

Informationsverarbeitung
Datenverschlüsselung
Festlegung des Algorithmus DEA 1
 Identisch mit ISO/DIS 8227 Ausgabe 1985

DIN
ISO 8227

Information processing; Data encipherment;
 Specification of algorithm DEA 1
 Identical with ISO/DIS 8227 edition 1985

Einsprüche bis 31. Oktober 1985

Anwendungswarnvermerk auf der
 letzten Seite beachten!

Das internationale Schriftstück ISO/DIS 8227, Ausgabe 1985-06-13,
 "Information processing; Data encipherment; Specification of algorithm DEA 1",
 ist unverändert in diesen deutschen Norm-Entwurf übernommen worden.

Nationales Vorwort

In diesem Norm-Entwurf ist der von ISO/TC 97/SC 20¹⁾ verabschiedete Internationale Norm-Entwurf ISO/DIS 8227, Ausgabe 1985-06-13, unverändert wiedergegeben. Dieser Internationale Norm-Entwurf wurde unter Mitwirkung des Ausschusses "Datenverschlüsselung" des Normenausschusses Informationsverarbeitungssysteme (NI) erarbeitet.

Der Norm-Entwurf DIN ISO 8227 liegt hiermit in deutscher Übersetzung vor. Anwendungen dieser Festlegungen werden vor allem im Bereich der Datenübermittlung (ISO/TC 97/SC 6), der Offenen Systeme (ISO/TC 97/SC 21) und des Bankwesens (ISO/TC 68) erwartet.

Die Anwendung dieser Festlegungen erfordert möglicherweise die Berücksichtigung von Patenten (z. B. D.P. 2231849 und D.P. 2252670). Inwieweit hierdurch die Möglichkeit der nationalen Normung beeinträchtigt ist, wird zur Zeit durch das DIN geklärt.

Auf internationaler Ebene sind die Verhandlungen zwischen dem Patentinhaber IBM und ISO/TC 97 abgeschlossen worden, und die Anforderungen der ISO (siehe ISO DIRECTIVES Annex 1E "Rules for reference to patented items in International Standards") sind erfüllt.

- ¹⁾ ISO - International Organization for Standardization
 TC 97 - Information Processing Systems
 SC 20 - Data Cryptographic Techniques

Fortsetzung Seite 2 bis 28

Normenausschuß Informationsverarbeitungssysteme (NI) im DIN
 Deutsches Institut für Normung e.V.

Jede Art der Vervielfältigung, auch auszugsweise, nur mit Genehmigung des DIN Deutsches Institut für Normung e.V., Berlin, gestattet.

Deutsche Übersetzung

Informationsverarbeitung - Datenverschlüsselung

Festlegung des Algorithmus DEA 1

Inhalt

	Seite
1 Zweck und Anwendungsbereich	3
2 Verweisungen auf andere Normen	4
3 Begriffe	4
4 Verträglichkeit	5
5 Der Algorithmus DEA 1	5
ANHANG A – Eigenschaften des Algorithmus DEA 1	19
ANHANG B – Beispiel für die Arbeitsweise des Verschlüsselungsalgorithmus	22
ANHANG C – Information über Patente	28

1 Zweck und Anwendungsbereich

Diese Norm legt einen Blockschlüsselalgorithmus fest, der für Verschlüsselung und Entschlüsselung von Daten einen geheimen Schlüssel benutzt.

Für jeden vorgegebenen Schlüssel wird durch diese Norm sowohl für die Entschlüsselung als auch die Verschlüsselung eine Transformation von einem Eingabeblock in einen zugehörigen Ausgabeblock festgelegt.

Die Anwendung dieses Algorithmus kann von gewissen Eigenschaften abhängen, die im Anhang A beschrieben sind, der nicht Bestandteil der Norm ist.

Anmerkungen

1. Diese Norm ist inhaltlich gleich mit dem Normentwurf ISO DIS 8227 und mit Ausnahme der Vorschrift für die Benutzung der Bits 8, 16, ... des Schlüsselblocks auch mit der Federal Information Processing Standards Publication 46, die vom United States National Bureau of Standards herausgegeben worden ist. Diese Norm schließt die Normung weiterer Verschlüsselungsalgorithmen nicht aus.
2. Die Betriebsarten für 64-bit-Blockschlüsselalgorithmus sind im Normentwurf DIN ISO 8372 beschrieben.
3. Verfahren der Mehrfachverschlüsselung mit unterschiedlichen Schlüsseln können in späteren Normen behandelt werden.
4. Die Anwendung dieser Norm kann die Benutzung eines Patents einschließen. (Siehe Anhang C)

2 Verweisungen auf andere Normen

DIN ISO 8372 Betriebsarten für 64-bit-Blockschlüsselungsalgorithmen, z.Zt. noch Entwurf.

3 Begriffe und Bezeichnungen

3.1 Begriffe

3.1.1 Schlüsselblock: Ein Block von 64 bit, aus dem der 56-bit-Schlüssel gemäß der Vorschrift von 5.1.2 entnommen wird.

3.1.2 Schlüssel: Die 56-bit-Größe, die den Algorithmus steuert und entsprechend Abschnitt 5 eine aus den 2^{56} möglichen Transformationen eindeutig auswählt.

3.2 Konventionen und Bezeichnungen

3.2.1 Dort, wo Blöcke von Bits mit Symbolen wie z.B. L, R, B_1 , B_2 , B_8 bezeichnet sind, gelten folgende Konventionen:

- a) LR bezeichnet den Block, der aus den Bits von L gefolgt von den Bits von R besteht.
- b) Die Folge $B_1 B_2 \dots B_8$ bezeichnet den Block, der aus den Bits von B_1 gefolgt von denen aus B_2 (usw.) bis zu den Bits von B_8 besteht.
- c) Die Bit-Positionen eines Blocks sind beginnend mit 1 für das am weitesten links stehende Bit numeriert.
- d) Bei den verwendeten Abkürzungen wurden aus Kompatibilitätsgründen die Abkürzungen der englischsprachigen ISO-Norm übernommen.

3.2.2 Das Symbol $\oplus$ wird für die bitweise Addition modulo 2 (das "exklusive Oder") verwendet.

4 VERTRÄGLICHKEIT

Eine Implementation, die für jede Eingabe und alle Schlüssel die gleiche Ausgabe erzeugt, wie sie durch den Verschlüsselungs- und Entschlüsselungsalgorithmus erzeugt wird, der in Abschnitt 5 beschrieben ist, ist mit den Anforderungen dieser Norm verträglich, auch wenn die Arbeitsweise der Durchführung sich von der in dieser Norm vorgesehenen unterscheidet.

5 DER ALGORITHMUS DEA 1

5.1 Allgemeine Beschreibung

Verschlüsselung und Entschlüsselung sind Algorithmen, die von einem Schlüssel von 56 bit gesteuert und auf Blöcke von 64 bit angewendet werden. Der 56-bit-Schlüssel ist in einem Schlüsselblock von 64 bit enthalten. Die Bits 8, 16, 24, 32, 40, 48, 56 und 64 dieses Schlüsselblocks werden nicht von dem Algorithmus ausgewertet. Ihre Verwendung ist in dieser Norm nicht spezifiziert.

Anmerkung: In einigen Anwendungen des Algorithmus werden die Bits 8, 16, 24, 32, 40, 48, 56 und 64 als ungerade Paritätsbits für das jeweilige Oktet, das sie abschließen, benutzt.

Die Entschlüsselung wird mit dem gleichen Schlüssel durchgeführt wie die Verschlüsselung. Dabei ist der Zugriff auf die Bits des Schlüssels so geändert, daß der Entschlüsselungsprozeß den Verschlüsselungsprozeß gerade rückgängig macht.

Ein Block, der verschlüsselt werden soll, wird einer Initialpermutation unterworfen (IP). Es folgt eine komplexe schlüsselabhängige Berechnung und schließlich eine Permutation (IP^{-1}), die zu der Initialpermutation invers ist. Die schlüsselabhängige Berechnung kann mit Hilfe einer Verschlüsselungsfunktion (f) und einer Teilschlüsselfolge (KS) definiert werden.

Der Algorithmus für die Verschlüsselung ist in 5.2, der inverse Algorithmus für die Entschlüsselung in 5.3 beschrieben. Die Verschlüsselungsfunktion

(f) ist in 5.4 mit Hilfe primitiver Funktionen beschrieben. Dies sind Auswahlfunktionen ($S_1, S_2, \dots, S_8$), die Erweiterungsfunktion (E) und die Permutationsfunktion (P). Die Schlüsselfolge (KS) wird in 5.5 beschrieben.

5.2 Verschlüsselungsalgorithmus

5.2.1 Berechnungsschritte

Der Algorithmus gliedert sich in folgende Berechnungsschritte (Siehe Bild 1):

- a) Eine Initialpermutation des zu verschlüsselnden Eingabeblocks von 64 bit (siehe 5.2.2).
- b) 16 Iterationen einer schlüsselabhängigen Berechnung, beginnend mit dem permutierten Eingabeblock (siehe 5.2.3), gefolgt von einer Vertauschung der linken und rechten Hälfte des Ergebnisblocks.
- c) Eine abschließende Permutation, die invers zu der Initialpermutation ist (siehe 5.2.4).

5.2.2 Initialpermutation

Die 64 bit des zu verschlüsselnden Eingabeblocks werden zunächst der Initialpermutation unterworfen, die als IP bezeichnet wird und in Tabelle 1 definiert ist. Diese Tabelle ist so zu lesen, daß das Bit 58 des ursprünglichen Eingabeblocks zum Bit 1 des permutierten Eingabeblocks, das Bit 50 zum Bit 2, etc., und schließlich das Bit 7 des ursprünglichen Eingabeblocks zum letzten Bit des permutierten Eingabeblocks wird.

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

Tabelle 1. Initialpermutation IP

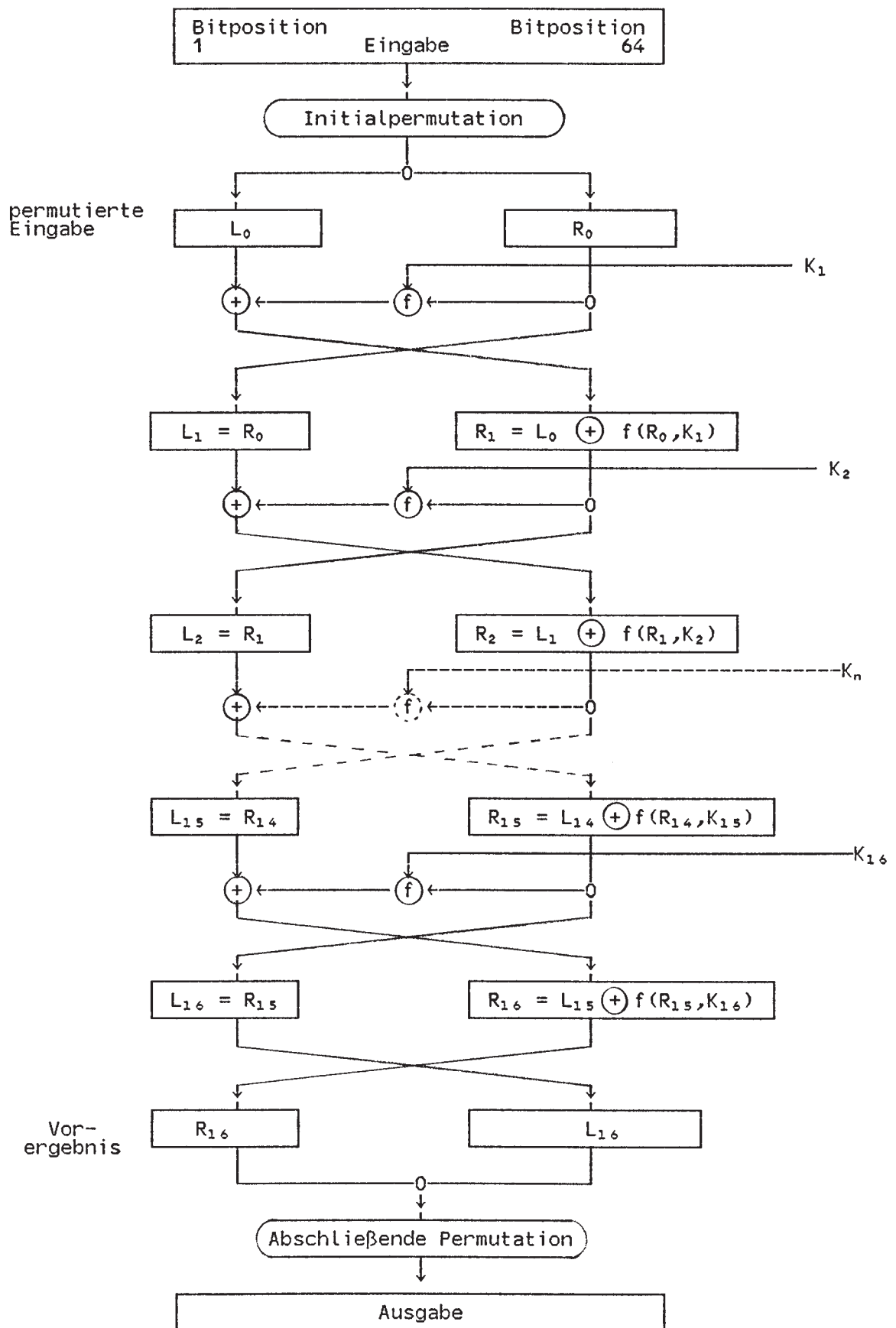


BILD 1. Verschlüsselungsverfahren

5.2.3 Schlüsselabhängige Berechnung

5.2.3.1 Ein gemäß Spezifikation in 5.2.2 erzeugter permutierter Eingabeblock durchläuft eine 16-stufige iterative Berechnung, der jeweils eine Vertauschung von Blöcken folgt. Jede Iteration enthält die Operation der in 5.4 definierten Verschlüsselungsfunktion (f), deren Argument aus 2 Blöcken besteht:

- a) ein 32-bit-Block (R), der die rechte Hälfte des 64-bit-Blocks LR ist;
- b) ein 48-bit-Block (K), der aus dem 56-bit-Schlüssel abgeleitet wird, wie in 5.2.3.2 spezifiziert ist.

Das Ergebnis L_n R_n der n -ten Iteration mit dem Argument L_{n-1} R_{n-1} ist durch folgende Gleichungen definiert:

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n),$$

wobei

- $\oplus$ die in 3.2.2 definierte Bedeutung hat,
- K_n der Block von 48 Bits ist, wie in 5.2.3.2 spezifiziert, und
- f die Verschlüsselungsfunktion ist, die in 5.4 spezifiziert ist.

Nach der 16. Iteration werden die Blöcke L_{16} R_{16} vertauscht, um das vorläufige Ergebnis $VE=R_{16}$ L_{16} zu erzeugen.

5.2.3.2 Für jede Iteration wird ein unterschiedlicher Block K_n von 48 Schlüsselbits aus dem 56-bit-Schlüssel (KEY) ausgewählt:

$$K_n = KS(n, KEY),$$

wobei

- n die Nummer der jeweiligen Iteration ist ($1 \leq n \leq 16$)
- KS die in 5.5 definierte Funktion KS ist, welche die Teilschlüsselfolge festlegt
- K_n der 48-bit-Block ist, der in der n -ten Iteration der Berechnung benutzt wird, die in 5.2.3.1 spezifiziert ist.

5.2.4 Abschließende Permutation

Das am Ende der Berechnung nach 5.2.3 erzeugte Ergebnis VE wird durch die Permutation IP^{-1} (inverse Permutation zu IP, siehe Tabelle 2) umgeformt, d.h. das Endergebnis hat Bit 40 von VE als erstes Bit, Bit 8 von VE als zweites, etc. und schließlich Bit 25 von VE als letztes Bit. Der zu dem 64 bit langen Eingabeblock gehörende verschlüsselte Block ist also $IP^{-1}(R_{16} L_{16})$.

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
Tabelle 2. Inverse Initialpermutation IP^{-1}							

5.3 Entschlüsselungsalgorithmus

5.3.1 Berechnungsschritte

Der Algorithmus für die Entschlüsselung ist der gleiche wie der in 5.2 definierte mit der Abweichung, daß die Folge der Werte K_n umgekehrt wird. Der Algorithmus besteht also aus den folgenden Schritten:

- Eine Initialpermutation IP des zu entschlüsselnden Eingabeblocks von 64 bit.
- 16 Iterationen beginnend mit dem permutierten Eingabeblock wie in 5.2.3.1 spezifiziert, aber mit dem Unterschied, daß die Werte K_n in der Reihenfolge $K_{16}, K_{15}, \dots, K_1$ benutzt werden. Nach der 16. Iteration werden die linke und rechte Hälfte des Ergebnisblocks $VE = R_0 L_0$ vertauscht.
- Eine abschließende Permutation IP^{-1} , die zu der Initialpermutation invers ist.

5.3.2 Entschlüsselung als inverse Operation zur Verschlüsselung

Bei der Anwendung des Verschlüsselungsalgorithmus nach 5.2 auf einen