Kryptographische Algorithmen

Stand: 11.05.2007

Ausgegeben von:

Rechenzentrum Hochschule Harz

Sandra Thielert

Hochschule Harz
Friedrichstr. 57 – 59
38855 Wernigerode
03943 / 659 – 900

Inhalt

Abkürzungen

AES	Advanced Encryption Standard
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
IDEA	Internet Data Encryption Algorithm
MAC	Message Authentication Code
MD	Message Digest
NIST	National Institute of Standards and Technology
NSA	National Security Agency
RC	Rivest Cipher
RIPEMD	Race Integrity Primitives Evaluation Message Digest
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm

1 Einleitung

Die Kryptographie will Nachrichten vor unbefugtem Zugriff schützen. Hierbei wird die Nachricht, mittels mathematischer Verfahren codiert, so das es für Drittpersonen keine Möglichkeit besteht bzw. nur mit größtem Aufwand verbunden ist die Nachrichten zu ändern. Moderne Verfahren der Kryptografie entstanden aus den Geheimcodes vergangener Jahrzehnte und wurden durch eine tiefgründigere Mathematik deutlich verbessert [Enterasys].

Für alle Verfahren gilt, je länger der erzeugte Schlüssel ist, je mehr mögliche Kombinationen entstehen und umso schwieriger ist es den Schlüssel zu erraten.

Für die Codierung gibt es 3 Verfahrensweisen, die symmetrische Verschlüsselung, die asymmetrische Verschlüsselung und die hybriden Verschlüsselungsverfahren.

Die eingesetzten kryptographischen Verfahren zur Verschlüsslung von Daten werden regelmäßig durch einen Kreis führender Experten geprüft. Ist abzusehen, dass ein mathematisches Verfahren an Sicherheitswert verliert, so wird die Eignungsfeststellung nicht mehr verlängert.

2 Symmetrische Algorithmen (Private Key Kryptographie)

Die symmetrischen Verschlüsselungsverfahren, auch bezeichnet als Single Key Kryptographie, sind einfache und schnelle Verfahren, bei denen zum Verschlüsseln und zum Entschlüsseln derselbe Schlüssel verwendet wird (Abbildung 1). Problem bei diesen Verfahren besteht in der sicheren Verteilung der Schlüssel, der Geheimhaltung der Schlüssel an 2 Stellen, bei Empfänger und Sender, der Ableitbarkeit der Schlüssel voneinander und der Nachweisbarkeit wer, Empfänger oder Sender, eine Nachricht unterschrieben hat.

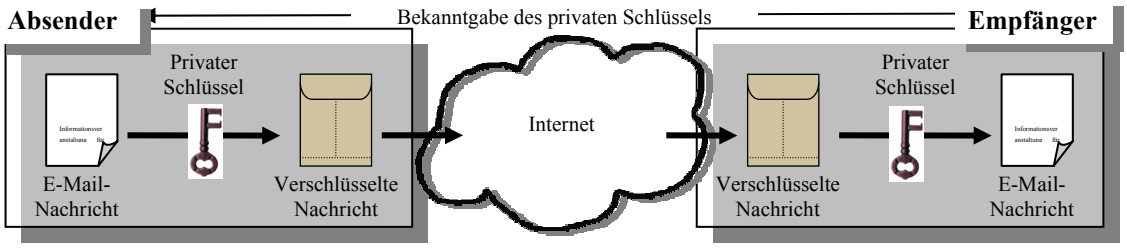

Abbildung 1: Symmetrische Verschlüsselung

Ein symmetrisches Verschlüsselungsverfahren wird als sicher anerkannt, wenn man aus dem verschlüsselten Text, mit unbekanntem Schlüssel den Klartext nicht ermitteln kann.

2.1 Rot n Verfahren

Das als Rot n bezeichnete Verfahren ist ein Vorfahr der heutigen Kryptographieverfahren und stammt aus den römischen Zeiten von Gaius Julius Cäsar. Hierbei werden alle Buchstaben des Textes um n Stellen im Alphabet verschoben. Beim Zurück verschieben ergibt sich der Klartext.

2.2 Vigenere-Chiffre (Vernam Chiffre)

Die Vigenere-Chiffre stammt aus dem 16. Jahrhundert und wurde von Blaise de Vigenere erfunden. Hierbei wird der Schlüssel dem Text so oft wie nötig zugeordnet. Danach werden die Buchstaben zur Verschlüsselung spaltenweise addiert mit A=0, B=1, C=2, ... Z=25.

Klartext	D i e s i s t e i n v e r s c h l u e s s e l t e r T e x t
Schlüssel (ALICE)	A L I C E A L I C E A L I C E A L I C E A L I C E A L I C E
Verschlüs-selter Text	D T M U M S E M K R V P Z U G H W C G W S P T V I R E M Z W

Tabelle 1: Verschlüsslung mit Vigenere - Verfahren

2.3 DES (Data Encryption Standard)

DES, auch bekannt unter dem Namen DEA (Data Encryption Algorithm), wurde 1970 bei IBM entwickelt und ist ein Blockchiffre-Verfahren, d.h. das die Daten in Blöcken von 64 Zeichen und einer Schlüssellänge von 56 bit verschlüsselt werden. Die Standardisierungsbehörde NIST (National Institut of Standards and Technology) hat dieses Verfahren 1977 als ein Standardverfahren für die Datenverschlüsselung anerkannt.

Da DES mittlerweile in die Jahre gekommen ist wurde es zu Triple-DES weiterentwickelt. Triple-DES verschlüsselt die 64 bit Datenblöcke durch eine dreimalige Ausführung von DES. Hierbei werden zwei 56 bit Schlüssel verwendet. Der Ablauf stellt sich folgendermaßen dar:

(1) Datenblöcke werden verschlüsselt mit Schlüssel 1
(2) Ergebnis wird verschlüsselt mit Schlüssel 2
(3) Ergebnis wird verschlüsselt mit Schlüssel 1

Durch die dreimalige Ausführung der DES Verschlüsselung erweitert sich der Suchraum auf $5 * 10^{33}$ mögliche Schlüssel.

2.4 IDEA (Internet Data Encryption Algorithm)

IDEA wurde 1990 von Xuejia Lai und James Massey in Zürich entwickelt und ist die erweiterte Version des DES – Algorithmus. Dieses Block-Chiffre-Verfahren verwendet eine Schlüssellänge von 128 bit.

2.5 RC4 (Rivest Cipher Nr.4)

Dieses Verfahren wurde 1978 von Ron Rivest entwickelt und basiert auf dem Konzept der Pseudozufallsgeneratoren und erreicht eine Schlüssellänge bis 2048 bit.

Ablauf:

(1)	Startwert auswählen	x
(2)	Generierung Schlüssel 1 durch	f(x)
(3)	Generierung Schlüssel 2 durch	f(f(x))
(4)	Generierung Schlüssel 3 durch	f(f(f(x)))

2.6 AES (Advanced Encryption Standard)

Dieses Verfahren wurde von John Daemen und Vincent Rijmen entwickelt und hat eine Schlüssellänge von 128 bis 256 bit

3 Asymmetrische Algorithmen (Public Key Kryptographie)

Bei den asymmetrischen Verschlüsselungsverfahren wird ein Schlüsselpaar erzeugt, mit einem öffentlichen und einem privaten Schlüssel. Mit dem öffentlichen Schlüssel, dem Public Key verschlüsselt der Absender die Nachricht und nur der Empfänger kann diese Nachricht lesen indem er die Nachricht mit seinem geheimen Schlüssel, Private Key entschlüsselt (Abbildung 2). Der Unterschied zwischen den beiden Schlüsseln ist nur auf die Verwendung des Schlüssels bezogen und auf die Person die diesen Schlüssel nutzen soll. Der Private Key soll vom Ersteller genutzt werden und muss geheimgehalten werden. Der öffentliche Schlüssel muss bekannt gegeben werden, so kann jeder eine verschlüsselte Nachricht an den Eigentümer senden.

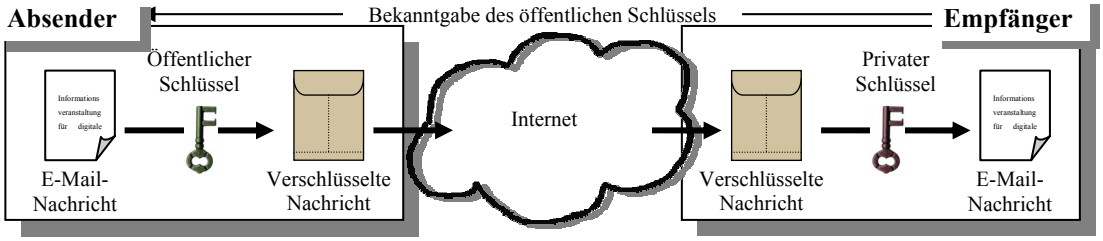

Abbildung 2: Asymmetrische Verschlüsselung

Sicher ist ein asymmetrisches Verfahren, wenn bei unbekanntem sowie auch bei bekanntem öffentlichen Schlüssel in eine Richtung keine Ver- bzw. Entschlüsslung vorgenommen werden kann [Richter]. Ebenfalls nach Richter gelten Schlüssellängen von 2048 bit bei asymmetrischen Verfahren zur Zeit als sicher.

Bei allen Verfahren zur asymmetrischen Schlüsselerzeugung besteht ein mathematischer Zusammenhang zwischen den Schlüsseln, aus diesem Grund haben diese Verfahren den Nachteil das sie sehr rechenaufwendig sind.

Weiterhin muss bei diesen Verfahren der öffentliche Schlüssel der Allgemeinheit zugänglich gemacht werden. Für die Authentisierung des Inhabers zum Öffentlichen Schlüssel werden Zertifikate, zur Bestätigung der Identität, genutzt. Die einzelnen Schritte zur Zertifizierung und Veröffentlichung der öffentlichen Schlüssel wird in einem weiteren Dokument namens „Public Key Infrastruktur“ noch genauer erläutert.

3.1 Diffie-Hellmann

Der Diffie-Hellmann-Algorithmus war das erste asymmetrische Verfahren und wurde 1976 von Whitfield Diffie und Martin Hellmann entwickelt.

Funktionsweise:

Schritt 1)	Auswahl einer Primzahl	n
Schritt 2)	Auswahl Zahl g	$g<n$ und $g \in N$
Schritt 3)	Auswahl Zahl x (von Absender)	$x<n$
Schritt 4)	Auswahl Zahl y (von Empfänger)	$y<n$
Schritt 5)	Absender berechnet	$g^x \pmod n = A$
Schritt 6)	Absender schickt Empfänger	A
Schritt 7)	Empfänger berechnet	$g^y \pmod n = B$
Schritt 8)	Empfänger schickt Absender	B
Schritt 9)	Absender berechnet aus B	$B^x \pmod n = K1$
Schritt 10)	Empfänger berechnet aus A	$A^y \pmod n = K2$

K1 und K2 sollten gleich sein und wird als K bezeichnet. Diese Zahl K kann jetzt als Schlüssel verwendet werden.

3.2 RSA (Rivest, Shamir, Adleman)

RSA wurde 1978 von Ronald Rivest, Fiat Shamir und Leonard Adleman veröffentlicht und nach ihnen benannt. Dieses Verfahren basiert auf dem mathematischen Verfahren der Primfaktorzerlegung großer Zahlen. Die Schlüssellänge beträgt 1024 – 2048 bit.

Ablauf:

(1)	A wählt 2 große Primzahlen	p & q
(2)	A bildet n aus	$n = p * q$
(3)	A wählt Schlüssel e mit der Bedingung	e teilerfremd zu $(p - 1) * (q - 1)$
(4)	A berechnet Schlüssel d mit	$d = e^{-1} \pmod{(p - 1) * (q - 1)}$

Der öffentliche Schlüssel wird bestimmt von e und n, der Private Schlüssel von d und n. Wenn B eine Nachricht an A senden will, so verschlüsselt er die Nachricht nach der folgenden Formel 1.

$$\text{Verschlüsselte Nachricht} = \text{Nachricht}^{e} \pmod{n}$$

Formel 1

A hat die Nachricht von B erhalten und kann diese mit der nachfolgenden Formel 2 wieder lesbar machen.

$$\text{Nachricht} = \text{Verschlüsselte Nachricht}^{d} \pmod{n}$$

Formel 2

4 Hybride Verschlüsselungsverfahren

Bei diesem Verfahren werden asymmetrische und symmetrische Verfahren kombiniert, um die Nachteile der beiden Verfahren auszuschließen. Die eigentliche Nachricht wird mittels einem symmetrischen Verfahren verschlüsselt. Zur Bestätigung der Authentifizierung wird das Dokument digital Signiert, erläutert im Abschnitt 4.2, und zur Gewährleistung der Unveränderlichkeit wird eine Prüfsumme, beschrieben im Abschnitt 4.1, von der Nachricht gebildet. Die Prüfsumme wird mit einem asymmetrischen Verfahren verschlüsselt. Im Abschnitt 4.3 ist der Gesamtablauf in einer Grafik anschaulich dargestellt.

4.1 Kryptographische Prüfsummen

Prüfsummen sind Hashfunktionen, auch Message Digest (MD) oder Message Authentication Code (MAC) genannt. Sie sollen die Echtheit bzw. Unveränderlichkeit einer Nachricht sicherstellen. Diese Prüfsummen müssen den folgenden Anforderungen entsprechen:

- Aufgrund einer Prüfsumme darf der zugrundliegende Text nicht ermittelbar sein
- Prüfsummen sollten eine Länge von 128 – 160 Bit besitzen
- Jedes Bit der Nachricht beeinflusst die Prüfsumme, daher sollte es unmöglich sein mehrere Nachrichten mit der selben Prüfsumme zu finden bzw. die Änderung spiegelt sich in der Prüfsumme wieder
- Eine Hashwert darf nicht umkehrbar sein, sonst könnten Dokumente aufgrund des Hashwertes angelegt werden

Ablauf:

1. Berechnung eines Hashwertes für das Dokument das verschlüsselt werden soll.
2. Verschlüsselung des Hashwertes mit dem privatem Schlüssel.
3. Versendung des Dokumentes
4. Empfänger dekodiert den verschlüsselten Hashwert mit dem öffentlichen Schlüssel des Absenders.
5. Empfänger erstellt Hashwert für das verschlüsselte empfangene Dokument
6. Vergleich der Hashwerte, wenn beide übereinstimmen ist das Dokument gültig.

MD2

Dieses Verfahren wurde von Ron Rivest entwickelt und ist eines der ältesten Prüfsummenverfahren mit einer Länge von 128 bit.

MD4

Dieses Verfahren wurde ebenfalls von Ron Rivest entwickelt.

MD5

MD5 ist eine Weiterentwicklung von MD4. Dieser Algorithmus erstellt aus einer Nachricht einen 128 bit langen Hashwert. Die Nachricht wird in Blöcken von 512 bit, die wiederum aufgeteilt sind in 16 Teilblöcken mit einer Länge von 32 bit, verarbeitet.

SHA

Dieses Verfahren wurde als Standard von der NIST und der NSA verabschiedet. Die erzeugte Prüfsumme ist 160 Bit lang, das Verfahren beruht auf einem ähnlichen Prinzip wie MD5.

RIPEMD-160

RIPEMD-160 ist ein europäisches Verfahren, entstanden aus dem Projekt RACE, mit einer gebildeten Prüfsumme von 160 Bit.

4.2 Digitale Signaturen

Digitale Signaturen, digitale Unterschriften, sollen die Echtheit eines Dokumentes anhand der Authentizität des Verfassers sicherstellen. Hierbei sollten folgende Anforderungen erfüllt sein:

- Nicht fälschbar
- Überprüfbare Echtheit
- Keine Übertragbarkeit auf andere Dokumente
- Nicht Änderbar

Ablauf nach [Weissleder]:

1. Signierung der Nachricht mit dem privaten Schlüssel
2. Verschlüsselung der unterschriebenen Nachricht mit dem öffentlichen Schlüssel des Empfängers
3. Empfänger entschlüsselt die Nachricht mit seinem privaten Schlüssel.
4. Empfänger prüft die Signierung mit dem öffentlichen Schlüssel des Senders.

4.3 Zusammenfassung

In diesem Abschnitt wird noch mal zur Verdeutlichung der Ablauf eines hybriden Verfahrens zur Verschlüsselung anhand einer Grafischen Darstellung (Abbildung 3) verdeutlicht.

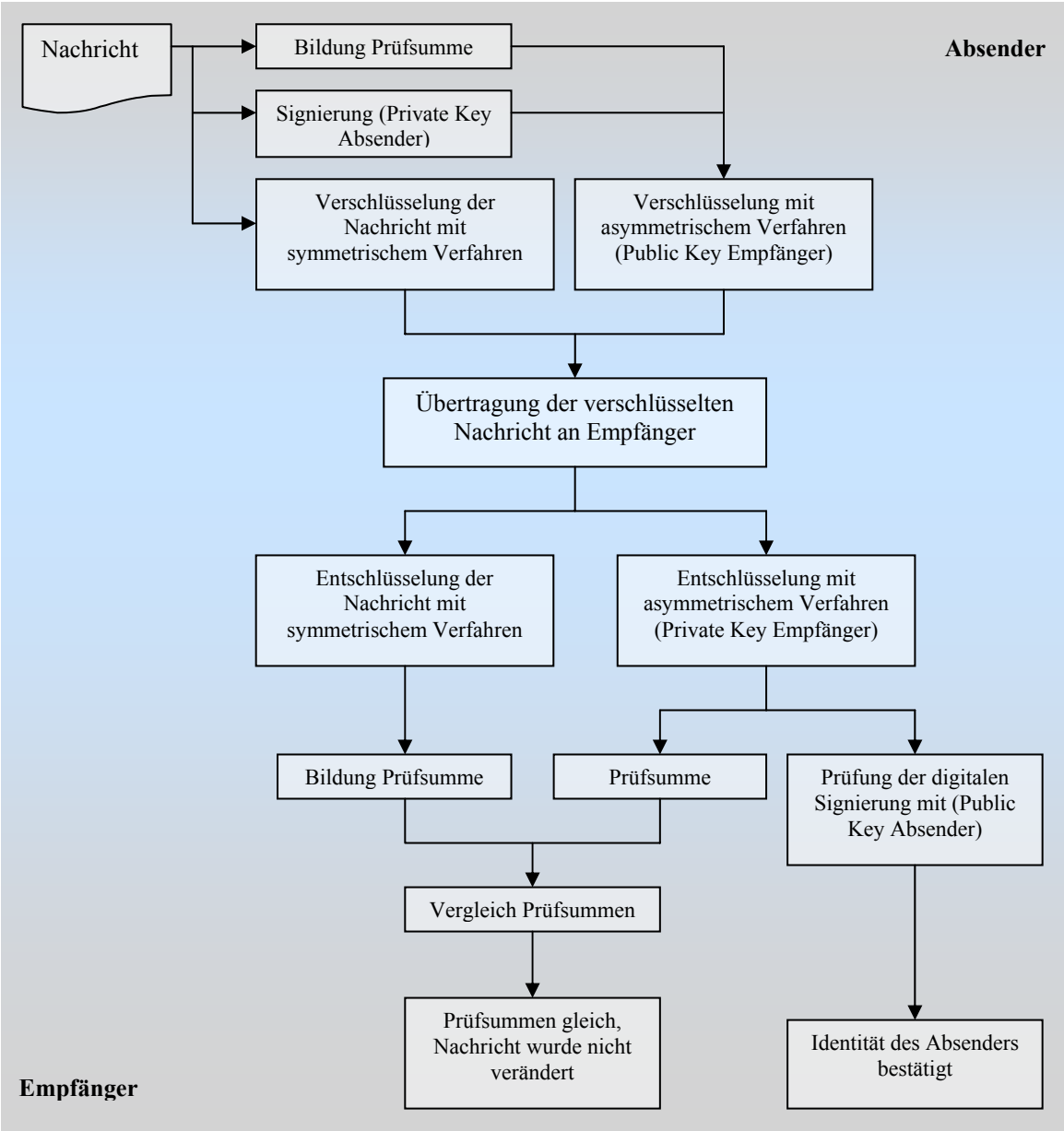

Abbildung 3: Darstellung Verschlüsselung einer Nachricht mit Prüfsumme und Digitaler Signatur

Literatur

[Richter] Richter, Helmut: Verschlüsselung im Internet. Leibnitz-Rechenzentrum München, 06.03.2002, http://www.lrz-muenchen.de/services/security/pki/

[Weissleder] Weissleder, Stephan: digitale Signaturen. Humboldt-Universität Berlin, WS 2001/02

[Enterasys] Enterasys Networks; Jahrbuch Kommunikationsnetze. Addison-Wesley, München 2002.