

Informationsverarbeitung
**Betriebsarten für einen
 64-bit-Blockschlüsselalgorithmus**
 Identisch mit ISO/DIS 8372 Ausgabe 1985

DIN
ISO 8372

Information processing; Modes of
 operation for a 64 bit block cipher
 algorithm
 Identical with ISO/DIS 8372 edition 1985

Einsprüche bis 31. Oktober 1985
 Anwendungswarnvermerk auf der
 letzten Seite beachten!

Das internationale Schriftstück ISO/DIS 8372, Ausgabe 1985-06-13, "Information processing; Modes of operation for a 64 bit block cipher algorithm", 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 8372, 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 8372 liegt hiermit in deutscher Übersetzung vor. Die im Abschnitt 8 genannten vier zusätzlichen Alternativen bedürfen nach Meinung des Ausschusses 20 des NI aus Konsistenzgründen noch weiterer Diskussionen im internationalen Gremium SC 20.

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. Inwieweit hierdurch die Möglichkeit der nationalen Normung beeinträchtigt ist, wird zur Zeit durch das DIN geklärt. Auf internationaler Ebene sind die Ermittlung der Patenthalter sowie Verhandlungen mit der Firma Burroughs noch nicht abgeschlossen.

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

Fortsetzung Seite 2 bis 16

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 – Betriebsarten für einen
64-bit-Blockschlüsselungsalgorithmus

Inhalt

	Seite
1 Zweck und Anwendungsbereich	3
2 Verweisungen auf andere Normen	3
3 Begriffe	4
4 Bezeichnungen	4
5 ECB-Betriebsart (Elektronisches Codebuch)	6
6 CBC-Betriebsart (Geheimtextblockverkettung)	6
7 CFB-Betriebsart (Geheimtextrückführung)	7
8 Bevorzugte Parameterwahl für die CFB-Betriebsart	10
9 OFB-Betriebsart (Schlüsseltextrückführung)	12
ANHANG – Die Eigenschaften der Betriebsarten	14

1 Zweck und Anwendungsbereich

1.1 Diese Norm beschreibt vier Betriebsarten für jeden beliebigen 64-bit Blockschlüsselungsalgorithmus mit geheimem Schlüssel. Im Anhang werden Eigenschaften dieser Betriebsarten beschrieben, jedoch ist der Anhang nicht Teil der Norm.

Anmerkung: Die beschriebenen Betriebsarten sind insbesondere anwendbar auf den Algorithmus DEA 1, der im Norm-Entwurf DIN ISO 8227 beschrieben ist.

1.2 Diese Norm gibt zu jedem 64-bit-Blockschlüsselungsalgorithmus vier verschiedene Betriebsarten an, um für jede Anwendung (z.B. Datenübertragung, Datenspeicherung, Authentikation) eine geeignete Betriebsart zur Verfügung zu stellen. Die Norm enthält die Festlegungen der Betriebsarten sowie Hinweise zur Festlegung geeigneter Parameterwerte.

Anmerkung: Bei der Betriebsart Geheimtextrückführung ("Cipher Feedback" (CFB) (siehe 7)) werden zwei Parameter j und k , bei der Betriebsart Schlüsseltextrückführung ("Output Feedback" (OFB)) wird ein Parameter j verwendet. Wird eine dieser Betriebsarten benutzt, müssen diese Parameterwerte festgelegt werden und von allen kommunizierenden Partnern in der festgelegten Weise benutzt werden.

2 Verweisungen auf andere Normen

DIN ISO 8227, Informationsverarbeitung – Datenverschlüsselung – Festlegung des Algorithmus DEA 1, z. Z. noch Entwurf.

3 BEGRIFFE

3.1 Klartext: Unverschlüsselte Information.

3.2 Geheimtext: Verschlüsselte Information.

3.3 Blockverkettung: Eine Verschlüsselung von Information, bei der jeder Geheimtextblock sowohl vom entsprechenden Klartextblock als auch vom vorhergehenden Geheimtextblock abhängt.

3.4 Initialisierungswert (IV): Ein Wert, der zur Festlegung des Anfangszustands des Verschlüsselungsverfahrens benötigt wird.

3.5 Startvariable (SV): Eine Variable, die aus dem Initialisierungswert abgeleitet wird. Sie wird zur Definition des Anfangszustandes bei der jeweiligen Betriebsart des Verschlüsselungsverfahrens benötigt.

Anmerkung: Verfahren zur Ableitung der Startvariablen aus dem Initialisierungswert werden in dieser Norm nicht festgelegt. Sie müssen in den Anwendungen dieser Norm beschrieben werden.

3.6 Kryptographische Synchronisation: Die Koordination des Verschlüsselungs- und Entschlüsselungsverfahrens.

4 BEZEICHNUNGEN

In dieser Norm wird die funktionale Abhängigkeit, die durch das Blockschlüsselungsverfahren gegeben ist, wie folgt bezeichnet:

$$C = e_K(P).$$

Dabei ist P der Klartextblock, C der Geheimtextblock und K der Schlüssel. Der Ausdruck e_K steht für die Operation der Verschlüsselung mit Hilfe des Schlüssels K.

Die zugehörige Entschlüsselungsfunktion wird wie folgt geschrieben:

$$P = d_K(C).$$

Mit Großbuchstaben bezeichnete Variablen, wie z.B. C und P, stellen eindimensionale Felder von Bits dar, z.B. sind

$$A = (a_1, a_2, \dots, a_m) \quad B = (b_1, b_2, \dots, b_m)$$

Felder von m Bits, die von links mit 1 bis m nummeriert sind.

Die Operation der Addition modulo 2, auch als 'exclusives Oder' bekannt, wird hier mit dem Symbol $\oplus$ bezeichnet. Bei Feldern wird diese Operation definiert durch:

$$A \oplus B = (a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_m \oplus b_m).$$

Die Auswahloperation für die ersten j Bits von A wird wie folgt bezeichnet:

$$A \sim j = (a_1, a_2, \dots, a_j).$$

Diese Operation ist nur definiert, wenn $j \leq m$ ist.

Im folgenden wird ein Schiebefunktion definiert:

$$S_k(X|F) = (x_{k+1}, x_{k+2}, \dots, x_m, f_1, f_2, \dots, f_k).$$

Dabei ist X eine m-bit-Variable, F eine k-bit-Variable mit $k \leq m$ und das Ergebnis $S_k(X|F)$ ist wieder eine m-bit-Variable. Die Wirkung dieser Funktion ist eine Linksverschiebung um k Stellen in dem Feld X, wobei die ersten k Bits von X verlorengehen, während in die rechts freigewordenen Stellen das Feld F eingesetzt wird.

Eine im folgenden benutzte Anwendung dieser Funktion geht von der l-bit-Variablen $I(l)$ aus, deren Elemente sämtlich 1 sind. Die Variable C von j bit ($j \leq l$) wird von rechts in das Feld geschoben:

$$S_j(I(l)|C) = (1, 1, \dots, 1, c_1, c_2, \dots, c_j).$$

Es verbleiben noch $l-j$ 'Einsen' im Ergebnisfeld.