The Data Encryption Standard (DES)

The following describes how DES works and additionally illuminates background aspects during the cipher process.

The latter sets its focus in the visualization of all round ciphers $(m_{i-1}, m_i)_{i=1,\dots,17}$ with $m_i \in \{0,1\}^{32}$, all round keys $(K_i)_{i=1,\dots,16}$ with $K_i \in \{0,1\}^{48}$ and some statistical data that demonstrate DES' avalanche capabilities.

Moreover we describe, with respect to (w.r.t.) a key $k \in \{0,1\}^{64}$, the background in the evaluation of fixed points $p \in \{0,1\}^{64}$ (defined by $DES(k,p) = p$) as well as anti fixed points (defined by $DES(k,p) = \overline{p}$, where $\overline{(x_i)} := (1 - x_i)$ is a bitwise complementation). Within this context we also clarify the role of the special keys $k(5j)_{j=0,1,2,3}$ and $k(3n)_{n=1,2,3,4}$.

(1) Encryption and Decryption

The DES cipher is a bijective mapping $DES : \{0,1\}^{64} \to \{0,1\}^{64}$ that encrypts a 64 bit block (called plaintext) into a 64 bit block (called ciphertext).

Crucial in the generation of successive round ciphers $(m_{i-1}, m_i)_{i=1,\dots,17}$ (for encryption and decryption) is the equation $m_{i+1} := m_{i-1} \oplus f(m_i, K_i)$ due to its use in the evaluation of successive rounds $(m_{i-1}, m_i) \overset{K_i}{\to} (m_i, m_{i-1} \oplus f(m_i, K_i))$. DES' bijectivity is justified by the bijectivity of $\psi : \{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32} \times \{0,1\}^{32} : (a,b) \to (b, a \oplus f(a,K))$ where f may be any function, K any round key, and $IP : \{0,1\}^{64} \to \{0,1\}^{64}$. IP is noted as *initial permutation*. The bijectivity ensures also that the whole sequence $(m_{i-1}, m_i)_{i=1,\dots,17}$ is determined if we know any single round (m_{i_0-1}, m_{i_0}), $1 \le i_0 \le 17$ (and key k).

Encryption of a Plaintext p

$$p \overset{IP}{\to} (m_0, m_1) \overset{K_1}{\to} (m_1, m_2) \overset{K_2}{\to} \dots \overset{K_8}{\to} (m_8, m_9) \to \dots \overset{K_{16}}{\to} (m_{16}, m_{17}) \overset{Flip}{\to} (m_{17}, m_{16}) \overset{IP^{-1}}{\to} c$$

Since (in neighbored rounds) the right part of a previous round is copied to be the left part in the new round (hence redundancy appears), it is enough to visualize only $(m_i)_{i=0,\dots,17}$ instead of $(m_{i-1}, m_i)_{i=1,\dots,17}$ (see Figure 1). The most right column "DIST" displays the Hamming distances $dist(m_{i-1}, m_i)_{i=1,\dots,17}$. Interestingly, we realize $dist(m_{i-1}, m_i) \approx 16$ for all $i = 1, \dots, 17$.

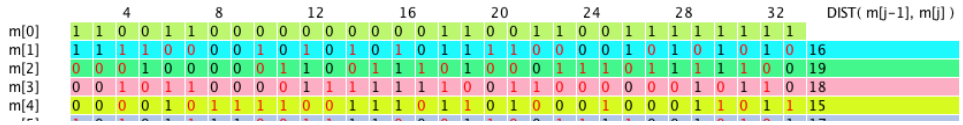

Figure 1: The first 3 round ciphers $(m_0, m_1) \overset{K_1}{\to} \dots \overset{K_3}{\to} (m_3, m_4)$

Decryption of a Ciphertext c

$$c \overset{IP}{\to} (m_{17}, m_{16}) \overset{K_{16}}{\to} (m_{16}, m_{15}) \overset{K_{15}}{\to} \ldots \overset{K_9}{\to} (m_9, m_8) \to \ldots \overset{K_1}{\to} (m_1, m_0) \overset{Flip}{\to} (m_0, m_1) \overset{IP^{-1}}{\to} p$$

The decryption process runs logically in the same way as the encryption process. It starts with input $c = IP^{-1}(m_{17}, m_{16})$ but applies the round keys in inverse order $(K_{16}, K_{15}, \ldots, K_2, K_1)$, whereas encryption's order is $(K_1, K_2, \ldots, K_{15}, K_{16})$.

(2) Generation of Round Keys $(K_i)_{i=1,\ldots,16}$ from a Given Key k

Figure 2: Color patterns of round keys $K_1, \ldots, K_4$, deduced from $k(9)$.

Each set of round keys $(K_i)_{i=1,\ldots,16}$ is deduced from a key $k := (k_i)_{i=1,\ldots,64}$ and generates round ciphers via $m_{i+1} = m_{i-1} \oplus f(m_i, K_i)$.
We describe the generation of $(K_i)_{i=1,\ldots,16}$, using $PC_1 : \{0,1\}^{64} \to \{0,1\}^{28} \times \{0,1\}^{28}$, $PC_2 : \{0,1\}^{28} \times \{0,1\}^{28} \to \{0,1\}^{48}$ and $(v_1, \ldots, v_{16}) \in \{1,2\}^{16}$ (full definitions may be taken from literature).

Moreover we explain the role of $(C_i, D_i)_{i=0,\ldots,16}$ which merely present some intermediate values during the generation of round keys:

(a) For $k \in \{0,1\}^{64}$ we define $(C_0, D_0) := PC_1(k) := \overbrace{k_{57}k_{49}\ldots k_{36}}^{C_0}, \overbrace{k_{63}k_{55}\ldots k_4}^{D_0}$
(b) For $i = 1, \ldots, 16$, $C_i :=$ cyclic left shift of C_{i-1} about v_i positions. Similar holds for the generation of the (D_i).

Due to $v_1 + \ldots + v_{16} = 28$, sixteen left shifts will generate C_0 again (resp. D_0). Since $K_i := PC_2(C_i, D_i)$, PC_2 selects specific positions from (C_i, D_i) to build up K_i.

In (3) on page 3 we will prove that each anti/fixed point is associated with one of eight keys, known as *weak keys* $:= \{k(0), k(5), k(10), k(15)\}$ or *semi weak keys* $:= \{k(3), k(6), k(9), k(12)\}$. Due to this association, *weak* and *semi weak keys* play a special role among all keys. Round keys, deduced from these keys, with redundant information towards each other, are therefore visualized in the panel "Roundkeys K_i" (see Figure 2) by a blue-yellow color pattern. For any keys other than *weak/semi weak keys*, color patterns have no meaning, but values have.

Figure 2 shows a colored matrix M where round key K_i is represented by line i.

The meaning of colors: Inside M we specify the 12 block matrices $[(1, 4k+1), (16, 4k+4)]_{k=0,1,\ldots,11}$. For each of these block matrices it holds (in case of *weak/semi weak keys*) that quadruples with the same color have the same content.

Example: Encrypt in "Key/Plaintext" the setting $(k(9), p)$ with any 64 bit plaintext p, and then watch the panel "Round keys K_i". The 1^{st} block matrix $[(1,1),(16,4)]$ shows that blue quadruples have value $(0,1,1,0)$ and yellow quadruples have value $(1,0,0,1)$. The 3^{rd} block matrix $[(1,9),(16,13)]$ shows that blue quadruples have value $(1,0,1,0)$ and yellow quadruples have value $(0,1,1,0)$.

(3) Evaluation of Fixed and Anti Fixed Points

The treatment of anti/fixed points completes the discussion of DES' properties and the program is able to evaluate all anti/fixed points that are known today (Dec 2011). The four *weak (resp. semi weak) keys* also represent the solutions of the problems $DES(k,.) = [DES(k,.)]^{-1}$ (resp. $DES(k,.) = [DES(k',.)]^{-1}$).

Fixed points

A fixed point p w.r.t. a key k is defined by $DES(k,p) = p$. Until today it is unknown how many fixed points exist (w.r.t. a key k), but it is known that there are 2^{32} fixed points for each of the four *weak keys* $k(5j)_{j=0,\ldots,3}$. To understand why let us have a closer look to the encryption process with its round ciphers.

$$p \overset{IP}{\to} (m_0, m_1) \overset{K_1}{\to} (m_1, m_2) \overset{K_2}{\to} \ldots \overset{K_8}{\to} (m_8, m_9) \to \ldots \overset{K_{16}}{\to} (m_{16}, m_{17}) \overset{Flip}{\to} (m_{17}, m_{16}) \overset{IP^{-1}}{\to} c$$

Applying the sequence generating equation $m_{i+1} = m_{i-1} \oplus f(m_i, K_i), i = 1, \ldots, 16$, towards a fixed point p w.r.t. a key k, it must (among others) hold: $p = c$ and $(m_0, m_1) = (m_{17}, m_{16})$ and $m_{15} = m_{17} \oplus f(m_{15}, K_{15}) = m_0 \oplus f(m_1, K_{16})$. Hence, if $K_{16} = K_1$, then $m_{15} = m_0 \oplus f(m_1, K_1) = m_2$. Proceeding one more step we get $m_{14} = m_{16} \oplus f(m_{15}, K_{15}) = m_1 \oplus f(m_2, K_{15})$. Applying the similar assumption $K_{15} = K_2$, we conclude $m_{14} = m_1 \oplus f(m_2, K_2) = m_3$. Repeated use of the assumption $K_{17-i} = K_i$ for $i = 1, \ldots, 16$ finally delivers the symmetry $m_{17-k} = m_k$ for $k = 0, 1, \ldots, 17$. Especially we have $m_8 = m_9$.

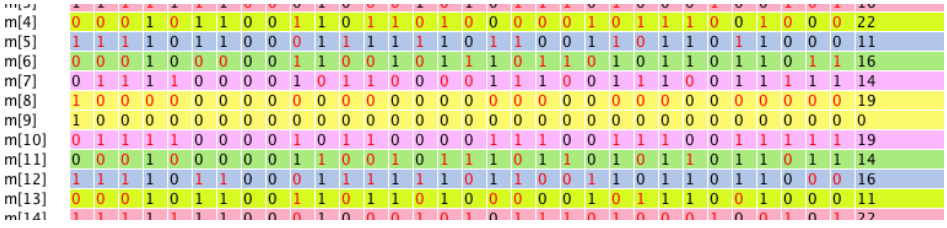

Figure 3: Symmetry: $m_{17-i} = m_i \iff Color(row[17-i]) = Color(row[i])$

Furthermore, recall that each single round (m_{i_0-1}, m_{i_0}) generates all (m_i). So especially (m_8, m_9) does with $m_8 = m_9$. Hence, if we select any $m_8 \in \{0,1\}^{32}$ and generate missing (m_i) via $m_9 := m_8$ and $m_{i+1} = m_{i-1} \oplus f(m_i, K_i)$, then we finally evaluate in c a fixed point that preserves the symmetry $m_{17-i} = m_i$.
Obviously, we also could start with any other round (m_{i-1}, m_i) as long as this

generates (m_8, m_9) with $m_8 = m_9$. To omit the check "$m_8 \stackrel{?}{=} m_9$", we start most easy: we define $m_8 \in \{0,1\}^{64}$ and proceed as described before.
In the program, a user enters any $m_8 \in \{0,1\}^{32}$ and the internal algorithm completes missing rounds via $m_9 := m_8$. Additionally, the symmetry $m_{17-i} = m_i$ allows a reduced visualization, displaying only $m_8, m_9, m_{10}, \ldots, m_{16}, m_{17}$. If a user wants to see all (m_i), he copies (p, k) into the panel "Key/Plaintext" and encrypts p w.r.t. key k. The program will display all $(m_i)_{i=0,\ldots,17}$ (see Figure 3).

Finally, there is the open question: "What keys $k \in \{0,1\}^{64}$ generate round keys (K_i) such that $K_{17-i} = K_i$?". It can be proven that these keys k are $k(0), k(5), k(10), k(15)$, where $k(abcd) := \left[a^3b^4(P_1)c^3d^4(P_2)\right]^2 \left[a^4b^3(P_3)c^4d^3(P_4)\right]^2$ (powers represent bit repetitions) with $a, b, c, d \in \{0,1\}$ and odd parity producing bits (P_k). Moreover, these keys satisfy the stronger $K_i \stackrel{all\ i,j}{=} K_j$ (see panel "Round keys K_j").

Example: To present $k(5) = k(5_{10})$, we proceed as follows:
$k(5) = k(0101) = \left[0^3 1^4(1) 0^3 1^4(0)\right]^2 \left[0^4 1^3(0) 0^4 1^3(0)\right]^2 =$ `1F1F 1F1F 0E0E 0E0E`.

Anti Fixed points
An anti fixed point p w.r.t. a key k is defined by $DES(k, p) = \overline{p}$. Until today it is unknown how many anti fixed points exist (w.r.t. a key k), but it is known that there are 2^{32} anti fixed points for each of the four *semi weak keys* $k(3n)_{j=1,\ldots,4}$.

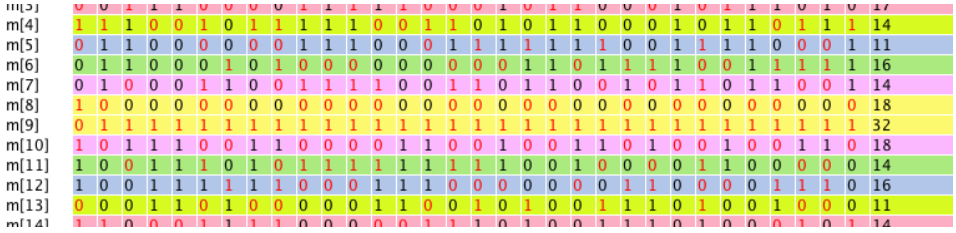

Figure 4: Symmetry: $m_{17-i} = \overline{m_i} \iff Color(row[17-i]) = Color(row[i])$

Their generation proceeds likely to the generation of fixed points but proves to be slightly more complex. We have to apply three equations: $m_{i+1} = m_{i-1} \oplus f(m_i, K_i)$, $f(\overline{m}, \overline{K}) = f(m, K)$ and $\overline{x} \oplus y = \overline{x \oplus y}$. To find anti fixed points, let us have a closer look to the encryption process with its round ciphers and consider

$$p \stackrel{IP}{\to} (m_0, m_1) \stackrel{K_1}{\to} (m_1, m_2) \stackrel{K_2}{\to} \ldots \stackrel{K_8}{\to} (m_8, m_9) \to \ldots \stackrel{K_{16}}{\to} (m_{16}, m_{17}) \stackrel{Flip}{\to} (m_{17}, m_{16}) \stackrel{IP^{-1}}{\to} c = \overline{p}$$

Hence $(m_{17}, m_{16}) = IP(\overline{p}) = \overline{IP(p)} = \overline{(m_0, m_1)} = (\overline{m_0}, \overline{m_1})$, it follows $m_{17} = \overline{m_0}$ and $m_{16} = \overline{m_1}$. Moreover $m_{15} = m_{17} \oplus f(m_{16}, K_{16}) = \overline{m_0} \oplus f(\overline{m_1}, K_{16})$. So, if we have a key k that forces $K_{16} = \overline{K_1}$, then $\overline{m_0} \oplus f(\overline{m_1}, \overline{K_1}) = \overline{m_0} \oplus f(m_1, K_1) = \overline{m_0 \oplus f(m_1, K_1)} = \overline{m_2}$ and it follows $m_{15} = \overline{m_2}$.

As you see, the relations between subkeys needed to generate anti fixed points are given by $K_{17-i} = \overline{K_i}$ $(i = 1, \ldots, 16)$. As a consequence, we get the round cipher's relations $m_{17-k} = \overline{m_k}$ $(k = 1, \ldots, 17)$, and especially $m_8 = \overline{m_9}$.
Finally, we need to answer "What keys $k \in \{0,1\}^{64}$ generate round keys (K_i) such that $K_{17-i} = \overline{K_i}$?". Again, it can be proven that these keys k are $k(3), k(6), k(9), k(12)$.

The two statements below finish the discussion about anti fixed points (AFP) and fixed points (FP). Both of them are due to $DES(\overline{k}, \overline{p}) = \overline{DES(k,p)}$ and demonstrate how to find new anti/fixed points if previous ones are known.

$$(1) \quad FP(k, m_8) = \eta \iff FP(\overline{k}, \overline{m_8}) = \overline{\eta}$$
$$(2) \quad AFP(k, m_8) = \eta \iff AFP(\overline{k}, \overline{m_8}) = \overline{\eta}$$

Summary: The generation of fixed points and anti fixed points proceeds similar, but anti fixed points need additionally the operation "complementation" (bitwise complementation). Symmetries $m_{17-i} = m_i$ for fixed points and $m_{17-i} = \overline{m_i}$ for anti fixed points apply. So far, anti/fixed points are only known w.r.t. the *weak/semi weak keys*. Each of these keys should be omitted due to the known relation between plaintexts/ciphertexts.

(4) The Internal Avalanche Effect with respect to Input Differences Δp

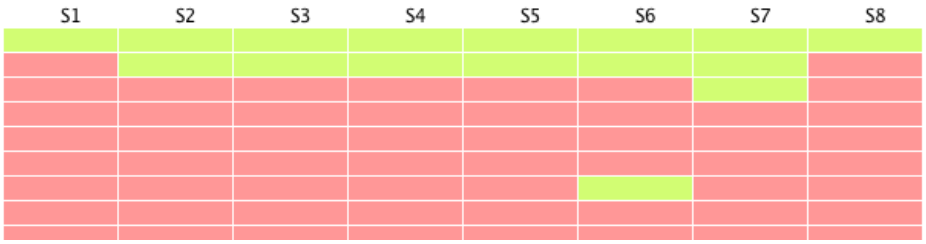

Figure 5: Cell (i, j) = YELLOW $\iff$ In round i, S-Box j gets same input feed

Given a key k and plaintexts $p, p + \Delta p$, we run $DES(k, p)$ and $DES(k, p + \Delta p)$. Since S-Boxes (due to their nonlinearity) act as DES' heart, a natural question (especially for $\Delta p = e_i := i^{th}$ *unit vector* or $\Delta p = e_i + e_j$) is: "Looking at round ciphers generated by (k, p) and $(k, p + \Delta p)$, what S-Boxes get different input feed ?". The answer is visualized per round and per S-Box in a yellow-red colored matrix (Figure 5). Its colors state:

- Cell (i, j) is RED $\iff$ In round i, S-Box j gets different input feed
- Cell (i, j) is YELLOW $\iff$ In round i, S-Box j gets the same input feed

Since it is not at all obvious how these colors are generated, we give a justification

that uses Figures 6, 7 and that finally points to the rows in panel "$m_0 - m_{17}$".

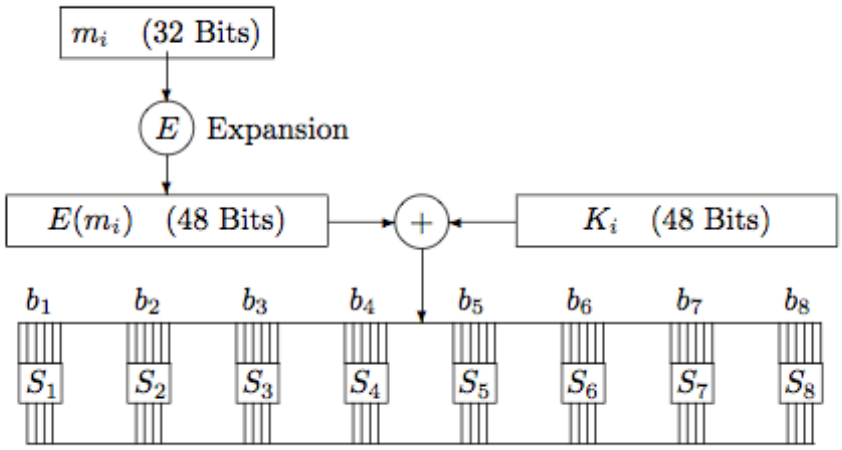

Figure 6: Input feed $E(m_i) \oplus K_i$ for all eight S-Boxes

Figure 6: We see that (in round i) the eight S-Boxes get $E(m_i) \oplus K_i$ and $E(m_i') \oplus K_i$ as input feed. Since K_i is redundant, it delivers no contribution to the difference in input feed, and thus may be ignored. Therefore we only deal with $E(m_i)$, $E(m_i')$. And since the applet's panels only show m_i but not the required $E(m_i)$, our problem is: "How can we retrieve $E(m_i)$ from m_i ?". The answer can be read from Figure 7 that visualizes the properties of the expansion function E.

Figure 7: Obviously, S-Box j gets input bits from $E(m_i)$ with numbers $6(j-1)+1, 6(j-1)+1, \ldots, 6j$ (in Figure 7 the boxes with 6 numbers in the lowest line). They originate in m_i from bits with numbers $4(j-1)$ $(mod\ 32)$, $4(j-1)+1$ $(mod\ 32), \ldots, 4j$ $(mod\ 32)$, $4j+1$ $(mod\ 32)$ (where $\mathbb{Z}/32\mathbb{Z} := \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{32}\}$, hence bit numbers $0, 33$ are represented by numbers $32, 1$).

Examples:
- In round i, S-Box 1 gets feed from m_i's bits $32, 1, 2, 3, 4, 5$.
- In round i, S-Box 2 gets feed from m_i's bits $4, 5, 6, 7, 8, 9$.
- In round i, S-Box 8 gets feed from m_i's bits $28, 29, 30, 31, 32, 1$.

Hence, to find cells' (i, j) color in Figure 5, we have to copy and encrypt, one by one, (k, p) and $(k, p + \Delta p)$ into "Key/Plaintext". Then compare in panel "$m_1 - m_{17}$" the strings m_i at positions $4(j-1)$ $(mod\ 32)$, $4(j-1)+1$ $(mod\ 32), \ldots,$ $4j$ $(mod\ 32)$, $4j+1$ $(mod\ 32)$.

Tests proved the color pattern to be "nearly independent on (k, p)" and hence more or less only depend on Δp. This means more precisely, that most of the cell's

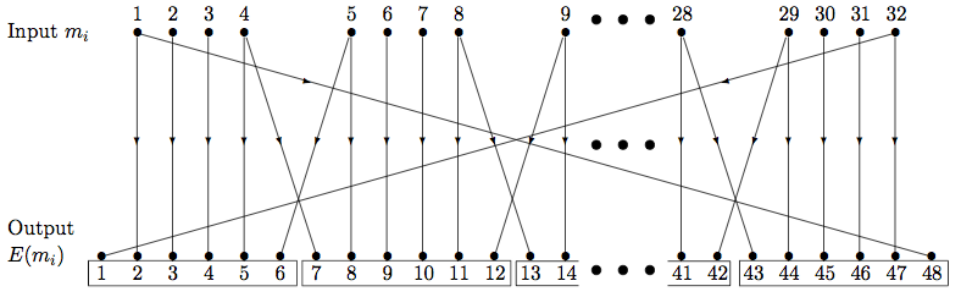

Figure 7: The effect of the expansion function E

colors are invariant under encryptions with varying (k, p) as long as $\Delta p \equiv const$, and only very few cells depend on settings (k, p). By running multiple encryptions with randomly varying (k, p) but constant Δp, we can see how color patterns change slightly with each new run. Since the color pattern as a whole describes how input differences spread during the whole encryption process, it may be considered as a measure of DES' avalanche capabilities.
Roughly it can be stated that starting with round 4, even "small" input differences Δp (i.e. $dist(\Delta p, 0) \leq 2$) spread – due to the four "cross overs" inside the expansion function E (see Figure 7) – over all S-Boxes and thus DES produces completely different ciphertexts.

(5) Literature for an in Depth Understanding of DES' Properties

[Ba09] W. Baltes: *Charakteristika des DES und deren programmiertechnische Visualisierung*, Masterthesis in Computer Science, supervised by Prof. Dr. Jörg Keller, Fern-Universität in Hagen (GER), February 2009

[Bi88] E. Biham and A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*, (Extended Abstract), 1988, Springer, pp. 2-21, Advances in Cryptology: Proceedings of CRYPTO '88, Springer, 1990, pp. 450-468

[Bi91] E. Biham and A. Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*, CTYPTO '90 & Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991

[Bi92] E. Biham and A. Shamir: *Differential Cryptanalysis of the Full 16-Round DES*, Advances in Cryptology: Proceedings of CRYPTO '92, Springer, 1993, pp. 487-496

[Bu04] Johannes Buchmann, *Einführung in die Kryptographie*, Springer, 2004, ISBN 3-540-40508-9

[Br86] E.F. Brickell, J.H. Moore, and M.R. Purtill, *Structure in the S-Boxes of the DES*, Advances in Cryptology: Proceedings of CRYPTO '86, Springer, 1987, pp. 3-8

[Co94] D. Coppersmith, *The Data Encryption Standard (DES) and its strength against attacks*, IBM J. Res. Develop., Vol. 38, No. 3, May 1994, pp. 243-250

[Da82] Donald W. Davies, *Some Regular Properties of the DES Algorithm*, Advances in Cryptology: Proceedings of Crypto '82, Plenum Press, 1983, pp. 89-96

[Ko82] Matthias König, Elmar Meyer zu Bexten, *DES Data Encryption Standard*, 14. August 1996, *http://www.uni-paderborn.de/fachbereich/AG/agmadh/.../bexten.ps.gz*

[Ln00] Susan Landau, *Standing the Test of Time: The Data Encryption Standard*, Notices of the AMS, March 2000, pp. 341-349

[Mo86] J.H. Moore and G.J. Simmons, *Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys*, Proceedings of Eurocrypt '86, Linköping, Sweden, May 20-22, 1986

[Mo87] J.H. Moore and G.J. Simmons, *Cycle Structure of the DES with Weak and Semi-Weak Keys*, Advances in Cryptology: Proceedings of CRYPTO '86 s, Springer, 1987, pp. 9-32