$ なる y に対して

$$y = g^i$$

を満たす i を求める問題を**離散対数問題**という。

p が巨大、たとえば、10 進法で 500 桁ぐらいになると、離散対数問題はとてつもなく難しいのである。もちろん、原理的には i を小さい順にとり、g^i を計算すれば、いつかは辿りつくのであるが、一体どなたがそれを確認するのか？　あるいは、そのときには、すでに地球は宇宙の藻屑となっているかも知れない。

したがって、しばらくは離散対数問題をとくことは**不可能**であると仮定して話しをしていく。

これらを前置きとして、エルガマル暗号システムを説明しよう。暗号で通信を行いたい独立した構成員の集団を Ω とする。Ω の中ではある巨大な素数 p と乗法群 F_p^* の原始元 g は共通なもので、構成員は p および g は知っているものとする。まず、各構成員 A は各自、ランダムな大きな自然数 a_A $(a_A < p-1)$ を選び

$$e_A = g^{a_A}$$

を計算し、e_A を公開する。a_A は秘匿する。A 以外の人は、e_A を知っても a_A を計算することはできない。断っておきますが、この「できない」は原理的にできない

のではなく、実際に、あるいは現実的に「できない」のです。今後、このことについては断りませんので、よろしく。さて、アリス (A) がボブ (B) へ第三者に分からないように平文 P を暗号で送りたいとする。アリスは次の手続きをとる。

(1)　乱数 k を選ぶ。この k は通信の度に異なるものを選ぶ。まず、g^k を計算する。次に、ボブの公開パラメタ e_B を探して、e_B^k を計算し、ついで、$Pe_B^k = Pg^{a_B k}$ を計算する。

(2)　アリスはボブへ組 $(g^k, Pg^{a_B k})$ を送る。

この組 $(g^k, Pg^{a_B k})$ を受け取ったボブは自分の秘匿パラメタ a_B を知っているので

$$\{g^k\}^{a_B} = g^{a_B k}$$

が計算できる。これから、$g^{a_B k}$ の逆数 $g^{-a_B k}$ が得られる。この逆数を $Pg^{a_B k}$ に乗じることにより、平文 P をボブは入手することになる。

今、第三者（オスカーと呼ばれる）がこの組 $(g^k, Pg^{a_B k})$ を手に入れたとする。オスカーはボブの公開パラメタ $e_B = g^{a_B}$ を知っているから、k を知ることによって、$g^{a_B k}$ を知ることができるのだが、g^k から k をしることは**不可能！**　従って、オスカーが手に入れることができるのは g^k と g^{a_B} だけである。ところが、つぎのような、ほとんど確実と噂されている予想があるのである。

Diffie-Hellman の予想　g^k と g^{a_B} から $g^{a_B k}$ を計算することは**不可能**である。

よって、オスカーは平文 P を手に入れることはできないのである。

例題 2.9 大きな素数を使うと訳がわからなくなる恐れがありますから、$p = 43$ とする。原始元として $g = 18$ をつかう。アリスがボブへ送りたい平文を $P = 37$ であるとする。アリスは乱数 k として、19 を選んだ。また、ボブの秘匿パラメタは $a_B = 25$ としよう。そうすると $e_B = g^{a_B} = 30$ となる。$g^k = 18^{19} = 28$ である。$g^{a_B k} = 30^{19} = 29$ であるから、$Pg^{a_B k} = 41$ 。従って、アリスはボブへ組 $(28, 41)$ を送ることになる。これを受け取ったボブは $\{g^k\}^{a_B} = 29$ をえる。これから、$g^{-a_B k} = 3$ を得る。$Pg^{a_B k} = 41$ にこの 3 を乗じると $P = 37$ が得られる筈である。$41 \times 3 = 37 = P$ 。得られましたね！

もう少し現実味のある数値の例をあげましょう。

例題 2.10 基礎になる素数と原始元をそれぞれ

$$p = 57390219840184391, \quad g = 5785576927204$$

とする。ボブの秘匿パラメタと公開パラメタをそれぞれ

$$a_B = 4758509309309, \quad g^{a_B} = 53174298763394825$$

とする。アリスが平文 $P = 67847753004982$ をボブへ送ろうとしている。そのために使う乱数を $k = 4839209303009409$ とした。アリスは k とボブの公開パラメタ g^{a_B} を用いて

$$g^k = 20471503608461237, \quad g^{a_B k} = 48354733724204630$$

を計算し、ついで

$$Pg^{a_B k} = 20959492184555032$$

を得て、アリスはボブへ組 $(g^k, Pg^{a_B k})$ を送る。ボブはこれを受け取り、早速自分の秘匿パラメタ a_B を用いて

$$\{g^k\}^{a_B} = g^{a_B k} = 48354733724204630, \quad g^{-a_B k} = 23183998621650890$$

を得る。この最後の値を $Pg^{a_B k}$ へ乗じて、元の平文 $P = 67847753004982$ がボブの手元に入るのである。

2.5 認証

これまでの社会においては、自分が自分であることを証明するには、運転免許証や署名または健康保険証などが使用されてきた。ATM などを利用するには、カードと暗証番号が要求される。暗証番号は別として、その他の証明手段は物理的なものであり、ネットワーク社会においては利用できない。

ネットワーク社会においてはディジタル信号による通信を媒介とする自己証明が不可欠である。ここでは、公開鍵暗号システムを利用しての**認証**（自己証明）についての初歩を話したい。

署名と認証とは良く似ている。署名は保存される必要があるが、認証は保存される必要はないことが多い。また、署名は文書全体になされる必要があるため、特殊な加工（ハッシュ関数の利用）が要求される一方、認証は概して短い文の処理で達成される。例題をもって具体的にお話ししましょう。

例題 2.11 (エルガマル暗号システムによる認証) アリス (A) がボブ (B) に対して、アリスであることを証明することを考える。アリスのフルネームを P で表す。いま、アリスとボブが利用しているエルガマル暗号システムの基礎になる素数を p とし、F_p^* の原始元を g とする。構成員 Y の秘匿、公開パラメタをそれぞれ $\alpha_Y,\ g_Y = g^{\alpha_Y}$ であらわすことにしよう。認証の手続きは次のようになる。

(1) アリスはボブの公開パラメタ g_B を探し、自分の秘匿パラメタ α_A を用いて、$e(A,B) = \{g_B\}^{\alpha_A}$ を計算する。

(2) ついで、アリスは $Pe(A,B)$ を計算して、ボブへ送る。

(3) $Pe(A,B)$ を受け取ったボブは、これがアリスから送られたものであることを確認するために、アリスの公開パラメタ g_A を探し、$e(A,B) = \{g_A\}^{\alpha_B}$ を計算する。

(4) さらに、ボブは $inv(A,B) = e(A,B)^{-1}$ を計算して、これを $Pe(A,B)$ に乗じて P を得る。これで、送り主がアリスであることを承認することになる。

例題 2.12 (RSA 暗号システムによる認証) 前例題と同じ認証の問題を RSA 暗号システムを利用して考えよう。構成員 Y の秘匿、公開パラメタともに、添字 Y で表すことにする。$n_A < n_B$ とする。

(1) アリスは自分の秘匿パラメタ d_A を用いて、$P_A = P^{d_A} \bmod n_A$ を計算する。

(2) ついで、アリスはボブの公開パラメタ $\{n_B, e_B\}$ をもちいて、$P(A,B) = (P_A)^{e_B} \bmod n_B$ を計算して、ボブへ送る。

(3) $P(A,B)$ を受け取ったボブは自分の秘匿パラメタ d_B を用いて、$P_A = P(A,B)^{d_B} \bmod n_B$ を計算する。

(4) ついで、ボブはアリスの公開パラメタ $\{n_A, e_A\}$ を用いて、$P = (P_A)^{e_A} \bmod n_A$ を得て、このメッセージがアリスから来たものであることを承認する。

例題 2.13 (エルガマル暗号システムによる認証の実例) アリスとボブが参加する暗号システムがエルガマル暗号システムであるとして、その基礎的パラメタ、およびアリス、ボブの秘匿パラメタを次のように定める。

$$
\begin{aligned}
p &= 476929193900483 \\
g &= 435707320960 \\
a_A &= 57832842920927 \\
a_B &= 24783703804721
\end{aligned}
$$

このとき、アリスおよびボブの公開パラメタは次のようになる。

$$\begin{aligned} g_A &= g^{a_A} = 193807912723584 \\ g_B &= g^{a_B} = 121037467259902 \end{aligned}$$

いま、アリスの自己証明の文を $P = 75022090201745$ とする。アリスはまずボブの公開パラメタ g_B を見て、自分の秘匿パラメタ a_A を用いて

$$e(A,B) = \{g_B\}^{a_A} = 265585636095466$$

を計算して、ついで $Pe(A,B) = 343821383397651$ をボブへ送る。ボブはこのデータ C がアリスから送られたものであることを確認するために、アリスの公開パラメタ g_A をとり、自分の秘匿パラメタを用いて

$$e(B,A) = e(A,B) = \{g_A\}^{a_B} = 265585636095466$$

を計算して、ついで $e(B,A)^{-1} = 395247222995204$ を得る。これをデータ C に乗じて

$$C \times e(B,A)^{-1} = 75022090201745 = P$$

を得て、送り手がアリスであることを確認する。

例題 2.14 (RSA 暗号システムによる認証の実例) アリスとボブの RSA 暗号システムのパラメタ $\{p, q, n = pq, \varphi(n), e, d, \}$ （$n,\ e$ のみを公開）をそれぞれ

$$\begin{aligned} \{p_A, q_A, n_A, \varphi(n_A), e_A, d_A\} &= \{373, 607, 226411, 225432, 35473, 37393\} \\ \{p_B, q_B, n_B, \varphi(n_B), e_B, d_B\} &= \{461, 947, 436567, 435160, 73059, 333659\} \end{aligned}$$

とする。アリスが自己証明の文 $P = 170573$ をボブに送って自分がアリスであることを証明することを考えよう。まず、アリスは自分の秘匿パラメタ d_A を用いて

$$P^{d_A} \bmod n_A = 220750\ (= C)$$

を計算し、ついで、ボブの公開パラメタ $\{n_B, e_B\}$ を用いて

$$C^{e_B} \bmod n_B = 153359\ (= AU)$$

を計算して、ボブへ送る。これを受け取ったボブは自分の秘匿パラメタ d_B を用いて

$$AU^{d_B} \bmod n_B = 220750 = C$$

を得て、ついで、アリスの公開パラメタ $\{n_A, e_A\}$ を用いて

$$C^{e_A} \bmod n_A = P^{d_A e_A} \bmod n_A = P$$

を得る。これによって、送り手がアリスであることを確認するのであるよ。

2.6 暗号鍵交換システム

一般に、公開暗号システムはセキュリティの強いシステムであるが、暗号化や復号化に時間が掛かるという欠点をもつ。処理の速さからすると、§2.1 で述べた古典的暗号システム（対称暗号システム）の方が優れる。従って、長い平文を暗号化するような場合には、認証や重要な部分は公開暗号システムを用いるが、さほど重要ではない部分は対称暗号システムを用いるといった、「日和見主義的」あるいは「ご都合主義的」な方法を用いるのである。いつも一貫性がベストとは限らないのだ。

さて、対称暗号システムを用いるとなると、鍵を交換しなければならない。アリスが用いた暗号化鍵をなんとかボブへ伝えなければならない。ドースルー？郵送するのはかったるい。電話で伝えたくとも、盗聴が怖い。ドースルー？

例えば、アリスがボブへ送る暗号文の一部にヴィジュネール暗号（参照　§2.1）を用いるとする。アリスが用いる暗号化鍵が”dictionary”とすると、これをボブへ伝えなければ、ボブはこの鍵を求めて頻度解析をおこなわなければならない。平文が短いとそれは不可能である。この暗号化された通信文がラブレターだったらボブにとって悲劇である。もっとも、ボブもアリスを愛しているならば、の話しではあるが …

代表的な鍵交換システムを例で説明しましょう。

例題 2.15 (Diffie-Hellman 鍵交換システム) アリスとボブが参加している離散対数を利用した暗号システムの基礎パラメタである素数 p と F_p^* の原始元をそれぞれ次のように定める。

$$\begin{aligned} p &= 5930204048231 \\ g &= 65998209817. \end{aligned}$$

アリスとボブの秘匿パラメタをそれぞれ次のように定める。

$$\begin{aligned} a_A &= 5720921092121 \\ a_B &= 4728182390175. \end{aligned}$$

このとき、アリスとボブの公開パラメタは次のようになる。

$$\begin{aligned} g_A &= g^{a_A} = 4571974152858 \\ g_B &= g^{a_B} = 2961999623964. \end{aligned}$$

アリスとボブは対称暗号のパラメタ $d(A,B)$ を次のようにするのである。

$$d(A,B) = g^{a_A a_B} = 3384471491518.$$

例えば、アリスがボブへ送る文のある部分がヴィジュネール暗号であり、その暗号の暗号化鍵を上の $d(A,B)$ であるとする。アルファベットとして普通の英字アルファベットとすると、$d(A,B)$ を 26 進法表現になおせばよいのだ。これはカンタンな計算で

$$d(A,B) = (16,5,9,25,4,17,6,11,0)_{26} = \mathrm{QFJZERGLA}$$

であることが分かる。このアリスとボブの共通鍵は、この二人にしか知られない鍵である。なぜなら、Diffie − Hellman の予想 によって、公開されている二人のパラメタ $g^{a_A},\ g^{a_B}$ から $g^{a_A a_B} = d(A,B)$ を求めることは**不可能**であるからである。

RSA 暗号システムを用いて同じような鍵の交換ができるだろうか？　考えてみよう。