Der Data Encryption Standard (DES)

DES wurde im Juli 1977 als Standard zur nichtmilitärischen Verschlüsselung eingeführt und in den Jahren 1983, 1988 und 1993 als Standard bestätigt.

Das Verfahren wurde von IBM auf der Grundlage eines früheren Entwurfs (Lucifer) entwickelt. Die Designziele umfassten folgende Punkte:

- Hohe Sicherheit
- Vollständige Spezifikation und gute Verständlichkeit
- Geheimhaltung des Schlüssels, nicht des Algorithmus
- Verfügbarkeit für alle Benutzer
- Vielseitigkeit
- Effizienz
- Eignung für Hardware-Implementation
- Exportierbarkeit

Basis unserer Darstellung ist die Veröffentlichung „Federal Information Processing Standards Publication 46-2“ des National Bureau of Standards vom 30. Dezember 1993.

DES ist ein Standard zur Ver- und Entschlüsselung von Binärdaten mit Hilfe eines geheimen binären Schlüssels. Es handelt sich also um ein symmetrisches Verfahren. Der Schlüssel besteht aus 64 Bits, von denen allerdings nur 56 durch den Algorithmus genutzt werden, während die übrigen 8 Bits zur Fehlererkennung benutzt werden sollen (ungerade Parität).

DES verschlüsselt Blöcke von 64 Bits unter der Kontrolle des Schlüssels, wobei ein Geheimtext von ebenfalls 64 Bits entsteht. Zur Entschlüsselung wird der gleiche Algorithmus verwendet, wobei sich allerdings der Zugriff auf die Bits des Schlüssels verändert (günstig speziell für Hardware-Implementationen).

Sei x ein zu verschlüsselnder Klartext von 64 Bits und K der Schlüssel. Mit $\oplus$ bezeichnen wir die Exklusiv-Oder-Verknüpfung (XOR) von Bits $0 \oplus 0 = 1 \oplus 1 = 0$ und $0 \oplus 1 = 1 \oplus 0 = 1$, die stellenweise auf Folgen von Bits erweitert wird.

Die Verschlüsselung von x kann in drei Phasen zerlegt werden:

1. Gemäß einer festen Bit-Permutation IP wird x in x_0 transformiert. Wir zerlegen x_0 in zwei Teilblöcke L_0, R_0 von je 32 Bits, $x_0 = L_0 R_0$.

2. In 16 Runden werden für $1 \leq i \leq 16$ nun Blöcke L_i, R_i nach folgendem Schema berechnet:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

   Die Funktion f verarbeitet zwei Folgen von 32 bzw. 48 Bits und wird später beschrieben. Die Argumente K_i von f werden aus dem 56 Bit langen Schlüssel K abgeleitet.

3. Der Geheimtext y wird durch

$$y = IP^{-1}(R_{16}L_{16})$$

   bestimmt, wobei IP^{-1} die feste zu IP inverse Permutation ist.

Die Permutationen IP und IP^{-1} werden durch Tabellen definiert. Diese wie auch die folgenden Tabellen sind von links nach rechts und oben nach unten zu lesen. Ein Eintrag i an Position j bedeutet, dass Bit i der Eingabe an Position j der Ausgabe erscheint.

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Eine zentrale Rolle im DES spielt die Funktion f. Sie kombiniert Information aus der in einer Runde vorliegenden Verschlüsselung mit einer Auswahl von Bits des Schlüssels. Der erzeugte Wert wird durch XOR mit der Verschlüsselung verknüpft.

Die Funktion f erhält ein Argument A (32 Bits) und ein Argument J (48 Bits). Es werden folgende Schritte ausgeführt:

1. Das Argument A wird durch eine Expansionsfunktion E auf $E(A)$ mit 48 Bits erweitert. Dabei werden alle 32 Bits von A verwendet, einige werden wiederholt.
2. Der Wert $B = E(A) \oplus J$ wird berechnet und in 8 Blöcke von jeweils 6 Bits zerlegt, $B = B_1B_2B_3B_4B_5B_6B_7B_8$.
3. Jeder der 8 Blöcke wird in einen Block von 4 Bits übersetzt. Dazu dienen feste Tabellen $S_1, \ldots, S_8$ der Größe 4×16. Sei $B_j = b_1b_2b_3b_4b_5b_6$ mit $b_i \in \{0, 1\}$. Dann bestimmen b_1b_6 als Binärzahl aufgefasst eine Zeile von S_j, während $b_2b_3b_4b_5$ eine Spalte auswählen. Der Eintrag von S_j an der bezeichneten Position ist eine Zahl im Bereich $0 \ldots 15$, die als Binärzahl aufgefasst den 4 Bit Block C_j festlegt.
4. Die Konkatenation $C_1C_2C_3C_4C_5C_6C_7C_8$ wird der festen Permutation P unterworfen. Die Folge von Bits, die sich so ergibt, ist der Wert von $f(A, J)$.

Die Expansionsfunktion E wird durch folgende Tabelle festgelegt:

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Die abschließende Permutation P ist gegeben durch:

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Die Tabellen S_j zur Auswahl von 4 Bit langen Blöcken haben folgende Struktur:

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Schließlich muss noch beschrieben werden, wie die Folge der Argumente $K_1, \ldots, K_{16}$ für f auf der Basis von K berechnet werden.

1. Von den 64 Bits des Schlüssels K werden 56 gemäß einer festen Funktion $PC{-}1$ ausgewählt und mit $C_0 D_0$ bezeichnet, wobei C_0 und D_0 jeweils 28 Bits enthalten.

2. Für $1 \leq i \leq 16$ werden

$$\begin{aligned} C_i &= LS_i(C_{i-1}) \\ D_i &= LS_i(D_{i-1}) \end{aligned}$$

   berechnet. Dabei bezeichnet LS_i eine zyklische Verschiebung um ein Bit für $i \in \{1, 2, 9, 16\}$ und sonst eine Verschiebung um zwei Bits. Der Wert K_i ergibt sich durch Anwendung der festen Funktion $PC{-}2$ auf $C_i D_i$.

$PC-1$

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

$PC-2$

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Dass die Entschlüsselung den gleichen Algorithmus benutzen kann (mit umgekehrtem Zugriff auf die K_i) geht aus folgender Überlegung hervor.

Die abschließende Permutation IP^{-1} und IP am Anfang des Algorithmus heben ihre Wirkung auf und brauchen nicht betrachtet zu werden.

Aus der Eingabe R_iL_i berechnet eine DES-Runde

$$\begin{aligned} L' &= L_i \\ R' &= R_i \oplus f(L_i, K_i) \end{aligned}$$

und wegen $L_i = R_{i-1}$ gilt $L' = R_{i-1}$ und

$$\begin{aligned} R' &= R_i \oplus f(L_i, K_i) \\ &= R_i \oplus f(R_{i-1}, K_i) \\ &= (L_{i-1} \oplus f(R_{i-1}, K_i)) \oplus f(R_{i-1}, K_i) \\ &= L_{i-1}. \end{aligned}$$

Nach 16 Runden liegt daher R_0L_0 vor, woraus durch Vertauschen der Hälften $x_0 = L_0R_0$ wird.

Beispiele

Klartext:

1100110000000000110011001111111111110000101010101111000010101010

Schlüssel:

0001001100110100010101110111100110011011101111001101111111110001

$$
\begin{aligned}
E(R_0) &= 0111101000010101010101010111101000010101010101 \\
K_1 &= 0001101100000010111011111111100011100000111001 0 \\
E(R_0) \oplus K_1 &= 0110000100010111011101010000110011001010010 0111 \\
f(R_0, K_1) &= 00100011010010101010100110111011 \\
R_1 &= 11101111010010100110010101000100
\end{aligned}
$$

$$
\begin{aligned}
E(R_1) &= 0111010111101010010101000011000010101010000010 01 \\
K_2 &= 0111100110101110110110011101101111001001111001 01 \\
E(R_1) \oplus K_2 &= 0000110001000100100011011110101101100011111011 00 \\
f(R_1, K_2) &= 00111100101010111000011110100011 \\
R_2 &= 11001100000000010111011100001001
\end{aligned}
$$

$$
\begin{aligned}
E(R_2) &= 111001011000000000000010101110101110100001010011 \\
K_3 &= 010101011111110010001010010000101100111110011001 \\
E(R_2) \oplus K_3 &= 101100000111110010001000111110000010011111001010 \\
f(R_2, K_3) &= 010011010001011001101110101100000 \\
R_3 &= 101000100101110000001011111110100
\end{aligned}
$$

$$
\begin{aligned}
E(R_3) &= 010100000100001011111000000001010111111110101001 \\
K_4 &= 011100101010110111010110110110110011010100011101 \\
E(R_3) \oplus K_4 &= 001000101110111100101110110111100100101010110100 \\
f(R_3, K_4) &= 101110110010001101110111010011100 \\
R_4 &= 011101110010001000000000001000101
\end{aligned}
$$

$$
\begin{aligned}
E(R_4) &= 101110101110100100000100000000000000001000001010 \\
K_5 &= 011111001110110000000111111010110101001110101000 \\
E(R_4) \oplus K_5 &= 110001100000010100000011111010110101000110100010 \\
f(R_4, K_5) &= 001010000001001110101101110000011 \\
R_5 &= 100010100100111110100110001101111
\end{aligned}
$$

$$
\begin{aligned}
E(R_5) &= 11000101010000100101111111010000110000011010111 \\
K_6 &= 01100011101001010011111001010000011110110010111 \\
E(R_5) \oplus K_6 &= 10100110111001110110000110000000101110101000000 \\
f(R_5, K_6) &= 10011110010001011100110100101100 \\
R_6 &= 11101001011001111100110101101001
\end{aligned}
$$

$$
\begin{aligned}
E(R_6) &= 11110101001010110000111111100101101010110101010011 \\
K_7 &= 11101100100001001011011111110110000110001011110 0 \\
E(R_6) \oplus K_7 &= 00011001101011111011100000010011101100111110111 1 \\
f(R_6, K_7) &= 10001100000001010001110000100111 \\
R_7 &= 00000110010010101011101000010000
\end{aligned}
$$

$$
\begin{aligned}
E(R_7) &= 00000000110000100101010101011111010000001010000 0 \\
K_8 &= 11110111100010100011101011000001001110111111101 1 \\
E(R_7) \oplus K_8 &= 11110111010010000110111110011110011110110101101 1 \\
f(R_7, K_8) &= 00111100000011101000011011111001 \\
R_8 &= 11010101011010010100101110010000
\end{aligned}
$$

$$
\begin{aligned}
E(R_8) &= 011010101010101101010010101001010111110010100001 \\
K_9 &= 111000001101101111101011111011011110011110000001 \\
E(R_8) \oplus K_9 &= 100010100111000010111001010010001001101100100000 \\
f(R_8, K_9) &= 00100010001101100111110001101010 \\
R_9 &= 00100100011111001100011001111010
\end{aligned}
$$

$$
\begin{aligned}
E(R_9) &= 000100001000001111111001011000001100001111110100 \\
K_{10} &= 101100011111001101000111101110100100011001001111 \\
E(R_9) \oplus K_{10} &= 101000010111000010111110110110101000010110111011 \\
f(R_9, K_{10}) &= 01100010101111001001110000100010 \\
R_{10} &= 10110111110101011101011110110010
\end{aligned}
$$

$$
\begin{aligned}
E(R_{10}) &= 010110101111111010101011111010101111110110100101 \\
K_{11} &= 001000010101111111010011110111101101001110000110 \\
E(R_{10}) \oplus K_{11} &= 011110111010000101111000001101000010111000100011 \\
f(R_{10}, K_{11}) &= 11100001000001001111101000000010 \\
R_{11} &= 11000101011110000011110001111000
\end{aligned}
$$

$$
\begin{aligned}
E(R_{11}) &= 011000001010101111110000000111111000001111110001 \\
K_{12} &= 011101010111000111110101100101000110011111101001 \\
E(R_{11}) \oplus K_{12} &= 000101011101101000000101100010111110010000011000 \\
f(R_{11}, K_{12}) &= 11000010011010001100111111101010 \\
R_{12} &= 01110101101111010001100001011000
\end{aligned}
$$

$$
\begin{aligned}
E(R_{12}) &= 001110101011110111111010100011110000001011110000 \\
K_{13} &= 100101111100010111010001111110101011101001000001 \\
E(R_{12}) \oplus K_{13} &= 101011010111100000101011011101011011100010110001 \\
f(R_{12}, K_{13}) &= 11011101101110110010100100100010 \\
R_{13} &= 00011000110000110001010101011010
\end{aligned}
$$

$$
\begin{aligned}
E(R_{13}) &= 000011110001011000000110100010101010101011110100 \\
K_{14} &= 010111110100001110110111111100101110011100111010 \\
E(R_{13}) \oplus K_{14} &= 010100000101010110110001011110000100110111001110 \\
f(R_{13}, K_{14}) &= 10110111001100011000111001010101 \\
R_{14} &= 11000010100011001001011000001101
\end{aligned}
$$

$$
\begin{aligned}
E(R_{14}) &= 11100000010101000101100101001010110000000101101 1 \\
K_{15} &= 10111111100100011000110100111101001111110000101 0 \\
E(R_{14}) \oplus K_{15} &= 01011111110001011101010001110111111111101010001 \\
f(R_{14}, K_{15}) &= 01011011100000010010011101101110 \\
R_{15} &= 01000011010000100011001000110100
\end{aligned}
$$

$$
\begin{aligned}
E(R_{15}) &= 00100000011010100000010000011010010000011010100 0 \\
K_{16} &= 11001011001111011000101100001110000101111111010 1 \\
E(R_{15}) \oplus K_{16} &= 11101011010101111000111100010100010101100101110 1 \\
f(R_{15}, K_{16}) &= 11001000110000000100111110011000 \\
R_{16} &= 00001010010011001101100110010101
\end{aligned}
$$

Geheimtext:

1000010111101000000100110101010000001111000010101011010000000101

Klartext:

1100110000000000110011000111111111110000101010101111000010101010

Schlüssel:

0001001100110100010101110111100110011011101111001101111111110001

$$
\begin{aligned}
E(R_0) &= 0111101000010101010101010111101000010101010101 \\
K_1 &= 0001101100000010111011111111100011100000111001 0 \\
E(R_0) \oplus K_1 &= 0110000100010111011101010000110011001010010 0111 \\
f(R_0, K_1) &= 00100011010010101010100110111011 \\
R_1 &= 11101111010010100110010111000100
\end{aligned}
$$

$$
\begin{aligned}
E(R_1) &= 0111010111101010010101000011000010111110000010 01 \\
K_2 &= 0111100110101110110110011101101111001001111001 01 \\
E(R_1) \oplus K_2 &= 0000110001000100100011011110101101110111111011 00 \\
f(R_1, K_2) &= 00101100101110111010011110101010 \\
R_2 &= 11011100000100010101011100000000
\end{aligned}
$$

$$
\begin{aligned}
E(R_2) &= 011011111000000010100010101010101110100000000001 \\
K_3 &= 010101011111110010001010010000101100111110011001 \\
E(R_2) \oplus K_3 &= 001110100111110000101000111010000010011110011000 \\
f(R_2, K_3) &= 00100110100000000111100111100100 \\
R_3 &= 11001001110010100001110000100000
\end{aligned}
$$

$$
\begin{aligned}
E(R_3) &= 011001010011111001010100000011111000000100000001 \\
K_4 &= 011100101010110111010110110110110011010100011101 \\
E(R_3) \oplus K_4 &= 000101111001001110000010110101001011010000011100 \\
f(R_3, K_4) &= 10011110000000011001011001101010 \\
R_4 &= 01000010000100001100000101101010
\end{aligned}
$$

$$
\begin{aligned}
E(R_4) &= 001000000100000010100001011000000010101101010100 \\
K_5 &= 011111001110110000000111111010110101001110101000 \\
E(R_4) \oplus K_5 &= 010111001010110010100110100010110111100011111100 \\
f(R_4, K_5) &= 01000110101010000110111010101011 \\
R_5 &= 10001111011000100111001010001011
\end{aligned}
$$

$$
\begin{aligned}
E(R_5) &= 110001011110101100000100001110100101010001010111 \\
K_6 &= 011000111010010100111110010100000111101100101111 \\
E(R_5) \oplus K_6 &= 101001100100111000111010011010100010111101111000 \\
f(R_5, K_6) &= 01011110011000111100110000111000 \\
R_6 &= 00011100011100110000110101010010
\end{aligned}
$$

$$
\begin{aligned}
E(R_6) &= 000011111000001110100110100001011010101010100100 \\
K_7 &= 111011001000010010110111111101100001100010111100 \\
E(R_6) \oplus K_7 &= 111000110000011100010001011100111011001000011000 \\
f(R_6, K_7) &= 00000011000101000101111010110111 \\
R_7 &= 10001100011101100010110000111100
\end{aligned}
$$

$$
\begin{aligned}
E(R_7) &= 010001011000001110101100000101011000000111111001 \\
K_8 &= 111101111000101000111010110000010011101111111011 \\
E(R_7) \oplus K_8 &= 101100100000100110010110110101001011101000000010 \\
f(R_7, K_8) &= 10010100000100100001001100001001 \\
R_8 &= 10001000011000010001111001011011
\end{aligned}
$$

$$
\begin{aligned}
E(R_8) &= 11000101000000110000001010001111110000101111 0111 \\
K_9 &= 11100000110110111110101111101101111001111 0000001 \\
E(R_8) \oplus K_9 &= 00100101110110001110100101100010001001010111 0110 \\
f(R_8, K_9) &= 01111011111111001100101101101100 \\
R_9 &= 11110111100010101110011101010000
\end{aligned}
$$

$$
\begin{aligned}
E(R_9) &= 01111010111111000101010101110000111010101010000 1 \\
K_{10} &= 10110001111100110100011110111010010001100100 1111 \\
E(R_9) \oplus K_{10} &= 11001011000011110001001011001010101011001110 1110 \\
f(R_9, K_{10}) &= 00110011110100111100000100010100 \\
R_{10} &= 10111011101100101101111101001111
\end{aligned}
$$

$$
\begin{aligned}
E(R_{10}) &= 11011111011111011010010101101111111010100101 1111 \\
K_{11} &= 00100001010111111101001111011110110100111000011 0 \\
E(R_{10}) \oplus K_{11} &= 11111110001000100111011010110001001110011101 1001 \\
f(R_{10}, K_{11}) &= 01100100110011001011000011010111 \\
R_{11} &= 10010011010001100101011110000111
\end{aligned}
$$

$$
\begin{aligned}
E(R_{11}) &= 11001010011010100000110000101010111110000001111 \\
K_{12} &= 01110101011100011111010110010100011001111110100 1 \\
E(R_{11}) \oplus K_{12} &= 10111111000110111111100110111110100110111110011 0 \\
f(R_{11}, K_{12}) &= 01110111000111011111111001000110 \\
R_{12} &= 11001100101011110010000100001001
\end{aligned}
$$

$$
\begin{aligned}
E(R_{12}) &= 11100101100101010101111010010000001010000101001 1 \\
K_{13} &= 10010111110001011101000111111010101110100100000 1 \\
E(R_{12}) \oplus K_{13} &= 01110010010100001000111101101010100100100001001 0 \\
f(R_{12}, K_{13}) &= 11011010010110000010110000000001 \\
R_{13} &= 01001001000111100111101110000110
\end{aligned}
$$

$$
\begin{aligned}
E(R_{13}) &= 00100101001010001111110000111111011111000000110 0 \\
K_{14} &= 01011111010000111011011111110010111001110011101 0 \\
E(R_{13}) \oplus K_{14} &= 01111010011010110100101111001101100110110011011 0 \\
f(R_{13}, K_{14}) &= 11101011010111001101111111100010 \\
R_{14} &= 00100111111100111111111011101011
\end{aligned}
$$

$$
\begin{aligned}
E(R_{14}) &= 100100001111111110100111111111111101011101010110 \\
K_{15} &= 101111111001000110001101001111010011111100001010 \\
E(R_{14}) \oplus K_{15} &= 001011110110111000101010110000101110100001011100 \\
f(R_{14}, K_{15}) &= 11101101011101010010011011110000 \\
R_{15} &= 10100100011010110101110101110110
\end{aligned}
$$

$$
\begin{aligned}
E(R_{15}) &= 010100001000001101010110101011111010101110101101 \\
K_{16} &= 110010110011110110001011000011100001011111110101 \\
E(R_{15}) \oplus K_{16} &= 100110111011111011011101101000011011110001011000 \\
f(R_{15}, K_{16}) &= 00010111111000010111100011110001 \\
R_{16} &= 00110000000100101000011000011010
\end{aligned}
$$

Geheimtext:

001010000011011110001110001010010101101111100010001010101000010 0

Einsatz von DES

DES lässt sich sehr effizient in Hard- oder Software implementieren. Die Permutationen und Abbildungen können durch „Verdrahtung“ bzw. Tabellen realisiert werden. Allerdings sind einige alternative Verfahren in Software wesentlich schneller. (Der Standard schrieb in seiner ursprünglichen Fassung eine Hardware-Implementation vor.)

Seit ca. 1980 sind DES-Verschlüsselungschips auf dem Markt, die Durchsatzraten liegen inzwischen über 1 Gbit/Sekunde.

Entsprechend attraktiv ist der Einsatz von DES für Behörden und Firmen. Amerikanische Banken nutzen DES zur Verschlüsselung von PINs und im Zahlungsverkehr.

Betriebsarten von DES

Für den Einsatz des DES zur Verschlüsselung eines Datenstroms $x_1 x_2 \ldots$ schlägt der Standard vier Betriebsarten vor:

Electronic Codebook (ECB): Jeder Block von 64 Bits wird mit dem gleichen K verschlüsselt, $y_i = c_K(x_i)$.

Cipher Block Chaining (CBC): Ein y_0 wird festgelegt. Dann wird $y_i = c_K(y_{i-1} \oplus x_i)$ für $i \geq 1$ gesetzt.

Output Feedback (OFB): Ein z_0 wird festgelegt. Eine Folge z_i wird für $i \geq 1$ durch $z_i = c_K(z_{i-1})$ gebildet. Der Geheimtext wird durch $y_i = x_i \oplus z_i$ gebildet.

Cipher Feedback (CFB): Ein y_0 wird festgelegt. Folgen z_i, y_i werden durch $z_i = c_K(y_{i-1})$ und $y_i = x_i \oplus z_i$ gebildet.

Beachte: Wird in CBC oder CFB ein Stück Klartext x_i verändert, dann wirkt sich dies auf alle Geheimtextblöcke y_j mit $j \geq i$ aus.

Beispiel eines moderneren Block-Verfahrens

Das Verfahren Skipjack wurde ab 1985 von der NSA entwickelt und unterlag der Geheimhaltung. Es wurde zunächst nur in „versiegelter“ Hardware implementiert.

Im Jahr 1998 wurde das Verfahren offengelegt, davor waren mur folgende Details bekannt:

- Es ist ein iteratives Block-Verfahren.

- Die Blocklänge beträgt 64 Bits.
- Die Schlüssellänge beträgt 80 Bits.
- Jede Ver- oder Entschlüsselung benötigt 32 Runden.

Eine Expertengruppe gab folgendes Argument für die Sicherheit von Skipjack: Unter der Annahme, dass sich die Kosten von Rechenleistung alle 18 Monate halbieren, wird der Aufwand zum Brechen von Skipjack durch vollständige Suche im Schlüsselraum von Skipjack erst in 36 Jahren den Wert erreichen, der für DES heute gilt.