The One-Round Functions of the DES Generate thc Alternating Group

Ralph Wernsdorf

SIT Gesellschaft für Systeme der Informationstechnik mbH
O-1252 Grünheide (Mark), Germany
Charlottenstraße 7

Abstract: In each of thc 16 DES rounds we have a permutation of 64-bit-blocks. According to the corresponding key-block there are 2^{48} possible permutations per round. In this paper we will prove that these permutations generate the alternating group. The main parts of the paper are the proof that the generated group is 3-transitive, and the application of a result from P. J. Cameron based on the classification of finite simple groups. A corollary concerning n-round functions generalizes the result.

1 Introduction

In each of the 16 DES-rounds a permutation of 64-bit-blocks is carried out /NBS 77/. According to the corresponding key-block there are 2^{48} possible permutations per round. In the following we will answer the question which group they generate.

A question like this is important from the cryptographic point of view. If the generated group is "too small" in a certain sense, then the algorithm might be vulnerable to cryptanalytic attacks (see for example /KRS 88/ and /RM 85/).

Several publications are concerned with group theoretic properties of the DES or DES-like ciphers:

- Coppersmith/Grossman in /CG 75/ and Even/Goldreich in /EG 83/ derived general results on "DES-like functions". The one-round permutations of DES form a subset of those functions. Further research in the direction of "DES-like permutations" is done by Pieprzyk/Zhang in /PZ 90/. The permutations defined there also generate the alternating group.

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 99-112, 1993.

- Reeds/Manferdelli in /RM 85/ and Chaum/Evertse in /CE 86/ exclude the existence of several classes of nontrivial linear factors.
- Group theoretic properties of the 16-round DES-cipher are subject of papers written by Kaliski/Rivest/Sherman /KRS 88/ and Simmons/Moore /SM 87/. The results support the hypothesis that the corresponding group is not "small".

The main result obtained in this paper is stated in Theorem 1. It will be proved that the 2^{48} one-round permutations generate the alternating group, i.e. that the generated group is "large". An essential part of the proof is done in Section 3. There the 3-transitivity of the group is derived from some computational results concerning properties of the S-boxes. In Section 4 we complete the proof of Theorem 1. For this purpose we apply some propositions of P. J. Cameron /Cam 81/ based on the classification of finite simple groups. Corollary 4 shows that the result also holds for n-round functions with independent subkeys.

2 Notations

$\forall\, (m, n) \in N^2 \;:\; \overline{m\,,n} := \{m, m+1, \dots, n\}$ for $m \le n$.

$\forall\, m \in N \;:\; V_m := \{0, 1\}^m$ (m-dimensional vector space over $\{0, 1\}$)

$\forall\, a \in V_{2m} \;:\; a_L := (a_1, a_2, \dots, a_m)$

$\forall\, a \in V_{2m} \;:\; a_R := (a_{m+1}, a_{m+2}, \dots, a_{2m})$ $\quad (a = (a_L, a_R))$.

$\langle\Pi\rangle$:= the permutation group generated by the set Π of permutations.

$A_{2^{64}}$:= the alternating group on V_{64}.

$S_{2^{64}}$:= the symmetric group on V_{64}.

We consider the set of functions F_k: $V_{32} \times V_{32} \to V_{32} \times V_{32}$:

$\forall\, k \in V_{48}\; \forall\, a \in V_{32}\; \forall\, b \in V_{32}$: $F_k(a, b) := (b, a \oplus S(k \oplus EPb))$,

where E: $V_{32} \to V_{48}$, P: $V_{32} \to V_{32}$ and S: $V_{48} \to V_{32}$ are defined according to /NBS 77/.

The functions F_k represent permutations on V_{64} and describe one round of the DES-algorithm, if we follow an equivalent description of the DES algorithm given in /DDF 84/ on page 183. (This modification does not influence the group theoretical properties considered here.)

The main object of our interest will be the group G:

$$G := \langle\{F_k \in S_{2^{64}} \mid k \in V_{48}\}\rangle.$$

Further we will use the following notations:

$$d \quad := (\underset{1}{0}, \underset{2}{0}, \underset{...}{...}, \underset{30}{0}, \underset{31}{1}, \underset{32}{0}, \underset{...}{...}, \underset{64}{0}) \in V_{64}$$

$$d' \quad := (\underset{1}{0}, \underset{2}{0}, \underset{...}{...}, \underset{21}{0}, \underset{22}{1}, \underset{23}{0}, \underset{...}{...}, \underset{48}{0}) \in V_{48}$$

$G_o \quad := \{g \in G \mid g(0) = 0\}$ - stabilizer of zero

$G_{o,d} \quad := \{g \in G \mid g(0) = 0 \wedge g(d) = d\}$ - stabilizer of zero and d

$M \quad := \{(k, k') \in V_{48}^2 \mid k \neq k' \wedge S(k) = S(k')\}$

$M_{d'} \quad := \{(k, k') \in V_{48}^2 \mid k \neq k' \wedge S(k) = S(k') \wedge S(k \oplus d') = S(k' \oplus d')\}$

$\forall\, (k, k') \in M \;\; \forall\, (a, b) \in V_{32}^2$:

$$F^L_{k,k'}(a, b) \quad := \quad F^{-1}_{k'}(F_k(a, b)) \; = \; (a \oplus S(k \oplus EPb) \oplus S(k' \oplus EPb), b);$$

$$F^R_{k,k'}(a, b) \quad := \quad F_{k'}(F^{-1}_k(a, b)) \; = \; (a, b \oplus S(k \oplus EPa) \oplus S(k' \oplus EPa)).$$

(Obviously we have: $\quad \forall\, (k, k') \in M: \quad (F^L_{k,k'} \in G_{o,d} \wedge F^R_{k,k'} \in G_o)$ and

$\forall\, (k, k') \in M_{d'}: \quad (F^L_{k,k'} \in G_{o,d} \wedge F^R_{k,k'} \in G_{o,d}).$)

3 The 3-Transitivity of the Group G

Two elementary properties of G are stated in Lemma 1:

Lemma 1:

a) $G \subseteq A_{2^{64}}$ /EG 83/.

b) G is transitive on V_{64}.

Lemma 2 shows the way we will pursue to prove the 3-transitivity of G. Its proof can be derived from theorem 9.1. in the book of H. Wielandt /Wie 64/.

Lemma 2:

If $G_{o,d}$ is transitive on $V_{64} \setminus \{0, d\}$ and G_o is transitive on $V_{64} \setminus \{0\}$, then G is 3-transitive on V_{64}.

To prepare the next steps we consider the following linear subspaces:

$\forall j \in \overline{1,8}\ \forall y \in V_6 \setminus \{0\}$:

$U^j(y) \quad := L\{S_j((k_i)_{i=6j-5}^{6j} \oplus y) \oplus S_j((k'_i)_{i=6j-5}^{6j} \oplus y) \mid (k, k') \in M\}$

$U^j_{d'}(y) \quad := L\{S_j((k_i)_{i=6j-5}^{6j} \oplus y) \oplus S_j((k'_i)_{i=6j-5}^{6j} \oplus y) \mid (k, k') \in M_{d'}\}$.

(L := linear subspace of V_4 spanned by the given subset of V_4; S_j: $V_6 \to V_4$ denotes the j-th S - box; $(k_i)_{i=6j-5}^{6j}$ denotes the vector $(k_{6j-5}, k_{6j-4}, \dots, k_{6j})$.)

The propositions (a) - (d) of Lemma 3 were obtained by a computer program:

Lemma 3:

(a) $\forall j \in \overline{1,8} \setminus \{4\}\ \forall y \in V_6 \setminus \{0\}$: $U^j(y) = U^j_{d'}(y) = V_4$.

(b) $\forall y \in V_6 \setminus \{(0, 0, 0, 0, 0, 0), (1, 0, 1, 1, 1, 1)\}$: $U^4(y) \neq \{(0, 0, 0, 0)\}$.

(c) $U^4((1, 1, 1, 1, 0, 1)) = U^4_{d'}((1, 1, 1, 1, 0, 1)) = V_4$.

(d) $\forall y \in V_6 \setminus \{(0, 0, 0, 0, 0, 0), (0, 0, 0, 1, 0, 0), (1, 0, 1, 0, 1, 1), (1, 0, 1, 1, 1, 1)\}$:

$U^4_{d'}(y) \neq \{(0, 0, 0, 0)\}$.

Notations:

- "~" denotes the following equivalence:

$$\forall (x, y) \in V_{64}^2\colon (x \sim y \longleftrightarrow \exists g \in G_{o,d}\colon g(x) = y).$$

- Further we denote

$$e := (\underset{1}{1}, \underset{2}{1}, \underset{\dots}{\dots}, \underset{9}{1}, \underset{10}{0}, \underset{11}{1}, \underset{\dots}{\dots}, \underset{32}{1}) \in V_{32}.$$

Lemma 4:

$$\forall\ (z, z') \in V_{32}^{2}: (e, z) \sim (e, z').$$

Proof:

The proof uses propositions (a) and (c) of Lemma 3.

Let $(z, z') \in V_{32}^{2}$ be arbitrarily fixed.

Property (a) of Lemma 3 includes the equality $U_{d'}^{1}$ $((1, 1, 1, 1, 1, 1)) = V_4$; hence the vector $(z_1 \oplus z'_1, z_2 \oplus z'_2, z_3 \oplus z'_3, z_4 \oplus z'_4)$ is a linear combination of vectors

$S_1((k_i^1)_{i=1}^6 \oplus (1, 1, 1, 1, 1, 1)) \oplus S_1((k_i^2)_{i=1}^6 \oplus (1, 1, 1, 1, 1, 1)),$

where $(k^1, k^2) \in M_{d'}, (k_i^1)_{i=1}^6 \neq (k_i^2)_{i=1}^6$.

For the corresponding (k^1, k^2) we set:

$\forall\ i \in \overline{7{,}48}:\ k_i^1 = k_i^2 = 0.$

By carrying out the corresponding permutations $F^{R}_{k^1 k^2}$ we finally obtain:

$(e, z) \sim (e, (z'_1, z'_2, z'_3, z'_4, z_5, z_6, \ldots, z_{32})).$

Analogous, from $U_{d'}^{2}$ $((1, 1, 1, 1, 1, 1)) = V_4$ (see (a)) we obtain:

$(e, (z'_1, z'_2, z'_3, z'_4, z_5, z_6, \ldots, z_{32})) \sim (e, (z'_1, z'_2, z'_3, z'_4, z'_5, z'_6, z'_7, z'_8, z_9, z_{10}, \ldots, z_{32})).$

The continuation of these considerations (where the equality $U_{d'}^{4}$ $((1, 1, 1, 1, 0, 1)) = V_4$ follows from (c) and not from (a)) finally yields the statement of Lemma 4.

■

Lemma 5:

$$\forall\ a \in V_{64} \setminus \{0, d\}\ \exists\ z \in V_{32}: a \sim (e, z).$$

Proof:

Let $a \in V_{64} \setminus \{0, d\}$ be arbitrarily fixed.

At first we show:

$$\exists\, a' \in V_{64} \setminus \{0, d\}\colon (a' \sim a \wedge \exists\, i \in \overline{1,32} \setminus \{2, 5, 10, 18, 26, 31\}\colon a'_i = 1). \qquad \textbf{(1)}$$

If $\exists\, i \in \overline{1,32} \setminus \{2, 5, 10, 18, 26, 31\}$: $a_i = 1$, then we immediately obtain (1) ($a' := a$).

If not:

- If we have $\exists\, i \in \overline{33,64}$: $a_i = 1$,

  then because of (a), (b), the properties $\forall\, (k^1, k^2) \in M$: $F^{L}_{k^1,k^2} \in G_{o,d}$ and

  $\forall\, b \in V_{32}$: $([EPb]_{17} = [EPb]_{19} \wedge [EPb]_{24} = [EPb]_{26})$ **(2)**

  there exists a pair $(k^1, k^2) \in M$ and

  an index $j \in \overline{1,32} \setminus \{2, 5, 10, 18, 26, 31\}$ such that $[F^{L}_{k^1,k^2}(a)]_j = 1$.

  We fix $a' := F^{L}_{k^1,k^2}(a)$.

- If we have $\forall\, i \in \overline{33,64}$: $a_i = 0$,

  then because of (2), (d) and $a \notin \{0, d\}$ we obtain:

  $$\exists\, j \in \overline{33,64}\ \exists\, (k^1, k^2) \in M_{d'}\colon [F^{R}_{k^1,k^2}(a)]_j = 1.$$

  Hence, this case is traced back to the case: $\exists\, i \in \overline{33,64}$: $a_i = 1$.

Therefore the proof of (1) is complete.

We fix a vector $a' \in V_{64} \setminus \{0, d\}$ according to (1).

As a next step we prove:

$$\exists\, a'' \in V_{64} \setminus \{0, d\}\colon (a'' \sim a' \wedge \forall\, i \in \overline{1,32} \setminus \overline{13,16}\colon a''_i = e_i). \qquad \textbf{(3)}$$

If $\forall\, i \in \overline{1,32} \setminus \overline{13,16}$: $a'_i = e_i$, then we immediately obtain (3).

If not, then we choose an index $j \in \overline{1,32} \setminus \{2, 5, 10, 18, 26, 31\}$ with $a'_j = 1$ according to (1).

Property (a) implies:

$$\exists\, a^0 \in V_{64} \setminus \{0, d\}: (a^0 \sim a' \wedge [a^0]_L = [a']_L \wedge \forall\, i \in I(j): [a^0]_{32+i} = 1), \quad (4)$$

where the sets $I(j)$ are defined in table 1.

We fix $a^0 \in V_{64} \setminus \{0, d\}$ according to (4).

Because of (a) we obtain:

$$\exists\, a^1 \in V_{64} \setminus \{0, d\}: (a^1 \sim a^0 \wedge [a^1]_R = [a^0]_R \wedge \forall\, i \in J(j): a^1_i = e_i),$$

where the sets $J(j)$ are defined according to table 2.

In the case of $j \in \{1, 6, 9, 14, 16, 17, 19, 21, 22, 25, 29, 32\}$ property (3) holds with $a'' := a^1$. In the other case, (3) follows by carrying out the same procedure for a^1. At this we can take an index $j \in \overline{1,32} \setminus \{2, 5, 10, 18, 26, 31\}$ with $a^1_j = 1$ and the property $j \in \{1, 6, 9, 14, 16, 17, 19, 21, 22, 25, 29, 32\}$.

That is possible because of:

$$\forall\, j \in \overline{1,8}: \overline{4j\text{-}3, 4j} \cap \{1, 6, 9, 14, 16, 17, 19, 21, 22, 25, 29, 32\} \neq \varnothing.$$

This completes the proof of (3).

We fix $a'' \in V_{64} \setminus \{0, d\}$ according to (3). Then we can prove:

$$\exists\, z \in V_{32}: a'' \sim (e, z). \quad (5)$$

We have: $\forall\, i \in \overline{1,32} \setminus \overline{13,16}: a''_i = e_i$.

From this besides (a) and $\overline{13,16} \cap \{2, 5, 10, 18, 26, 31\} = \varnothing$ we get: $\exists\, z \in V_{32}: (a'' \sim ([a'']_L, z) \wedge z_{10} = 0 \wedge z_2 = z_5 = z_{18} = z_{26} = z_{31} = 1)$. We fix such a vector $z \in V_{32}$. Because of (c) the equivalence $([a'']_L, z) \sim (e, z)$ holds.

Therefore the proof of (5) is complete.

Considering the chain $a \sim a' \sim a'' \sim (e, z)$ we obtain the proposition of Lemma 5 from (1), (3) and (5).

j	$I(j)$
16 or 25	$\overline{1,4} \cup \overline{29,32}$
7 or 20	$\overline{1,4}$
21 or 29	$\overline{1,8}$
12 or 28	$\overline{5,8}$
1 or 17	$\overline{5,12}$
15 or 23	$\overline{9,12}$
8 or 24	$\overline{17,20}$
14 or 32	$\overline{17,24}$
3 or 27	$\overline{21,24}$
9 or 19	$\overline{21,28}$
13 or 30	$\overline{25,28}$
6 or 22	$\overline{25,32}$
4 or 11	$\overline{29,32}$

Table 1. Definition of $I(j)$

j	$\overline{1,32} \setminus (\overline{13,16} \cup J(j))$
1,6,9,14,16,17,19,21,22,25,29,32	$\varnothing$
7 or 20	$\overline{1,4} \cup \overline{25,28}$
12 or 28	$\overline{5,8} \cup \overline{21,24}$
15 or 23	$\overline{1,4} \cup \overline{9,12}$
8 or 24	$\overline{17,20} \cup \overline{29,32}$
3 or 27	$\overline{21,24}$
13 or 30	$\overline{17,20} \cup \overline{25,28}$
4 or 11	$\overline{9,12} \cup \overline{29,32}$

Table 2. Definition of $J(j)$

■

Corollary 1:

$$G_{o,d} \text{ is transitive on } V_{64} \setminus \{0, d\}.$$

Proof:

Let $(a, a') \in (V_{64} \setminus \{0, d\})^2$. By Lemma 4 and Lemma 5 we get:

$\exists\ (z, z') \in V_{32}^2$: $(a \sim (e, z) \sim (e, z') \sim a')$.

■

Corollary 2:

$$G_o \text{ is transitive on } V_{64} \setminus \{0\}.$$

Proof:

Because of Corollary 1 it suffices to show that

$\exists\ g \in G_o : g(d) \neq d$ $\quad$ ($g(d) \neq 0$ because of $g \in G_o$).

Let $(k, k') \in M \setminus M_{d'}$. $(M \setminus M_{d'} \neq \varnothing$; for example for $k = 0$ and

$$k' := (\underset{1}{0}, \underset{2}{0}, \underset{\ldots}{\ldots}, \underset{19}{0}, \underset{20}{1}, \underset{21}{0}, \underset{22}{0}, \underset{23}{1}, \underset{24}{1}, \underset{25}{0}, \underset{\ldots}{\ldots}, \underset{48}{0})$$

we have $S(k) = S(k')$ and $S(k \oplus d') \neq S(k' \oplus d')$.)

$\Rightarrow F^{R}_{k,k'}(d) = (d_L, d_R \oplus S(k \oplus d') \oplus S(k' \oplus d')) \neq d.$

Since we know $F^{R}_{k,k'} \in G_o$, the proof is complete.

■

From Lemma 2, Corollary 1, and Corollary 2 we immediately obtain:

Corollary 3:

$$G \text{ is 3-transitive on } V_{64}.$$

4 Proof of the main Theorem

The proposition of Lemma 6 will help to complete the proof of the main theorem.

Lemma 6:

$$\exists\, (k, k') \in M\colon |\{x \in V_{64} \mid F^{R}_{k,k'}(x) = x\}| = 5 \cdot 2^{59}.$$

Proof:

We fix the following pair $(k, k') \in M$:

$$k := (\underset{1}{0}, \underset{2}{0}, \underset{\ldots}{\ldots}, \underset{12}{0}, \underset{13}{1}, \underset{14}{0}, \underset{\ldots}{\ldots}, \underset{48}{0}) \in V_{48} \text{ and}$$

$$k' := (\underset{1}{0}, \underset{2}{0}, \underset{\ldots}{\ldots}, \underset{17}{0}, \underset{18}{1}, \underset{19}{0}, \underset{\ldots}{\ldots}, \underset{48}{0}) \in V_{48}.$$

Then the permutation $F^R_{k,k'}$ exactly has the following set of fixed points:

$$\{(x_L, x_R) \in V_{64} \mid S(k \oplus EPx_L) \oplus S(k' \oplus EPx_L) = 0\} =$$

$$= \{(x_L, x_R) \in V_{64} \mid S_3(((k \oplus EPx_L)_j)_{j=13}^{18}) = S_3(((k' \oplus EPx_L)_j)_{j=13}^{18})\} =$$

$$= \{(x_L, x_R) \in V_{64} \mid (((EPx_L)_j)_{j=13}^{18}) \in \{(0,0,0,0,0,0), (1,0,0,0,0,1), (0,0,0,1,1,0), (1,0,0,1,1,1), (0,0,1,0,0,1), (1,0,1,0,0,0), (0,1,1,0,0,1), (1,1,1,0,0,0), (0,1,1,1,0,1), (1,1,1,1,0,0)\}\}.$$

Thus the permutation $F^R_{k,k'}$ exactly has $10 \cdot 2^{26} \cdot 2^{32} = 5 \cdot 2^{59}$ fixed points.

■

Theorem 1:

The following equality holds: $G = A_{2^{64}}$.

Proof:

Suppose $G \neq A_{2^{64}}$.

G is 3-transitive. Therefore we can apply proposition 5.2. of /Cam 81/ implying that G has a unique minimal normal subgroup which is Abelian or simple.

- Suppose that this normal subgroup is simple. Following the table on page 8 of /Cam 81/, which is based on the classification of finite simple groups (see also /CC 91/, p. 462), we obtain that 2^{64} has the form $\frac{q^2 - 1}{q - 1} = q + 1$, where q is a prime or a power of a prime. But because $2^{64} - 1$ is neither a prime nor a power of a prime, we get a contradiction.
- If this normal subgroup is Abelian, then G is "similar" to a subgroup of the affine group $Aff(V_{64})$ (see /Rob 82/, pp. 192-193).

  Two permutation groups H and H' on X and X', respectively, are called similar, if there exist an isomorphism α: $H \to H'$ and a bijection β: $X \to X'$ with the property:

  $\forall h \in H \ \forall x \in X$: $\beta(h(x)) = (\alpha(h))(\beta(x))$ (see /Rob 82/, p. 32).

That means that each element of G has the same cycle representation as a certain element of $Aff(V_{64})$. Particularly the number of fixed points of each element of G must be an element of the set $\{0, 2^0, 2^1, ..., 2^{64}\}$, because the fixed points of an affine mapping (if there are any) form an affine subspace of V_{64}.

From Lemma 6 we know that there exists an element of G with exactly $5 \cdot 2^{59}$ fixed points. Thus, also in the Abelian case we get a contradiction.

Hence, the supposition $G \neq A_{2^{64}}$ is wrong and the theorem is proved.

■

Corollary 4:

The groups $G_{(n)}$ generated by the n - round functions of the DES (with independent subkeys) are equal to $A_{2^{64}}$ $(n = 2, 3, ...)$.

Proof (sketch):

Obviously $G_{(n)}$ is a transitive subgroup of G.

Besides this, all permutations $F^R_{k,k'}$ and $F^L_{k,k'}$ also belong to $G_{(n)}$

(consider $(F_k \circ F_k \circ ... \circ F_k) \circ (F_{k'} \circ F_k \circ F_k \circ ... \circ F_k)^{-1} = F_k \circ F_{k'}^{-1}$

and $(F_k \circ F_k \circ ... \circ F_k)^{-1} \circ (F_k \circ F_k \circ ... \circ F_k \circ F_{k'}) = F_k^{-1} \circ F_{k'}$).

Because the given proofs of Lemma 4, Lemma 5, Corollary 2 and Lemma 6 make use of no other group elements than $F^R_{k,k'}$ and $F^L_{k,k'}$, we can prove $G_{(n)} = A_{2^{64}}$ in the same way as we proved $G = A_{2^{64}}$.

■

5 Conclusions

Theorem 1 gives an answer to an open question formulated for example by Pieprzyk/Zhang in /PZ 90/ ("Are the DES generators complete?"). The result shows that the structure of the one-round DES-permutations and the current S-boxes do not restrict the number of possible permutations attainable by composition. Since the generated alternating group $A_{2^{64}}$ is a large simple group and primitive on V_{64} we can exclude several imaginable cryptanalytic "shortcuts" of the DES-algorithm.

Though the proofs in this paper are based on various special properties of the permutations it is possible to find certain other S-boxes such that after replacement we obtain the same final result as in Theorem 1.

Finally, with regard to Corollary 4 one may expect that the set of 16-round DES-cipher-permutations generates the alternating group, too. This, however, remains an open question, because the influence of the DES key-scheduling must be taken into account.

Acknowledgement

The author would like to thank the members of the SIT GmbH for their help.

References

/Cam 81/ Cameron, P. J.: "Finite Permutation Groups and Finite Simple Groups" Bull. London Math. Soc., 13, 1981, 1-22

/CC 91/ Cameron, P. J.; Cannon, J.: "Fast Recognition of Doubly Transitive Groups" Journal of Symbolic Computation, 12, Nr. 4&5, 1991, 459-474

/CE 86/ Chaum, D.; Evertse, J. H.: "Cryptanalysis of DES with a reduced number of rounds; Sequences of linear factors in blockciphers" Proc. CRYPTO '85, Lect. Notes Comp. Sci., 218, 1986, 192-211

/CG 75/ Coppersmith, D.; Grossman, E.: "Generators for certain alternating groups with applications to cryptography" Journal of Applied Mathematics, 29, Nr. 4, 1975, 624-627

/DDF 84/ Davio, M.; Desmedt, Y.; Fosseprez, M. et al.: "Analytical Characteristics of the DES" Proc. CRYPTO '83, Plenum Press, New York and London, 1984, 171-202

/EG 83/ Even, S.; Goldreich, O.: "DES-like functions can generate the alternating group" IEEE Transactions on Information Theory, IT-29, Nr. 6, 1983, 863-865

/KRS 88/ Kaliski, B. S.; Rivest, R. L.; Sherman, A. T.: "Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DES)" Journal of Cryptology, 1, Nr. 1, 1988, 3-36

/NBS 77/ National Bureau of Standards: "Data Encryption Standard"
FIPS PUB 46, Washington, 1977

/PZ 90/ Pieprzyk, J.; Zhang, X. M.: "Permutation Generators of Alternating Groups"
Proc. AUSCRYPT '90, Lect. Notes Comp. Sci., 453, 1990, 237-244

/RM 85/ Reeds, J. A.; Manferdelli, J. L.: "DES has no per round linear factors"
Proc. CRYPTO '84, Lect. Notes Comp. Sci., 196, 1985, 377-389

/Rob 82/ Robinson, D. J. S.: "A Course in the Theory of Groups"
Springer, New York, Heidelberg, Berlin, 1982

/SM 87/ Simmons, G. J.; Moore, J. H.: "Cycle structure of the DES for keys having palindromic (or antipalindromic) sequences of round keys"
IEEE Transactions on Software Engineering, SE-13, Nr. 2, 1987, 262-273

/Wie 64/ Wielandt, H.: "Finite Permutation Groups"
Academic Press, New York, London, 1964