Grundlagen von Datenverschlüsselungssystemen und Stand der Normungsarbeiten

Autor(en): **Widmer, W. R.**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **77 (1986)**

Heft 1

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-904135

Grundlagen von Datenverschlüsselungssystemen und Stand der Normungsarbeiten

W.R. Widmer

Bitstromchiffrierung, Blockchiffrierung und Public-Key-Systeme sind die heute für den Datenschutz im Vordergrund stehenden Verfahren. Die internationale Standardisierungsorganisation ISO befasst sich seit 1981 mit der Normung und dem Einsatz von Algorithmen zur Datenchiffrierung. Zurzeit existieren Normenentwürfe für einen Chiffrieralgorithmus (DEA 1) und dessen Anwendung zur Chiffrierung und Authentisierung sowie Vorschläge für weitere Authentisieralgorithmen. In Vorbereitung sind zudem Public-Key-Systeme und Verfahren zur Schlüsselverteilung.

Le chiffrement à courant de bits ou par blocs et les systèmes de codes publics sont les procédés les plus actuels de protection des données. L'Organisation Internationale de Normalisation (ISO) s'occupe depuis 1981 de la normalisation et de l'utilisation d'algorithmes pour chiffrer des données. Il y a déjà des projets de normes pour un algorithme de chiffrement (DEA 1) et ses utilisations pour chiffrer et authentifier, ainsi que des propositions pour d'autres algorithmes d'authentification. En préparation sont des systèmes de codes publics et procédés de répartition des codes.

Adresse des Autors
Walter R. Widmer, GRETAG Aktiengesellschaft, Althardstrasse 70, 8105 Regensdorf.

1. Einleitung

Stetig zunehmende Speicherkapazitäten, dichtere Datennetze und schnellere Informationsverarbeitung haben zu einer explosionsartigen Vermehrung der gespeicherten Daten geführt. Beinahe jede erdenkliche Information ist irgendwo auf der Welt gespeichert und kann über internationale Datennetze abgerufen werden. Keine Frage, dass ein grosser Teil dieser Informationen für die Eigentümer einen beachtlichen Wert darstellen, denn deren Sammeln war schwierig, aufwendig oder sogar gefährlich. Andere Daten, z.B. persönlicher Natur, sind für gewisse Organisationen sehr wertvoll und müssen aus Gründen des Personenschutzes geheimgehalten werden. Informationseigentümer sind bedroht durch:

- Preisgabe vertraulicher oder klassifizierter Daten,
- Diebstahl von Daten,
- Modifikation von Daten.

Gegenmassnahmen sind:

- Einschliessen der Daten, Zugriff beschränken,
- Verschlüsseln der Daten,
- Überprüfen der Echtheit der Daten.

Diese Gegenmassnahmen beziehen sich auf alle Lebensphasen, d.h. auf die Speicherung, die Verarbeitung und Übermittlung der Daten. Während diese bei der Speicherung und Verarbeitung durch physikalische Isolation, Zugriffsschutz und kryptographische Methoden gesichert werden können, sind für die Sicherung der Übertragung nur kryptographische Methoden einsetzbar. Es ist deshalb sinnvoll, die wesentlichen Eigenschaften der in Frage kommenden Verfahren zu diskutieren.

2. Grundlegende Verfahren

2.1 Kryptographische Algorithmen

Ein kryptographischer Algorithmus definiert die Operation, die einen Klartext in ein Kryptogramm transformiert. Die am weitesten verbreitete Methode ist die Substitutionschiffrierung. In ihrer ursprünglichen Form, wie sie Cäsar eingesetzt hat, werden Buchstaben nach einer festen Tabelle durch andere ersetzt. Solche Kryptogramme können natürlich einfach gebrochen werden, da sich die Statistik des Klartexts direkt auf die des Kryptogramms überträgt. Um diese Attacke zu verunmöglichen, kann entweder das zugrunde gelegte Alphabet vergrössert werden oder die Substitutionstabelle nach jedem Schritt verändert werden. Diese beiden Entwicklungsrichtungen haben zu den beiden heute wichtigsten Verfahren Blockchiffrierung und Bitstromchiffrierung geführt.

2.2 Bitstromchiffrierung

Dieses heute am weitesten verbreitete Chiffrierverfahren ersetzt Bit für Bit einer Meldung, indem es ein von einem Chiffriergenerator erzeugtes Bit zu dem der Meldung addiert (modulo-2-addition). Es kann gezeigt werden, dass diese Chiffrierung perfekt, also absolut sicher ist, wenn das vom Chiffriergenerator erzeugte Chiffrierprogramm (Key stream) keinerlei Gesetzmässigkeiten aufweist. In der Realität wird das Chiffrierprogramm jedoch von einem Automaten in Funktion eines relativ kurzen Schlüssels erzeugt; es enthält demzufolge starke Abhängigkeiten. Wie in Figur 1 dargestellt, wird ein zwischen zwei Partnern vereinbarter Schlüssel verwendet, um den Algorithmus oder die Schaltungsanordnung sowie die Initialstellung der beiden Chiffriergeneratoren zu bestimmen. Davon ausgehend wird das Chiffrierprogramm erzeugt, eine Binärsequenz mit einer dem Klartext entsprechenden Länge. Die Sicherheit des Verfahrens ist durch die Erkennbarkeit der inneren Gesetzmässigkeiten bestimmt. Sie kann anhand von wenigen, allerdings nicht immer ein-

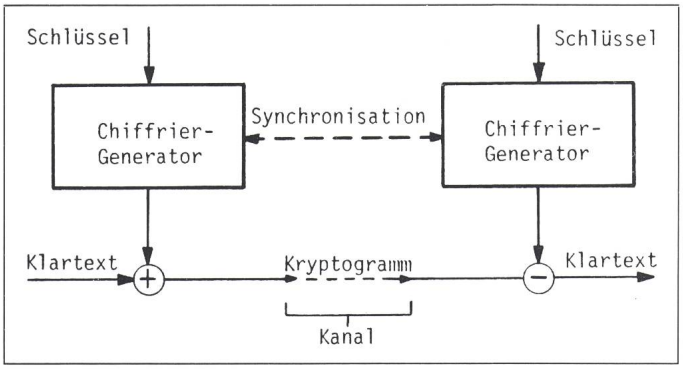


Fig. 1
Bitstromchiffrierung

fach bestimmbaren Charakteristika, abgeschätzt werden:

- *Periode* des Chiffrierprogramms: Anzahl Bits, die produziert werden können, bevor sich das Chiffrierprogramm wiederholt. Eine Wiederholung soll auch bei extremen oder unwahrscheinlichen Einsatzfällen ausgeschlossen sein.
- *Schlüsselmannigfaltigkeit:* mögliche Anzahl verschiedener Schlüssel; sie muss genügend gross sein, dass eine Attacke durch Absuchen aller Möglichkeiten aussichtslos ist.
- *Rekursionslänge:* Jede periodische Folge gehorcht einem Rekursionsgesetz. Die Spannweite des Rekursionsgesetzes nennt man die Rekursionslänge. Ist das Rekursionsgesetz linear, so müssen zur Bestimmung desselben lineare Gleichungen gelöst werden. Dies ist nicht unmöglich, ausser die Anzahl der Unbekannten sei überdimensional gross. Die Rekursionslänge der kürzesten linearen Rekursion, auch *lineare Komplexität* genannt, muss entsprechend gross gehalten werden.

2.3 Blockchiffrierung

Blockchiffrieralgorithmen transformieren Blöcke von Daten (64 bit oder mehr) auf einmal. Eine Transformationstabelle würde allerdings zu gross; die Abbildung erfolgt in einem schlüsselabhängigen Algorithmus (Figur 2). Die Tatsache, dass bei gleichem Schlüssel gleiche Klartextblöcke auch in gleiche Chiffratblöcke abgebildet werden, ist unbedenklich, da das Auftreten gleicher Klartextblöcke – jedenfalls bei statistisch gut verteiltem Klartext – unwahrscheinlich ist.

Blockchiffrieralgorithmen leiden unter der Tatsache, dass keine so präzisen Masse für die Sicherheit existieren, wie etwa die lineare Komplexität oder die Periode bei den Bitstromchiffrierverfahren. Für die Beurteilung der Sicherheit wichtige Masse sind die Schlüssellänge, die Kreuzkorrelation zwischen Klartext- und Kryptogrammblock sowie die Sensitivität des Kryptogrammblocks auf kleine Klartextänderungen. Prominentester Vertreter der Blockchiffrieralgorithmen ist der DEA1, der in einem späteren Kapitel behandelt wird.

2.4 Asymmetrische Chiffrierverfahren

Diese Verfahren, oft auch Public-Key-Systeme genannt, gehören zur Gruppe der Blockchiffrieralgorithmen, weisen aber einen wesentlichen Unterschied zu den klassischen (symmetrischen) Verfahren auf: Chiffrier- und Dechiffrierschlüssel sind nicht gleich, und einer kann nicht ohne Kenntnis der Erzeugungsparameter aus dem anderen abgeleitet werden.

Das heute bestbekannte Verfahren dieser Art wird nach dessen Erfindern *Rivest, Shamir* und *Adleman* RSA genannt. Jeder Teilnehmer erzeugt sich dabei aufgrund von speziell ausgewählten grossen Primzahlen einen Chiffrier- und einen Dechiffrierschlüssel. Die Berechnungsgrundlagen werden sodann vernichtet, der Dechiffrierschlüssel geheimgehalten und der Chiffrierschlüssel veröffentlicht. Nach dieser Initialisierung kann jedermann mit dem veröffentlichten Chiffrierschlüssel Meldungen chiffrieren, die nur der berechtigte Empfänger, nämlich der Besitzer des Dechiffrierschlüssels entziffern kann.

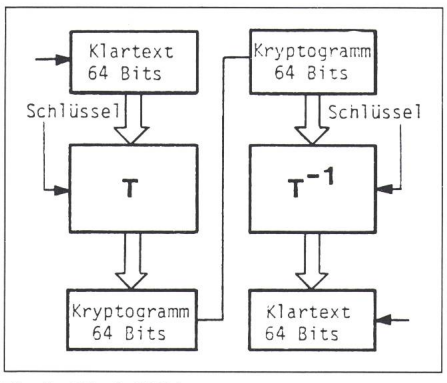


Fig. 2 Blockchiffrierung

Public-Key-Systeme scheinen auf den ersten Blick alle Probleme der Schlüsselverteilung zu lösen. In der Tat haben sie bestechende Eigenschaften; daneben treten aber weniger angenehme Nebenerscheinungen auf. So stellen sich Fragen der Identifizierung sowohl desjenigen, der einen Chiffrierschlüssel veröffentlicht, als auch desjenigen, der eine Meldung chiffriert (Authentisierung). Diese Probleme sind mit zusätzlichen Operationen lösbar. Etwas gravierender sind Probleme mit zu grossen Rechenzeiten. Die zu übertragende Meldung wird bei diesem Verfahren nämlich in etwa 500 bit lange Blöcke unterteilt, denen je eine ganze Zahl (aus einem endlichen Zahlenkörper) zugeordnet werden kann. Die Chiffrier- und Dechiffrieroperationen bestehen aus Exponentiationen dieser Zahlen. Diese Operationen können heute noch nicht mit vernünftigem Aufwand in den für die Datenübertragung notwendigen Geschwindigkeiten ausgeführt werden. Public-Key-Systeme können jedoch gut zur Schlüsselverteilung in konventionellen Chiffriersystemen eingesetzt werden. Wenn nicht allzuhäufig neue Schlüssel verteilt werden müssen, sind die Rechenzeiten ohne weiteres tragbar (z.B. 2 bis 3 Minuten auf einem IBM PC/XT).

3. Normung

1979 sahen die Mitglieder des technischen Kommittees TC 97 (Datenverarbeitung) der ISO (International Standards Organization) einen Bedarf für die Normung von Datenverschlüsselungsverfahren. In der Folge wurde eine Arbeitsgruppe aus Experten verschiedener Länder gebildet, mit dem Auftrag, folgende Themenkreise zu behandeln:

- Spezifikation eines Datenchiffrieralgorithmus,
- Methoden zur Anwendung der Chiffrierung in Datenverarbeitungsprotokollen,
- Richtlinien für den Einsatz der Chiffrierung, für das Gerätedesign und das Schlüsselmanagement.

1983 wurde die Arbeitsgruppe in das Subkommittee SC 20 (Data Cryptographic Techniques) umgewandelt. Der wesentliche Unterschied zur Arbeitsgruppe ist, dass darin die entspre-

chenden Organisationen der Mitgliederländer mit Stimmrecht pro Land vertreten sind und nicht Experten mit nur beratender Stimme. Die Schweiz ist mit der SNV-Gruppe 149/UK7 aktiv im SC20 vertreten. Der Verantwortungsbereich des SC20 wurde gegenüber der ursprünglichen Definition leicht erweitert und umfasst heute alle kryptographischen Techniken, insbesondere auch Public-Key-Systeme und Verfahren für die Authentisierung. Die eigentliche Bearbeitung der Themen erfolgt nicht im Subkommittee, sondern in drei Arbeitsgruppen (Working Groups), nämlich

- WG1: Secret key algorithms and their applications,
- WG2: Public key algorithms and their applications,
- WG3: The use of encipherment in the OSI architecture.

Im folgenden wird der Stand der Arbeiten in diesen drei Arbeitsgruppen dargelegt.

3.1 WG1: Algorithmen mit Geheimschlüssel

Als die ursprüngliche Arbeitsgruppe 1979 ihre Arbeit aufnahm, war das amerikanische Standardisierungsinstitut (ANSI) mit den Arbeiten am DES (Data Encryption Standard) bereits weit forgeschritten. Es lag deshalb auf der Hand, diesen Standard auch als internationale Norm vorzuschlagen. Vorsichtigerweise wurde eine kleine Namensänderung durchgeführt, und der Algorithmus wird nicht als *der* Standard, sondern als ein erster Blockchiffrieralgorithmus bezeichnet: DEA1 (Data Encryption Algorithm 1) [1]. Auf den Algorithmus muss hier nicht eingegangen werden, da er bereits mehrfach beschrieben und diskutiert wurde.

Es gibt auch heute im Stadium DIS (Draft International Standard) noch einige Stimmen, die keinen Sinn in der Normung eines Chiffrieralgorithmus sehen und sich auf Anwendungsnormen beschränken möchten. Diese werden durch Charakteristika des DEA1, wie etwa die geringe Schlüssellänge von nur 56 bit, unterstützt. Im weiteren fühlen sich die Europäer etwas benachteiligt, da nicht alle Entwicklungsgrundlagen offengelegt wurden und der Export von in den USA hergestellten integrierten Schaltungen von der Regierung stark eingeschränkt wird.

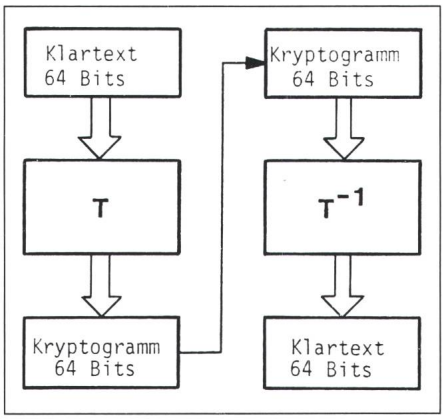


Fig. 3 ECB Electronic Code Book
T Verschlüsselung
T-1 Entschlüsselung

Bedeutend mehr Befürworter haben die Normen zur Anwendung eines Blockchiffrieralgorithmus. In [2] sind die vier Anwendungsarten beschrieben. Da sie für jeden Blockchiffrieralgorithmus mit Blocklängen von 64 bit Geltung haben und zudem eine wichtige Grundlage für den Einsatz der Chiffrierung in Datennetzen bilden, werden ihre wichtigsten Merkmale hier kurz beschrieben:

ECB Electronic Code Book (Fig. 3): Dies ist die grundlegende Betriebsart, in der ein Klartextblock der Länge 64 bit wie mit einer Tabelle (Codebuch) ohne weitere Verknüpfungen in einen anderen Block, den Chiffratblock, abgebildet wird. Solange der Schlüssel nicht verändert wird, werden deshalb Wiederholungen des Klartextes auch zu Wiederholungen im Chiffrat führen. Dieser Mode wird deshalb nicht für Datenchiffrierung, sondern für die Chiffrierung von Schlüsseln in Schlüsselverteilsystemen verwendet.

CBC Cipher Block Chaining (Fig. 4): In diesem Modus werden die aufeinanderfolgenden Blöcke verkettet, um den oben beschriebenen Nachteil zu beheben. Dem Kryptogramm wird ein zufälliger Initialvektor vorangestellt; die Chiffrierung der folgenden Blöcke wird dann von der Vorgeschichte abhängig gemacht, indem vor der Transformation zu jedem Klartextblock der vorangegangene Chiffratblock (bzw. der Initialvektor beim ersten Block) addiert wird. Der einzige kleine Nachteil dieses Verfahrens ist, dass sich die Folgen eines einzelnen Übertragungsfehlers auf zwei Blöcke ausdehnen.

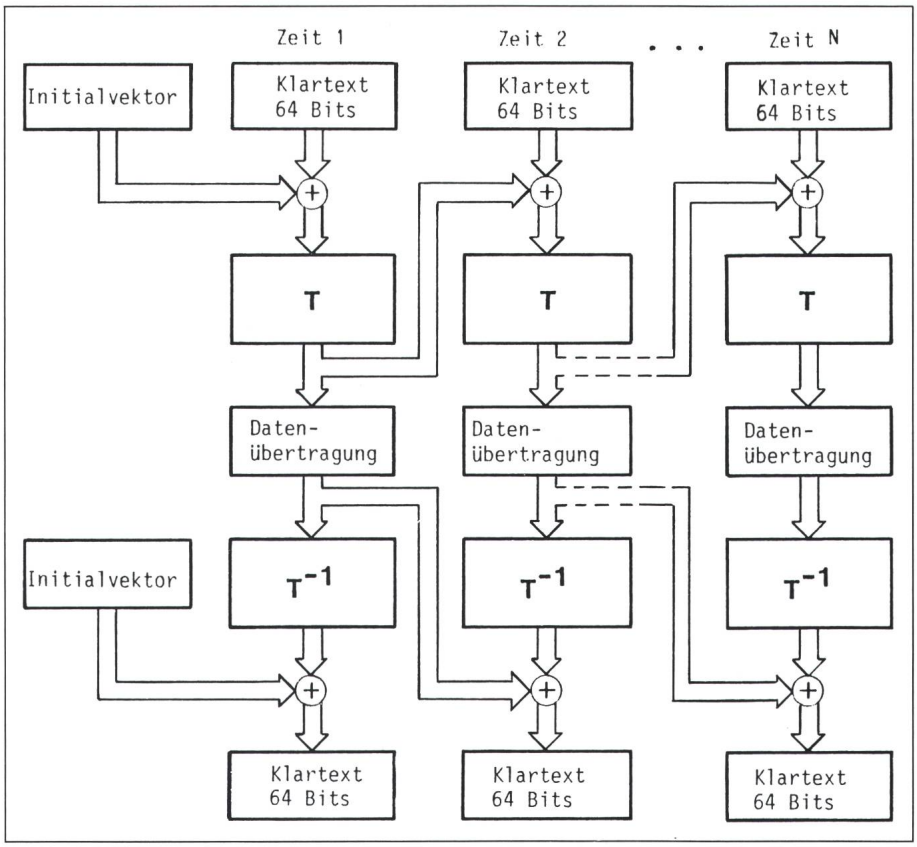


Fig. 4 CBC Cipher Block Chaining
T Verschlüsselung
T-1 Entschlüsselung
+ Exklusiv-OR

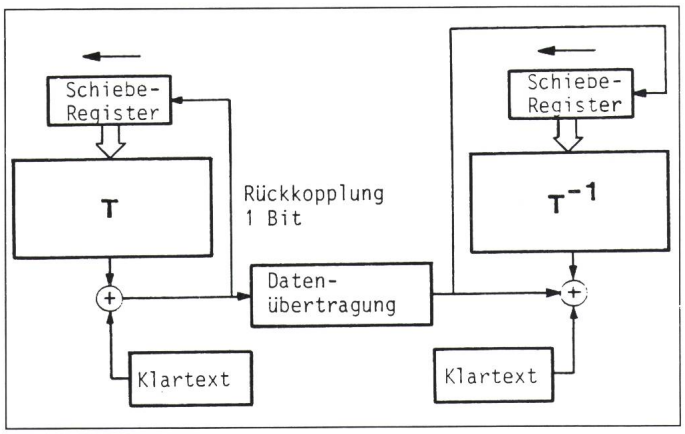


Fig. 5
CFB Cipher Feedback
T Verschlüsselung
T^{-1} Entschlüsselung

CFB Cipher Feedback (Fig. 5): In diesem Modus wird der Blockchiffrieralgorithmus eher im Sinne der Bitstromchiffrierung eingesetzt. Das Kryptogramm wird aus der Addition (modulo-2) des Klartexts mit dem Chiffrierprogramm gebildet. Sowohl auf der Sende- als auch auf der Empfangsseite wird laufend das Kryptogramm der jeweils letzten 64 bit in einem Schieberegister abgespeichert. Diese 64 bit werden mit dem Blockchiffrieralgorithmus transformiert. Aus dem Resultat wird ein bestimmtes bit ausgewählt und zum Chiffrieren verwendet. Dieses Verfahren hat den grossen *Vorteil,* dass *keine* Blocksynchronisierung zwischen den Partnern notwendig ist, denn die empfangende Maschine läuft innerhalb von 64 fehlerfreien bit automatisch ein. Ein Übertragungsfehler wirkt sich anderseits auch auf die folgenden 64 bit aus.

OFB Output Feedback (Fig. 6): In diesem Modus wird der Blockchiffrieralgorithmus genau wie ein autonomer Chiffriergenerator für die Bitstromchiffrierung eingesetzt, indem ausgehend von einem Initialvektor der transformierte Block jeweils wieder als Eingangsblock für die nächste Transformation verwendet wird. Der transformierte Block wird gleichzeitig als Chiffrierprogramm für die Chiffrierung modulo-2 verwendet.

Aufgabe der WG1 ist es auch, Algorithmen für die Authentisierung zu normen. Ein Entwurf dafür wurde von einem anderen ISO-Kommittee (TC68, Banking) ausgearbeitet [3]. In einem Vorschlag wird der DEA1 als Authentisierungsalgorithmus eingesetzt [4], die anderen beiden Vorschläge [5] und [6] enthalten neue Algorithmen, die sich besser für Softwareimplementationen eignen.

3.2 WG2: Algorithmen mit öffentlichem Schlüssel

Die Arbeitsgruppe, die sich mit asymmetrischen oder Public-Key-Systemen beschäftigt, hat sich vor gut einem Jahr gebildet und kann sich nicht auf irgendwelche nationalen Normen abstützen. Das Ziel der Arbeitsgruppe ist die Standardisierung von Verfahren, welche die aus der Literatur bekannten Public-Key-Algorithmen verwenden. Ein Bedarf für solche Verfahren existiert vor allem in den Gebieten

- Schlüsselverteilung für konventionelle (symmetrische) Chiffriersysteme,
- Authentisierung von «Smart cards»,
- Authentisierung von Zahlungsmeldungen,
- Anruferidentifikation in öffentlichen Datennetzen.

Neben diesen anwendungsorientierten Fragen oder den Fragen der Sicherheit der in Frage kommenden Algorithmen muss auch die Patentlage untersucht werden, denn die Normung patentierter Verfahren bedingt eine genaue Abklärung der Bereitschaft des Patentinhabers zur Lizenz unter vernünftigen Bedingungen. Nach all den Vorabklärungen ist die Arbeitsgruppe der Ansicht, dass das System nach RSA der geeignetste Kandidat für eine Normung ist. Die Arbeitsgruppe plant, im Juli 1986 einen ersten Normentwurf fertiggestellt zu haben.

3.3 WG3: Einsatz der Chiffrierung in Datennetzen

Chiffrieralgorithmen oder die Betriebsarten eines Blockchiffrieralgorithmus sagen noch nichts über deren Einsatzweise in Datennetzen aus. Diese wird bestimmt durch die Antwort auf die Frage, welche Information auf welchen Verbindungen geschützt werden soll. Damit befasst sich die Arbeitsgruppe WG3 anhand des Architekturmodells für offene Systeme (OSI, Open Systems Interconnection). In diesem Modell werden die Aufgaben jedes Datenend-, Übermittlungs- oder Vermittlungsgerätes in Ebenen aufgeteilt: zuunterst die physikalische Schnittstelle, dann die Linksteuerung, die Vermittlungssteuerung, die Transport- und die End-zu-End-Kontrolle sowie die höheren Protokolle zur Steuerung einer Session, der Darstellung und der Applikation.

In einfachen Worten kann gesagt werden, dass ein Benützer, der seine Daten möglichst kurz nach der Erfassung bis kurz vor der Verarbeitung (oder auch von der Verarbeitung bis zur Ausgabe usw.) geschützt haben möchte, in einer möglichst hohen Ebe-

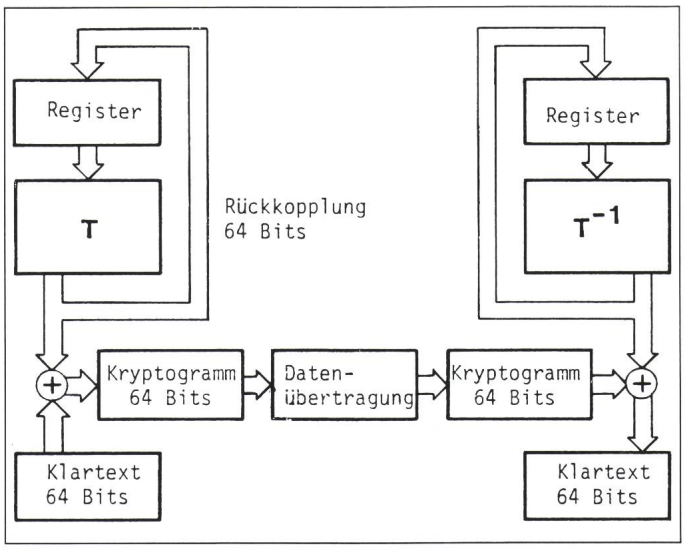


Fig. 6
OFB Output Feedback
T Verschlüsselung
T^{-1} Entschlüsselung

ne, einer der benützerorientierten Schichten des 7-Schichten-Modells chiffrieren sollte. Der Betreiber eines Datennetzes hingegen wird die Daten möglichst benützerunabhängig in einer der drei unteren Schichten chiffrieren. Ausnahmen von diesem Grundsatz rühren daher, dass

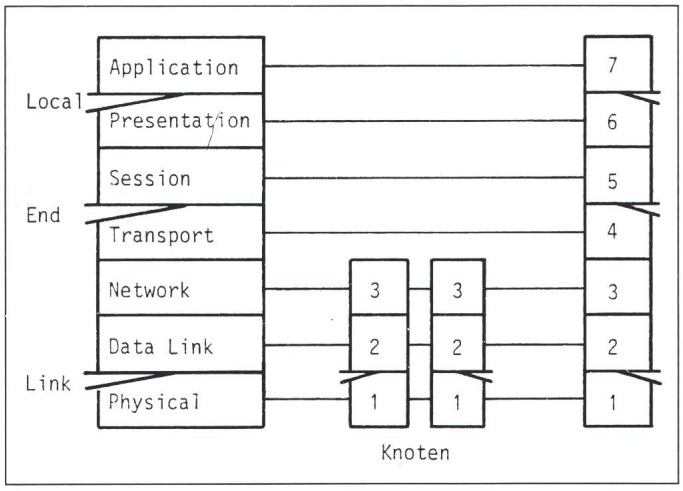
- die Chiffrierung in tieferen Ebenen meistens einfach realisierbar ist, da sie keine Eingriffe in bestehende höhere Protokolle notwendig macht,
- die Chiffrierung in tiefen Ebenen nicht nur die Information selbst, sondern auch Herkunft, Ziel und Verkehrshäufigkeit vor Analyse schützt,
- in tieferen Sichten Stand-alone-Chiffriergeräte eingesetzt werden können, die eine einfachere, von der Datenverarbeitung trennbare Sicherheitsorganisation erlauben.

Diese Gründe haben dazu geführt, dass sich der am weitesten fortgeschrittene Normenentwurf [7] mit der Chiffrierung auf der physikalischen Ebene befasst. Durch Anwendung des oben beschriebenen CFB-Modus wird nach dieser Norm jedes Bit chiffriert. Damit wird höchste Sicherheit auch bezüglich Meldungsstruktur und Häufigkeit erreicht. Das Verfahren ist jedoch nur auf Einzelstrecken, Mietleitungen oder leitungsvermittelten Wählnetzen einsetzbar.

Soll eine Chiffrierung von einem Teilnehmer zu einem anderen über ein meldungs- oder paketvermitteltes Netz erfolgen, so dürfen nur die reine Information, nicht aber die für die Netzsteuerung notwendigen Daten (z.B. Adressen) chiffriert werden. Bezogen auf das Architekturmodell (Fig. 7) heisst das, dass über der Ebene 3, also über den Link- und Vermittlungsprotokollen chiffriert werden muss. Gegenwärtig befasst sich die WG3 deshalb mit Chiffrierung in der Ebene 4. Der Blockchiffrieralgorithmus wird dabei im beschriebenen CBC-Modus verwendet. Für die genaue Einbettung der Chiffrierung in das ISO-Modell [8; 9] sind jedoch noch einige Fragen zu klären. Ein weiterer Bedarf besteht auch nach Chiffrierung in der Ebene 6 - dies würde erst lokale Sicherung der Daten zur Ablage auf Massenspeichern erlauben.

Das Subcommittee SC 20 wird sich im Januar 1986 treffen und dann von den Resultaten der Ende November 1985 stattfindenden Abstimmung über den Algorithmus DEA1 sowie über dessen Anwendungsarten Kenntnis nehmen. Es werden dann weitere Vorschläge entsprechend der oben beschriebenen Aufgabenstellung der drei Arbeitsgruppen zur Diskussion vorliegen.

Fig. 7
Chiffrierung im OSI Modell



Literatur

[1] ISO/DIS 8227: Information Processing—Data Encipherment—Specification of algorithm DEA1.
[2] ISO/DIS 8372: Information Processing—Modes of operation for a 64-bit block cipher algorithm.
[3] ISO/DIS 8730: Banking—Requirements for standard message authentication.
[4] ISO/DIS 8731: Banking—Approved Algorithms for message authentication, Part 1: DEA 1.
[5] ISO/DIS 8732: Banking—Approved Algorithms for message authentication, Part 2: MAA.
[6] ISO/DIS 8733: Banking—Approved Algorithms for message authentication, Part 3: DSA.
[7] ISO/DP 9160: Information Processing—Data Encipherment—Physical layer interoperability requirements.
[8] ISO 7498: Information Processing—Open Systems Interconnection—Reference Model.
[9] ISO 7498/DADX: Addendum to ISO 7498 on Security Architecture.