暗号系に現れる群構造

荻野大助 (Daisuke OGINO)
山形大学大学院理工学研究科
澤田秀樹 (Hideki SAWADA)
山形大学理学部数理科学科

2001 年 11 月

はじめに

本論文では組立関数が全単射となる暗号系をとりあげ, その組立関数全体の集合 U が, 平文集合 $\mathcal{M}$ の全単射全体が作る群 $P(\mathcal{M})$ の部分集合として, 特にブロック暗号のときに持つべき群論的な特徴:

(i) U は多くの元を持ち, かつ, それぞれの位数も大きい。しかし

(ii) U は群構造を持たない, すなわち

$$UU \not\subset U$$

となり, さらに

(iii) 条件

$$UUU \not\subset U$$

も満足する。

について考察する ([6] 及び [12] の 12.3 章)。このような特徴を持つ部分集合は剰余類分解を使って構成できることがわかる。また暗号系の組立関数の持つ群論的性質を研究することはその暗号系をより深く理解する上で重要である。例えば [10] では RSA 暗号 ([9]) の組立関数が生成する $P(\mathcal{M})$ の部分群の構造が明らかにされている。

1 暗号系の定義

暗号系の形式的な定義を与えたい。暗号の一般論については [1], [2], [3], [7], [12] や [13] などを参照して欲しい。

定義 1.1 $\mathcal{M}$ と $\mathcal{C}$ を長さ有限な記号列よりなる有限集合とする。このとき次の 5 つの集合 $\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ の組を暗号系 (cryptosystem) とよび $\mathcal{S}$ で表す。すなわち

$$\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}),$$

(i) 平文 (plaintext) の集合, $\mathcal{M}$

(ii) 暗文 (ciphertext) の集合, $\mathcal{C}$

(iii) 鍵 (key) の集合, $\mathcal{K}$

(iv) 組立関数 (enciphering transformation) の集合, $\mathcal{E} = \{E_K \mid K \in \mathcal{K}\}$,

$$E_K : \mathcal{M} \longrightarrow \mathcal{C}, \text{ ただし } K \in \mathcal{K}$$

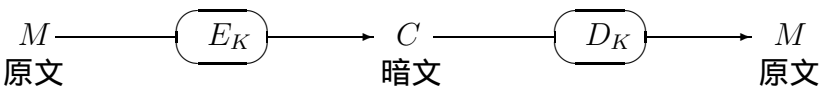
(v) 翻訳関数 (deciphering transformation) の集合 $\mathcal{D} = \{D_K \mid K \in \mathcal{K}\}$,

$$D_K : \mathcal{C} \longrightarrow \mathcal{M}, \text{ ただし } K \in \mathcal{K}$$

である。この 2 つの有限集合が互いに等しい数の元を含むときは, $\mathcal{M} = \mathcal{C}$ と仮定することが多い。 E_K $(K \in \mathcal{K})$ は $\mathcal{M}$ から $\mathcal{C}$ への写像, D_K は $\mathcal{C}$ から $\mathcal{M}$ への写像で,

$$D_K(E_K(M)) = M \ \ (\forall M \in \mathcal{M})$$

となっている。 このとき E_K は単射, D_K は全射となる。



上の定義において特に $|\mathcal{M}| = |\mathcal{C}|$ ならば E_K $(K \in \mathcal{K})$ は $\mathcal{M}$ から $\mathcal{C}$ への全単射となり, D_K はその逆写像となる。

定義 1.2 暗号系 $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ において $\mathcal{M} = \mathcal{C}$ であるとき集合 $\mathcal{M}$ の自分自身への全単射全体が作る群 $P(\mathcal{M})$ の部分群 G で $\mathcal{E}$ により生成されるもの, すなわち

$$G = \langle \mathcal{E} \rangle$$

を暗号系 $\mathcal{S}$ の群とよぶ。

この群 G は $\mathcal{M}$ に自然に作用している。

$$\begin{aligned} G \times \mathcal{M} &\longrightarrow \mathcal{M} \\ (g, m) &\longmapsto g(m) \end{aligned}$$

2　組立関数集合の群論的条件

暗号系 $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ において $\mathcal{M} = \mathcal{C}$ であるとき 集合 U は，非常に一般的ではあるが，「はじめに」で与えたような性質 (i), (ii), (iii) を持つことが望ましいとされている。そこでこの条件を若干強くした条件

$$UU \cap U = \emptyset \tag{1}$$
$$UUU \cap U = \emptyset \tag{2}$$

を満たす部分集合を群 G の中に構成する。$1 \notin U$ であるから G の部分群 H で $H \cap U = \emptyset$ となるものが存在する。この時

$$U \subset \bigcup_{g \notin H} gH$$

となることに注意しよう。

補題 2.1 G を群, H をその部分群とし自明でない両側剰余類を HgH $(g \notin H)$ とすれば

$$\begin{aligned}(gHgH) \cap gH &= \emptyset \\ (HgHg) \cap Hg &= \emptyset\end{aligned}$$

となる。

補題 2.2 G を群, H をその部分群とする。自明でない両側剰余類 HgH が条件 $gHg \cap H = \emptyset$ を満足するならば

$$\begin{aligned}(gHgHgH) \cap gH &= \emptyset \\ (HgHgHg) \cap Hg &= \emptyset\end{aligned}$$

となる。

定理 2.3 G を群, H をその部分群とする。

(i) G における H の自明でない左剰余類 gH において

$$(gHgH) \cap Hg^{-1} = \emptyset$$

となるならば, 集合 $U = gH \cup Hg^{-1}$ は条件 $U = U^{-1}$ かつ

$$(UU) \cap U = \emptyset$$

を満足する。

(ii) HgH を G における H の自明でない両側剰余類とする。このとき $gHg \cap H = \emptyset$ ならば, 集合 $V = gH$, $V' = Hg$ では以下の条件が成り立つ。

$$\begin{aligned}(VVV) \cap V &= \emptyset \\ (V'V'V') \cap V' &= \emptyset\end{aligned}$$

系 **2.4** G を群, N をその正規部分群とし, $\overline{G}$ を G の N による剰余群とする。このとき $\overline{G}$ の元 gN $(g \in G)$ に対して $\mathrm{ord}(gN) > 3$ ならば

(i) 集合 $U = gN \cup g^{-1}N$ は条件 $U = U^{-1}$ かつ

$$(UU) \cap U = \emptyset$$

を満足する。

(ii) 集合 $V = gN$ では条件

$$\underbrace{(VV \cdots V)}_{\mathrm{ord}(gN)} \cap V = \emptyset$$

が成り立つ。

以上で群論的条件 (1), (2) を満足する部分集合の構成法の一つが得られたことになる。

3 U の構成

対称群の中に条件

$$\begin{aligned}UU \cap U &= \emptyset \\ VVV \cap V &= \emptyset\end{aligned}$$

を満たす部分集合 U, V を構成するアルゴリズムを示す。以下の命題は良く知られている。

命題 **3.1** S_n $(n \neq 4)$ を次数 n の対称群とし，N を S_n の非自明な正規部分群とする。このとき

$$N = A_n$$

である。だだし，A_n は S_n の交代部分群である。

この命題より U を正規部分群から構成する場合は S_n の真部分群の中ですべきことがわかる。系 2.4 より

> S_n $(n \geq 5)$ は次数 n の対称群とし，H を S_n の非自明な部分群で商群
>
> $$\tilde{H} = N_{S_n}(H)/H$$
>
> が 3 以上の位数の元 gH $(g \in N_{S_n}(H))$ をもつとする。この時部分集合 $U = gH \cup g^{-1}H$ は条件：
>
> $$UU \cap U = \emptyset$$
>
> を満たし $V = gH$ は条件：
>
> $$VVV \cap V = \emptyset$$
>
> を満たす。

ことがわかる。

補題 3.2 S_n を次数 n $(n > 2)$ の対称群とし，$S_{\{1,\ldots,m\}}$ を $\{(1,2),(1,2,\ldots,m)\}$ $(1 < m < n)$ により生成される S_n の部分群とする。このとき

$$N_{S_n}(S_{\{1,\ldots,m\}}) = S_{\{1,\ldots,m\}} \times S_{\{m+1,\ldots,n\}}$$

である。だだし，$S_{\{m+1,\ldots,n\}}$ は $\{(m+1,m+2),(m+1,m+2,\ldots,n)\}$ により生成される S_n の部分群である。

上の補題から以下のようにして商群 $\tilde{H}$ を見つけることができる。

(i) $g = S_n$ は次数 $n \geq 5$ の対称群とする。

(ii) g の 2 つのランダムな元 h_1, h_2 をとる。

$$h_1 = (i_1, i_2, \ldots)(j_1, j_2, \ldots)\ldots$$
$$h_2 = (i'_1, i'_2, \ldots)(j'_1, j'_2, \ldots)\ldots$$

(iii) $\{1,2,\ldots,n\}$ から適当に自然数 $x_1, x_2, \ldots, x_l$ を選ぶ。

(iv) h_1 と h_2 の巡回置換から $x_1, \ldots, x_l$ を取り除く。例えば，$l = 2, x_1 = i_1 = i'_s$ であり，$x_2 = j_1 = j'_t$ であるとき，

$$
\begin{aligned}
h_1 &= (i_2, i_3, \ldots)(j_2, j_3, \ldots)\ldots \\
h_2 &= (i'_1, \ldots, i'_{s-1}, i'_{s+1}, \ldots)(j'_1, \ldots, j'_{t-1}, j'_{t+1}, \ldots)\ldots
\end{aligned}
$$

となる。ただし，h_1 と h_2 は $n-l$ 個のものの置換である。

$$h = Subgroup(g, [h_1, h_2])$$

とする。つまり，h は h_1 と h_2 により生成される g の部分群である。

(v) $n = Normalizer(g, h)$ とする。つまり，n は g における h の正規化群である。

(vi) $q = FactorGroup(n, h)$ とする。つまり，q は h による n の商群である。

4 GAP による実例 1

具体的に U や V を GAP4.2 (Groups, Algorithms and Programming 4.2, [5]) を用いて構成する。以下の計算はすべて CPU は Celeron850MHz, メモリは 384MB の LINUX PC で行なった。

はじめに $\{1, 2, \ldots, 16\}$ 上の対称群 g$(= S_{16})$ で計算する。その位数は 20922789888000 である。

対称群 g の二つの元 h1 と h2 によって生成される位数 239500800 の部分群を h とする。g における h の正規化群 n と h 上 n の商群 q を計算する。2 番目のランダムな元 n2 の自然な準同形，nat

$$
\begin{aligned}
\mathtt{nat}: \quad \mathtt{n} &\longrightarrow \mathtt{q}(= \mathtt{n/h}) \\
x &\longmapsto x\mathtt{h}
\end{aligned}
$$

による像の位数は 6 であるから，集合 $U = (\mathtt{n2})\mathtt{h} \cup (\mathtt{n2})^{-1}\mathtt{h}$ と $V = (\mathtt{n2})\mathtt{h}$ が構成できる。計算に要する時間は，920 $ms.$[1]である。

次に，$\{1, 2, \ldots, 32\}$ 上の対称群 g$(= S_{32})$ で計算する。

この n1 より集合 $U = (\mathtt{n1})\mathtt{h} \cup (\mathtt{n1})^{-1}\mathtt{h}$ と $V = (\mathtt{n1})\mathtt{h}$ が構成できる。計算に要する時間は，73640 $ms.$ である。

GAP による実例 1

[1] $ms.$ はミリセカンドである。

```
GAP4, Version: 4r2 fix8 of 7-June-2001, i686-pc-linux-gnu-gcc
gap> g:=SymmetricGroup(16);;
gap> h1:=Random(g);
( 1,16, 4, 8, 7)( 2,13,14,15, 3,11, 6, 9)
gap> h2:=Random(g);
( 1,14,12, 4, 7,10, 2,15, 5)( 3,13, 6,16, 9,11, 8)
gap> h1:=(1,7)(2,13,14,15,3,11,6,9);
( 1, 7)( 2,13,14,15, 3,11, 6, 9)
gap> h2:=(1,14,7,10,2,15,5)(3,13,6,9,11);
( 1,14, 7,10, 2,15, 5)( 3,13, 6, 9,11)
gap> h:=Subgroup(g,[h1,h2]);
Group([ ( 1, 7)( 2,13,14,15, 3,11, 6, 9),
  ( 1,14, 7,10, 2,15, 5)( 3,13, 6, 9,11) ])
gap> Size(h);
239500800
gap> n:=Normalizer(g,h);
<permutation group with 6 generators>
gap> Size(n);
11496038400
gap> q:=FactorGroup(n,h);
Group([ f1, f2, f3, f4, f5 ])
gap> nat:=NaturalHomomorphismByNormalSubgroup(n,h);;
gap> n1:=Random(n);
( 1, 7, 6)( 2,14, 9)( 3, 5,11,10,13,15)( 4,16)( 8,12)
gap> Image(nat,n1);
f1*f2*f3^2*f5
gap> Order(Image(nat,n1));
2
gap> n2:=Random(n);
( 2,11, 5,14,15, 7)( 3, 9,10,13, 6)( 4,16, 8)
gap> Image(nat,n2);
f1*f2*f5
gap> Order(Image(nat,n2));
6
gap> DisplayProfile();
  count  self/ms  chld/ms  function
             920           TOTAL
gap>

GAP4, Version: 4r2 fix8 of 7-June-2001, i686-pc-linux-gnu-gcc
gap> g:=SymmetricGroup(32);;
gap> h1:=Random(g);
( 1,31,13,11, 3,21, 2,25,18,10,12, 4,14,22,28,19,17,
 5, 6,15,29, 9,23,26,30,24,16, 8, 7)(20,32,27)
gap> h2:=Random(g);
( 1,25,16, 3,10,13,24,14,19,15,28,31,17,11, 2,20)
( 4, 5,26,29, 8,12, 9,22)( 6,30,32,21,23, 7)(18,27)
gap> h1:=(1,31,13,3,19,17,29,9,23);
```

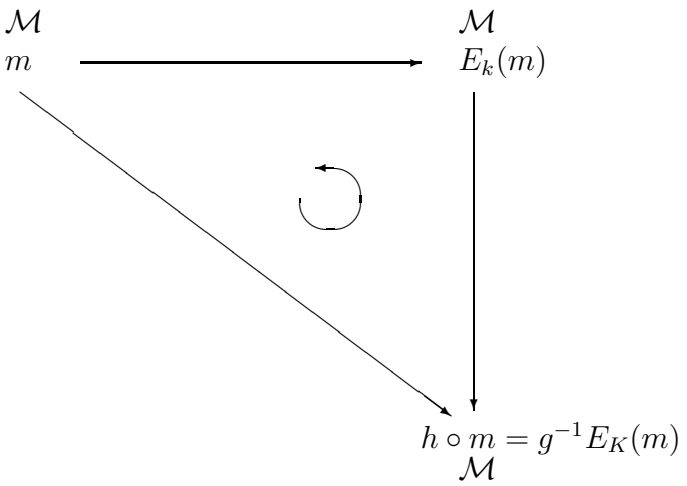
```
( 1,31,13, 3,19,17,29, 9,23)
gap> h2:=(1,3,13,19,31,17)(29,9);
( 1, 3,13,19,31,17)( 9,29)
gap> h:=Subgroup(g,[h1,h2]);
Group([ ( 1,31,13, 3,19,17,29, 9,23),
 ( 1, 3,13,19,31,17)( 9,29) ])
gap> Size(h);
181440
gap> n:=Normalizer(g,h);
<permutation group with 25 generators>
gap> Size(n);
9381179834206580323123200000
gap> q:=FactorGroup(n,h);
<permutation group with 25 generators>
gap> nat:=NaturalHomomorphismByNormalSubgroup(n,h);;
gap> n1:=Random(n);
( 1,23,19,31,29)( 2,20,10,28,32,16,14,24,26,25, 7, 8,
 30,21,18,11,22,15,27, 6)( 3, 9)( 4, 5,12)(13,17)
gap> Image(nat,n1);
( 3,16, 9,23,25,14,12,19,21,20, 7, 8,24,17,15,10,18,
 13,22, 6)( 4, 5,11)
gap> Order(Image(nat,n1));
60
gap> ProfileOperations(false);
  count  self/ms  chld/ms  function
           73640           TOTAL
gap>
```

5　ブロック暗号において可能な落し戸

この節では，ブロック暗号において群論的な落し戸が設定できることを説明したい。オスカーがブロック暗号 $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ においては，ある $g \in P(\mathcal{M})$ と部分群 $H(\subset P(\mathcal{M}))$ が存在して $\mathcal{E} = gH$ となることを知っていたら，このブロック暗号に落し戸を設定することができる。なぜなら

$$g^{-1}\mathcal{E} = H$$

が群構造をもち，任意の $E_K \in \mathcal{E}$ に対して $h = g^{-1}E_K$ が H に属しているからである。



この時ブロック暗号に Meet-in-the-Middle 既知平文攻撃 ([8]) を適用すれば以下のような H の元 h_1 と h_2 のペアを見つけることが可能である。

$$h = h_1 h_2 \text{ つまり } E_K = gh = gh_1 h_2$$

一般に，任意のブロック暗号 $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ に対して $P(\mathcal{M})$ の部分群 H をとれば，$P(\mathcal{M})$ は H の剰余類 $\{g_i H\}$ の和集合

$$\mathcal{E} \subset P(\mathcal{M}) = \bigcup_i g_i H$$

であるから、もし，オスカーが H の構造を知っていて，以下の条件を満たす剰余類の集合 $\{g_{i_t} H\}$ $(g_{i_t} \in P(\mathcal{M}))$ を得ていたなら，$\mathcal{S}$ に対して Meet-in-the-Middle 既知平文攻撃[2]を適用することができることになる。

$$\mathcal{E} \subset \bigcup_t g_{i_t} H$$

6 GAP による実例 2

$\mathcal{M}$ と $\mathcal{C}$ がビット列の長さ 4 の集合であるような暗号系 $\mathcal{S}$ を考える。$\mathcal{M}$ と $\mathcal{C}$ は 16 個の元からなるので，$\mathcal{M}$ の置換群 $P(\mathrm{M})$ は $S_{16}(= \mathrm{g})$ である。一般性を失わないように，以下のように仮定する。

[2] $E_K = g_{i_t} h$ であるとき集合 $\{g_{i_t}\}$ と H に注目して g_{i_t} と h を暗号文，平文の組から決定することもこの攻撃法の 1 つとみなしたい。

$$\mathcal{M} = \{1, 2, 3, \ldots, 16\}$$

ここで h の 2 つの元

$$x = (1, 2, 14, 11, 13, 15, 3, 5)(6, 7, 9, 10)$$
$$y = (1, 15, 14, 2, 13, 11)(3, 10, 9, 7, 6, 5)$$

をとり，x と y によって生成される h の部分群を h_sub とする。h_sub の位数は 259200 である。$\mathtt{h_sub} \subset \mathtt{h}$ であるから集合 $\mathcal{E} = (\mathtt{n2})\mathtt{h_sub}$ も以下の条件を満たす。

$$(\mathcal{E}\mathcal{E}) \cap \mathcal{E} = \emptyset \text{ と } (\mathcal{E}\mathcal{E}\mathcal{E}) \cap \mathcal{E} = \emptyset$$

h_sub のランダムな元 $\mathtt{z} = (1, 7, 3, 2, 13, 15, 6, 5, 9, 10)(11, 14)$ をとる。そして，暗号化関数 e を以下のように定義する。

$$\begin{aligned} \mathtt{e} &= \mathtt{n2} * \mathtt{z} \\ &= (1, 7, 13, 5, 11, 9)(2, 14, 6)(3, 10, 15)(4, 16, 8) \end{aligned}$$

与えられた平文が p=[1,2,3,4] であるなら，暗号文は以下のようになる。

$$\mathtt{c} = [1^{\mathtt{e}}, 2^{\mathtt{e}}, 3^{\mathtt{e}}, 4^{\mathtt{e}}] = [7, 14, 10, 16]$$

もし n2 と h_sub を知っていればこの暗号に meet-in-the-middle 既知平文攻撃を適用することができる。

この 723 個の候補から別の平文 $(\mathtt{p2} = [5, 6, 7])$，暗号文 $(\mathtt{c1} = [5^{\mathtt{e}}, 6^{\mathtt{e}}, 7^{\mathtt{e}}] = [11, 2, 13])$ を用いて鍵を絞り，鍵

$$\mathtt{z} = (1, 7, 3, 2, 13, 15, 6, 5, 9, 10)(11, 14)$$

を決定する。
計算に要する時間は，32470 $ms.$ であり，総計算時間は，33390 $ms.$ である。

次に，5 ビットの場合の暗号系を $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{E})$ とする。ただし，

$$\mathcal{E} = (\mathtt{n1})\mathtt{h_sub}$$

で h_sub は以下の様に構成する h の部分群である。

$\mathcal{M}$ と $\mathcal{C}$ は 32 の元からなるので，$\mathcal{M}$ の置換群 $P(\mathrm{M})$ は $S_{32}(= \mathtt{g})$ である。一般性を失わないように，以下のように仮定する。

$$\mathcal{M} = \{1, 2, 3, \ldots, 32\}$$

ここで

$$x = (1, 3, 9, 31, 29, 23, 19)$$
$$y = (1, 19, 17, 9, 3, 31, 29)$$

をとり，x と y によって生成される h の部分群を h_sub とする。h_sub の位数は 20160 である。h_sub $\subset$ h であるから集合 $\mathcal{E} =$ (n1)h_sub も以下の条件を満たす。

$$(\mathcal{E}\mathcal{E}) \cap \mathcal{E} = \emptyset \text{ と } (\mathcal{E}\mathcal{E}\mathcal{E}) \cap \mathcal{E} = \emptyset$$

h_sub のランダムな元 z $= (3, 17, 23, 19, 29, 31, 9)$ をとる。そして，暗号化関数 e を以下のように定義する。

$$\begin{aligned} \mathtt{e} &= \mathtt{n1} * \mathtt{z} \\ &= (1, 19, 9, 17, 13, 23, 29)(2, 20, 10, 28, 32, 16, 14, 24, 26, 25, \\ &\quad 7, 8, 30, 21, 18, 11, 22, 15, 27, 6)(4, 5, 12) \end{aligned}$$

与えられた平文が p=[1,2,3,4] であるなら，暗号文は以下のようになる。

$$\mathtt{c} = [1^{\mathtt{e}}, 2^{\mathtt{e}}, 3^{\mathtt{e}}, 4^{\mathtt{e}}] = [19, 20, 3, 5]$$

この 338 個の候補から別の平文 $(\mathtt{p2} = [9, 10, 11, 12, 13])$，暗号文 $(\mathtt{c1} := [9^{\mathtt{e}}, 10^{\mathtt{e}}, 11^{\mathtt{e}}, 12^{\mathtt{e}}, 13^{\mathtt{e}}] = [17, 28, 22, 4, 23])$ を用いて鍵を絞り，鍵

$$\mathtt{z} = (3, 17, 23, 19, 29, 31, 9)$$

を決定する。
計算に要する時間は，$2310\ ms.$ であり，総計算時間は，$75950\ ms.$ である。

GAP による実例 2

```
gap> x:=(1,2,14,11,13,15,3,5)(6,7,9,10);
( 1, 2,14,11,13,15, 3, 5)( 6, 7, 9,10)
gap> y:=(1,15,14,2,13,11)(3,10,9,7,6,5);
( 1,15,14, 2,13,11)( 3,10, 9, 7, 6, 5)
gap> h_sub:=Subgroup(h,[x,y]);
Group([ ( 1, 2,14,11,13,15, 3, 5)( 6, 7, 9,10),
  ( 1,15,14, 2,13,11)( 3,10, 9, 7, 6, 5) ])
gap> Size(h_sub);
259200
gap> z:=(1,7,3,2,13,15,6,5,9,10)(11,14);
( 1, 7, 3, 2,13,15, 6, 5, 9,10)(11,14)
```

```
gap> e:=n2*z;
( 1, 7,13, 5,11, 9)( 2,14, 6)( 3,10,15)( 4,16, 8)
gap> p:=[1,2,3,4];
[ 1, 2, 3, 4 ]
gap> c:=[1^e,2^e,3^e,4^e];
[ 7, 14, 10, 16 ]
gap> p1:=[1^n2,2^n2,3^n2,4^n2];
[ 1, 11, 9, 16 ]
gap> position:=[];v_1:=[];
[  ]
[  ]
gap> for i in [1..259200] do
> v:=Random(h_sub);
> if [1^v,11^v,9^v,16^v]=[7,14,10,16] then
> Add(position,i); Add(v_1,v);
> fi;
> od;
gap> Size(position); Size(v_1);
723
723
gap> c1:=[5^e,6^e,7^e];
[ 11, 2, 13 ]
gap> p2:=[5^n2,6^n2,7^n2];
[ 14, 3, 2 ]
gap> position:=[];v_2:=[];
[  ]
[  ]
gap> for i in [1..723] do
> v:=Random(v_1);
> if [14^v,3^v,2^v]=[11,2,13] then
> Add(position,i); Add(v_2,v);
> fi;
> od;
gap> Size(position); Size(v_2);
10
10
gap> DisplayProfile();
  count  self/ms  chld/ms  function

           32470           TOTAL
gap>

gap> x:=(1,3,9,31,29,23,19);
( 1, 3, 9,31,29,23,19)
gap> y:=(1,19,17,9,3,31,29);
( 1,19,17, 9, 3,31,29)
gap> h_sub:=Subgroup(h,[x,y]);
Group([ ( 1, 3, 9,31,29,23,19), ( 1,19,17, 9, 3,31,29) ])
```

```
gap> Size(h_sub);
20160
gap> z:=(3,17,23,19,29,31,9);
( 3,17,23,19,29,31, 9)
gap> e:=n1*z;
( 1,19, 9,17,13,23,29)( 2,20,10,28,32,16,14,24,26,25,
 7, 8,30,21,18,11,22,15,27, 6)( 4, 5,12)
gap> p:=[1,2,3,4];
[ 1, 2, 3, 4 ]
gap> c:=[1^e,2^e,3^e,4^e];
[ 19, 20, 3, 5 ]
gap> p1:=[1^n1,2^n1,3^n1,4^n1];
[ 23, 20, 9, 5 ]
gap> position:=[];v_1:=[];
[  ]
[  ]
gap> for i in [1..20160] do
> v:=Random(h_sub);
> if [23^v,20^v,9^v,5^v]=[19,20,3,5] then
> Add(position,i); Add(v_1,v);
> fi;
> od;
gap> Size(position); Size(v_1);
338
338
gap> c1:=[9^e,10^e,11^e,12^e,13^e];
[ 17, 28, 22, 4, 23 ]
gap> p2:=[9^n1,10^n1,11^n1,12^n1,13^n1];
[ 3, 28, 22, 4, 17 ]
gap> position:=[];v_2:=[];
[  ]
[  ]
gap> for i in [1..338] do
> v:=Random(v_1);
> if [3^v,28^v,22^v,4^v,17^v]=[17,28,22,4,23] then
> Add(position,i); Add(v_2,v);
> fi;
> od;
gap> Size(position); Size(v_2);
9
9
gap> DisplayProfile();
  count  self/ms  chld/ms  function

           2310           TOTAL
gap>
```

参考文献

[1] 池野信一, 小山謙二 「現代暗号理論 (第 5 版)」, 電子情報通信学会 1995

[2] 岡本龍明, 山本博資 「現代暗号」, 産業図書 1998

[3] 澤田秀樹 「暗号理論と代数学 (第 3 版)」, 海文堂 2000

[4] 澤田秀樹，荻野大助 「暗号系に現れる群構造」, パソコンリテラシ, vol.10, pp.29-31 2000

[5] The GAP Group, GAP -Groups, Algorithms and Programming 4.2. Aachen St Andrews, 2000.
(http://www-gap.dcs.st-and.ac.uk/gap)

[6] K.W.Campbell and M.J.Wierner, "DES is not a group", Advances in Cryptology-CRYPTO '92 Proceedings, Springer-Verlag (1992) pp.512-520.

[7] D.E.R.Denning, "Cryptography and data security", Addison-Wesley 1983

[8] B.S.Kaliski, Jr., R.L.Rivest, and A.T.Sherman, "Is the data encryption standard a group?", J. Cryptology, vol.1, pp.3-36, 1988.

[9] R.L.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol.21, No.2 (Feb. 1978) 120-126

[10] H.Sawada and T.Abe, "Groups and RSA cryptosystems", CRYPTOLOGIA, Vol.24, No.1 (2000) 34-40.

[11] H.Sawada, "On a Certain Algebraic Property of Block Ciphers", IEICE, Vol.E84-A, No.5 (2001) 1130-1134.

[12] B.Schneier, "Applied cryptography, 2nd edition", John Wiley & Sons, Inc. 1996

[13] D.R.Stinson, "Cryptography, theory and practice", CRC Press, Inc. 1995