Gerd Kuchelmeister

Sichere Kommunikation und Authentifizierung in einem Hochschulnetz

Diplomarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783832465513

Gerd Kuchelmeister

Sichere Kommunikation und Authentifizierung in einem Hochschulnetz

Diplom.de

Gerd Kuchelmeister

Sichere Kommunikation und Authentifizierung in einem Hochschulnetz

Diplomarbeit
an der Fachhochschule Ravensburg-Weingarten
Januar 2002 Abgabe

Diplom.de

Diplomica GmbH
Hermannstal 119k
22119 Hamburg

Fon: 040 / 655 99 20
Fax: 040 / 655 99 222

agentur@diplom.de
www.diplom.de

ID 6551

ID 6551
Kuchelmeister, Gerd: Sichere Kommunikation und Authentifizierung in einem Hochschulnetz
Hamburg: Diplomica GmbH, 2003
Zugl.: Weingarten, Fachhochschule, Diplomarbeit, 2002

Diplomica GmbH
http://www.diplom.de, Hamburg 2003
Printed in Germany

INHALTSVERZEICHNIS

1. EINLEITUNG

1.1 Einführung

Bis zum Jahr 1993 war das Internet ein fast reines Forschungsnetz.
Aber in den letzten Jahren hat sich dieses Netz rasant zu einem weltweiten Informations- und Kommunikationsmedium entwickelt, dass Unternehmen, Behörden und Privatpersonen gleichermaßen nutzen.
Die Zahl der Internetanwender steigt expotentiell, wobei das Medium immer mehr gesellschaftliche Bedeutung bekommt.
Alleine in Deutschland sind derzeit 30 Mio. Menschen online.
Das Handelsvolumen betrug 2001 alleine in den USA 170.000.000.000 $.
2002 wird sich laut Voraussagen von Forrester Research diese Volumen verdoppeln.

Bei den meisten, die über einen Zugang zu diesem Netz verfügen, beschränken sich die Kenntnisse über die Anwendungsmöglichkeiten auf Electronic Mail und Informationssuche. Selbst mehr oder weniger erfahrenen Nutzern bis hin zu Informatikern fehlen zum Teil das Hintergrundswissen und die genaue Funktionsweise des neuen Mediums.

Da das Internet ein öffentliches Medium wie das Telefonnetz ist, birgt es gewisse Gefahren des Missbrauchs, speziell auch der Wirtschaftsspionage, die die Unternehmen weltweit im Jahr mehrere Millionen Euro kosten.
Um dieser neuen Form der Kriminalität entgegen zu wirken, wird der Schrei der Nutzer, egal ob private Anwender oder Firmen, nach Sicherheit immer lauter.

Viele Internet-Produkt-Hersteller haben den Markt erkannt und maßgeschneiderte Lösungen auf ihre Produkte aufgesetzt, die dann aber gar nicht oder nur teilweise untereinander kompatibel waren.
Daher hat die Internet Society ihrer Internet Engineering Task Force IETF den Auftrag gegeben, ein Sicherheits-Protokoll zu entwickeln, auf der die Hersteller mit ihren Produkten aufsetzen können, sodass die Kunden auf herstellerspezifischen Lösungen nicht mehr angewiesen sind.
Es entstand IPSec, das in dieser Diplomarbeit noch ausführlich erklärt wird.

1.2 Aufgabenstellung

THEMA:

Sichere Kommunikation und Authentifizierung in einem Hochschulnetz.

BESCHREIBUNG:

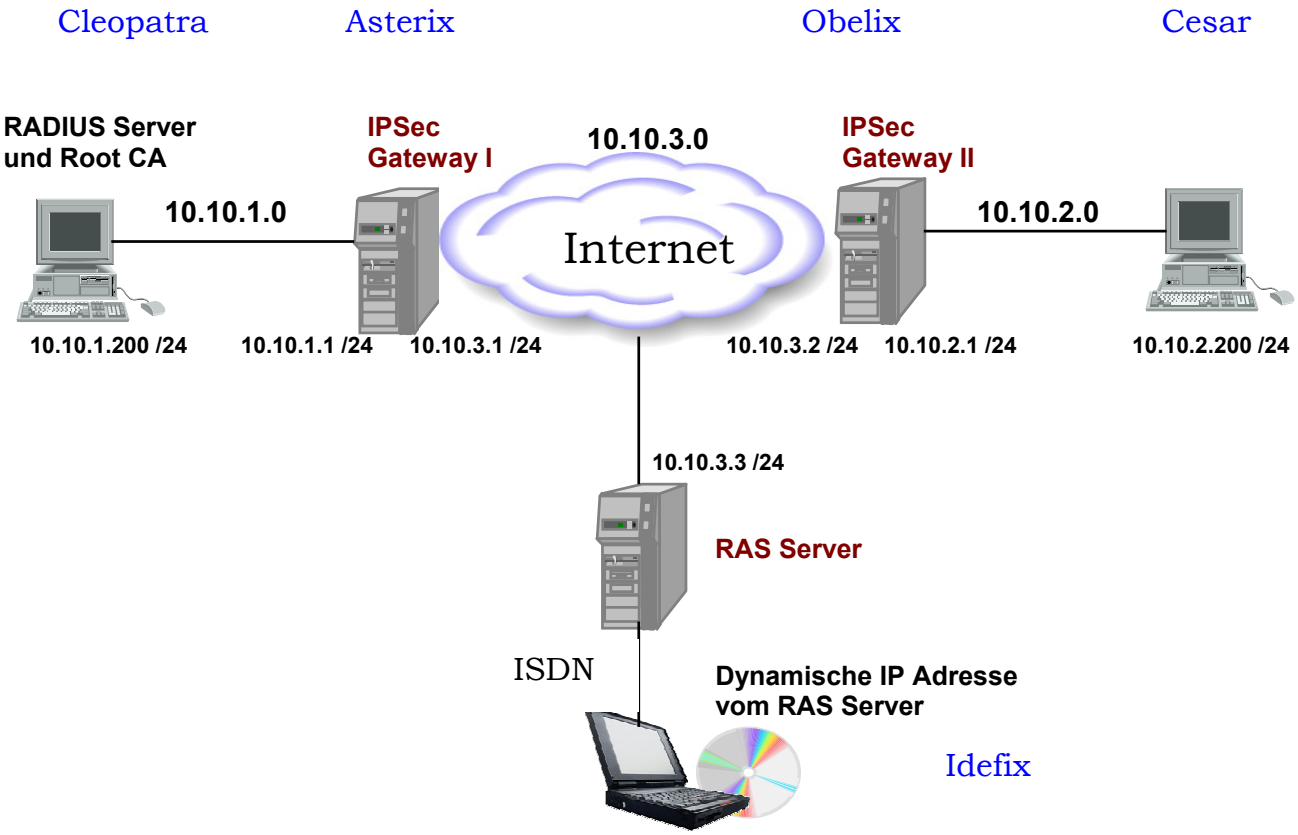
Ziel dieser Diplomarbeit ist es mit Hilfe von modernen Verschlüsselungsmethoden und einer zeitgemäßen Authentifizierung das Hochschulnetz abzusichern, wobei hier auch sichere Kommunikation mit E-Mail gewährleistet sein soll.
Weiterhin soll für die Verbindungen zu anderen Netzen, ein Tunnel durchs Internet aufgebaut werden. Dieses Thema wird ausführlich behandelt und ist Schwerpunkt dieser Diplomarbeit.
Es soll auch eine Lösung für eine sichere Einwahl vom Internet in ein privates Netz gefunden werden.

AUFGABEN:

- Installation eines Testnetzes und Einarbeitung in die Grundlagen der Kryptographie.
- Verschlüsselung des netzinternen Datenverkehrs mit Hilfe von IPSec.
- Aufbau eines Tunnels durchs Internet mit IPSec.
- IPSec Authentifizierung soll mit geteilten Schlüsseln und mit X.509 Zertifikaten erfolgen.
- Sichere E-Mail mit digitaler Signatur und Verschlüsselung durch Smartcard.
- Sichere Remote Einwahl in ein privates Netz.
- Ausführliche Dokumentation und Auswertung der Arbeiten.

1.3 Testnetztopologie und Arbeitsmittel

1.3.1 Testnetz



Beschreibung: **Abb. 1.3.1.1**

Die Netze 10.10.1.0 und 10.10.2.0 sind über das Internet verbunden, dass hier mit dem Netz 10.10.3.0 simuliert wird.
Die beiden Gateways dienen als Tunnelendpunkte für die beiden Netze.
Der Rechner mit der dynamischen IP Adresse soll sich in eines der beiden Netze über den RAS Server einwählen können.
Auf dem Client mit der IP Adresse 10.10.1.200 soll ein RADIUS Server und eine Root CA installiert werden. Der RADIUS Server dient zur Bereitstellung von Passwörtern, mit dem ein Rechner am RAS Server einen Zugang erhält. Die Root CA arbeitet als Trustcenter, mit dem X.509 Zertifikate ausgestellt werden können, die zur Authentifizierung von IPSec von den beiden Gateways benötigt werden. Die Zertifikate werden auch für die Signatur und Verschlüsselung von E-Mails verwendet.

1.3.2 Arbeitsmittel

- 6 x PC, 2 davon mit 2 NIC.
- Chipkartenleser und Smartcard von GEMPLUS.
- 1 x HUB.
- diverse Kabel.
- Microsoft Windows 2000 Advance Server und Windows 2000 professional.
- Vasco RADIUS Server Software und Hardwaretoken.
- ISDN Nebenstellenanlage mit Kabel.
- 2 x ISDN Fritzkarte.

1.3.3 Installation des Test Netz

Das Netz wurde wie in **Abb. 1.3.1.1** aufgebaut. Auf Asterix, dem RAS Server und Cleopatra ist Windows 2000 Advance Server installiert, auf Obelix und Cesar ist Windows 2000 Professional installiert.
Nach der Installation der Betriebssysteme wurden die Rechner vernetzt und konfiguriert.

Wie in Abb. 5.1.1 zu sehen, funktionieren Asterix und Obelix als Security Gateways d.h. sie sind auch als Router tätig.
Daher muss auf beiden Rechnern IP Forwarding eingeschaltet werden.
Diese kann man unter Windows 2000 mit dem Registrierungseditor konfigurieren.
Start -> Ausführen: „regedt32“ eingeben.
Danach öffnet sich der Editor.

Im Eintrag
HKEY_LOKAL_MASCHINE/SYSTEM/SERVICES/Tcpip/Parameters den Wert **IPEnableRouter** auf **1** ändern.

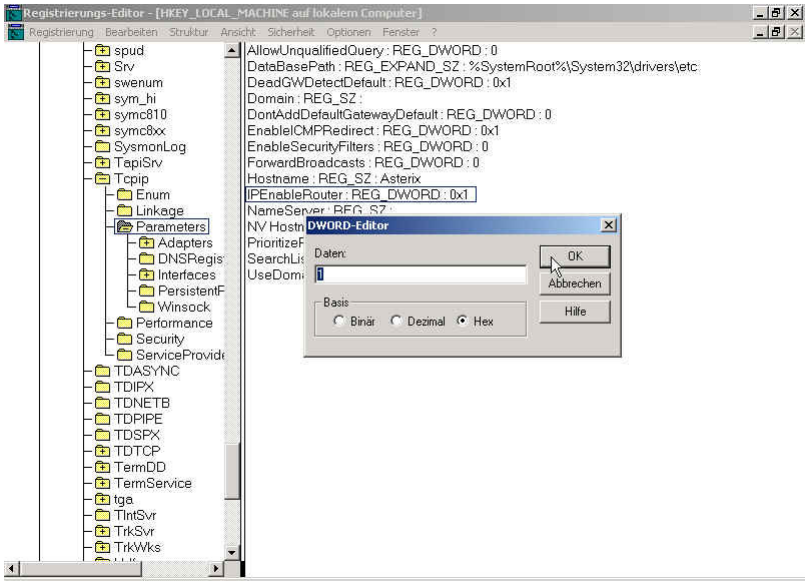


Abb. 1.3.3.1

Den Registrierungseditor dann wieder schließen und mit **Start -> Ausführen: „cmd“** eine Konsole öffnen.
Hier **„ipconfig /all“** eingeben.
Es muss nun folgende Ausgabe erscheinen.

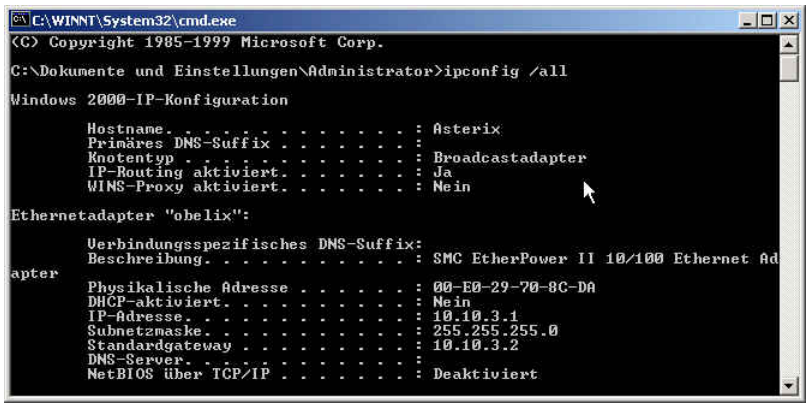


Abb. 1.3.3.2

Die Netzwerkkarten der Rechner müssen folgendermaßen konfiguriert werden. Die Konfigurationen können dann mit **Start -> Ausführen: „cmd“** Eingabe: **„ipconfig“** dargestellt werden.

Asterix:

```
Windows 2000-IP-Konfiguration
Ethernetadapter "Netz 10.10.3.0":
        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.3.1
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 10.10.3.2
Ethernetadapter "Netz 10.10.1.0":
        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.1.1
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . :
```

Obelix:

```
Windows 2000-IP-Konfiguration
Ethernetadapter "Netz 10.10.3.0":
        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.3.1
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 10.10.3.2
Ethernetadapter "Netz 10.10.1.0":
        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.1.1
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . :
```

Cleopatra:

```
Windows 2000-IP-Konfiguration
Ethernetadapter "Netz 10.10.1.0":
        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.1.200
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 10.10.1.1
```

Cesar:

```
Windows 2000-IP-Konfiguration
Ethernetadapter "Netz 10.10.2.0":
        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.2.200
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 10.10.2.1
```

Wenn die Netzwerkkarten so konfiguriert wurden, kann man die Verbindung zwischen Cesar und Cleopatra mit **Start -> Ausführen: „cmd“** Eingabe: **„ping 10.10.1.200“** überprüfen.

2. GRUNDLAGEN UND GLOSSAR

2.1 Verschlüsselung

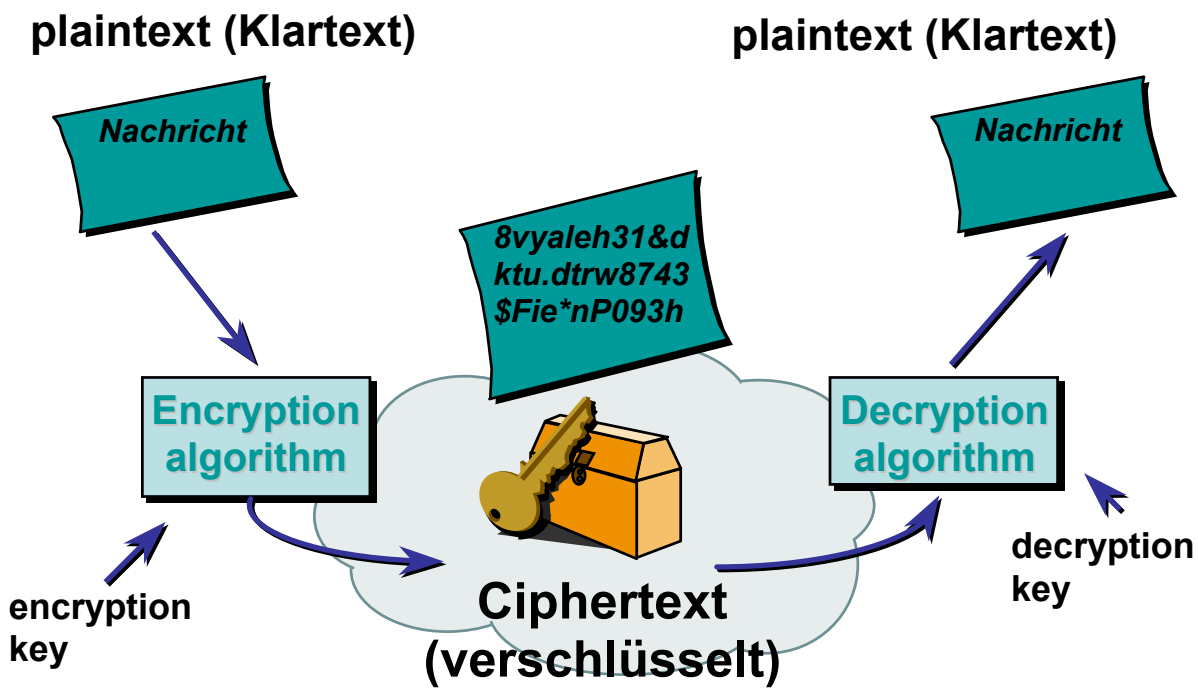


Abb. 2.1.1

2.2 Verschlüsselungsarten

Bei Verschlüsselungsalgorithmen ist der Schlüssel ein erforderlicher Parameter.
Der Algorithmus generiert zusammen mit dem Schlüssel aus dem Klartext den verschlüsselten Text.
Hierbei ist ganz wichtig, dass die Sicherheit eines Verfahrens nicht vom Algorithmus, sondern nur alleine vom Schlüssel abhängen darf.
Der nachfolgende Bericht aus der c't belegt dieses.

Die beiden israelischen Kryptologen Alex Biryukov und Adi Shamir haben Medienberichte zufolge den Verschlüsselungsalgorithmus geknackt, der GSM-Handy-Telefonate auf der Funkstrecke zur Mobiltelefon-Basisstation schützt.
Eines zeigen die Vorfälle um die GSM-Verschlüsselungsalgorithmen A5/1 und A5/2 aber schon jetzt deutlich: Der Versuch, Krypto-Verfahren geheim zu halten, dient nicht der Sicherheit.
Das hat anscheinend auch die GSM-Association gelernt: Ihr Sicherheitsdirektor James Moran äußerte dem Online Magazin Wired gegenüber, dass man künftige Algorithmen von vorneherein offen legen will, um der Fachwelt eine Prüfung zu ermöglichen. (n1/c't)

Es gibt zwei grundlegende Verschlüsselungsarten.

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

2.3 Symmetrische Verschlüsselung

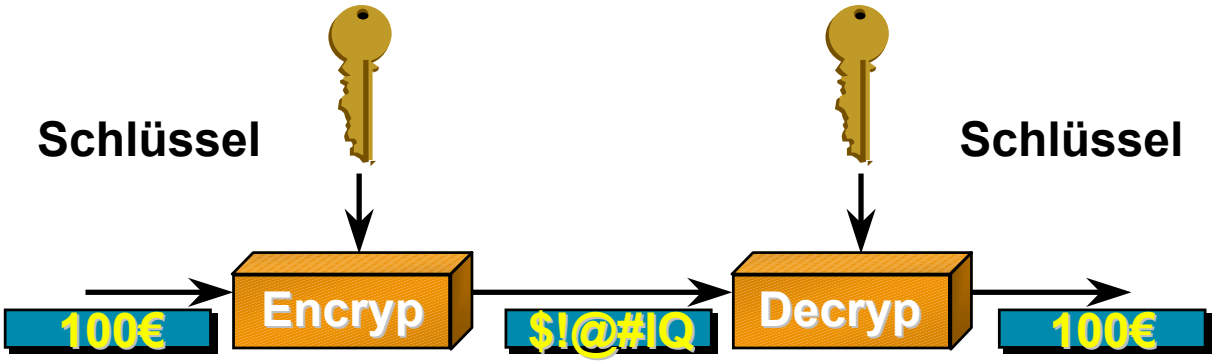


Abb. 2.3.1

Bei der synchronen Verschlüsselung, besitzen Sender und Empfänger den gleichen Schlüssel. Schlüssellängen gewöhnlich von 40-256 Bit.

Die mathematischen Funktionen der Ver- und Entschlüsselung:

E: Verschlüsselungsalgorithmus
D: Entschlüsselungsalgorithmus
K: Schlüssel
C: chipertext (Geheimtext)
M: plaintext (Klartext)

$$E_K(M)=C$$

$$D_K(C)=M$$

$$D_K(E_K(M))=M$$

Beispiele von symmetrischer Verschlüsselung sind DES, 3DES und AES. Der Vorteil eines symmetrischen Verschlüsselungsverfahrens liegt in der Geschwindigkeit, der Nachteil im Schlüsseltausch.

2.3.1 DES und 3DES

Bei DES und 3DES handelt es sich um den derzeit am meist benutzten symmetrischen Verschlüsselungsalgorithmus.
DES hat eine feste Schlüssellänge von 64 Bit, wobei nur 56 Bit benutzt werden.

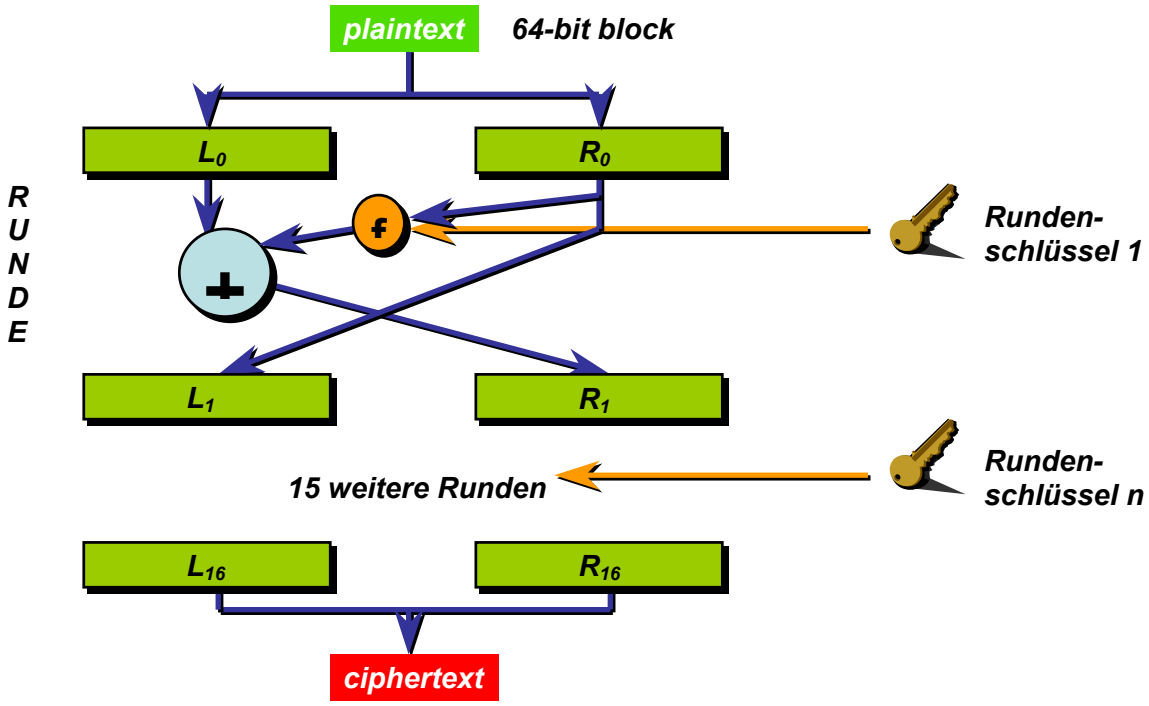


Abb. 2.3.1.1

Funktionsweise:

Die Nachricht wird in 64 Bit Blöcke geteilt, wobei diese wieder in eine linke und in eine rechte Hälfte mit 32 Bit geteilt wird (L_0 und $R_{0)}$
Die neue rechte Hälfte R_1 ergibt sich aus der $R_{0,}$ die über die Funktion f angewendet wird, in der als Parameter der Schlüssel der Runde n mit einwirkt und das Ergebnis mit der L_0 XOR- verknüpft wird.
Diese wird mit einer Rundenzahl von 16 wiederholt.

Die Funktion f

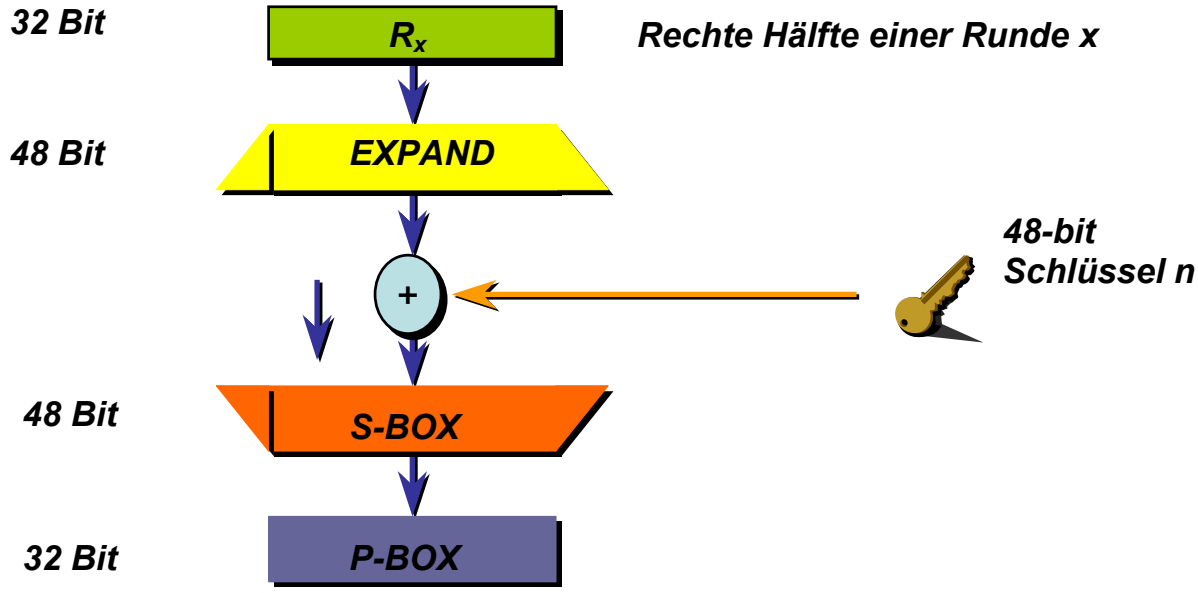


Abb. 2.3.1.2

Funktionsweise:

DES hat verschiedene Boxen, die Permutationen, Kompressionen, Expansionen und Verschiebungen ausführen.
Die Rechte Hälfte, die in die Funktion mit einfließt, wird auf 48 Bit expandiert.
Der 64 Bit Schlüssel wird auf 48 Bit komprimiert und dann XOR mit der Rechten Hälfte verknüpft.
Nun wird der Wert in die S-Box geschoben, die wieder einen 32 Bit Wert ausgibt.
Die S-Box ist der Teil von DES, der nicht linear ist, und somit die Sicherheit von DES ausmacht.
Es würde also nichts bringen, wenn man die Runden 16-mal durchläuft, denn es würde linear bleiben.
Nun wird mit der P-Box noch eine Permutation ausgeführt.
Jede Runde erhält einen neuen Schlüssel, der mit einem bestimmten Algorithmus von DES generiert wird.

Tripel DES

DES gilt heute als nicht mehr sicher. Daher wurde 3DES der Nachfolger. 3DES wendet DES dreimal hintereinander, mit zwei verschiedenen Schlüsseln, an.

Schema von 3DES

$$C=E_{K1}(D_{K2}(E_{K1}(M)))$$

Der Schlüsselraum erweitert sich somit auf 2^{112} was die Sicherheit erheblich erhöht.

2.3.2 AES

Da DES als nicht mehr sicher gilt, wurde von 1997 von NIST ein Nachfolger gesucht, der offen im Internet ausgeschrieben wurde.
Es wurden mehrere Wettbewerbe durchgeführt.
Gewonnen hat letztendlich die Blockchiffre Rijndael, die die Kriterien erfüllte.
AES ist seit Sommer 2001 als Standard anerkannt.

Kriterien

- Formal: AES muss eine symmetrische Blockchiffre sein, welche eine Blockgröße von 126 Bit und Schlüssellängen von 128, 192, 256 Bit arbeitet.
- Sicherheit: gegen Angriffe aller Art.
- Flexibilität: es soll erweiterbar sein.
- Effizienz: es soll effizienter als 3DES sein.
- Implementierung in Hardware und Software soll einfach sein.

Dieser Standard wird in nächster Zeit 3DES nach und nach ablösen.