Kryptographie

Guido Ehlert

LK Informatik 13/Thomae

Einstein-Gymnasium Potsdam

Februar 2002

Inhaltsverzeichnis

1 Definition

Die Kryptographie ist nach [1] die zusammenfassende Bezeichnung für die Methoden zur Verschlüsselung (Chiffrierung) und Entschlüsselung (Dechiffrierung) von Information. Die Wissenschaft der Kryptographie ist die Kryptologie, welche auch bezeichnet wird als Lehre von der Entwicklung und Bewertung von Verschlüsselungsverfahren zum Schutz von Daten. Die Kryptologie gilt heute als Teilgebiet der Informatik, weist aber enge Beziehungen zur Mathematik auf.

2 Notwendigkeit von Kryptosystemen

Kryptosysteme sind immer dann nötig, wenn Informationen jeglicher Art geheim zu halten sind. Besondere Bedeutung hat hierbei die Übermittlung von geheimen Daten über potenziell unsichere Verbindungen, z.B. per Telefon, Funk oder über das Internet. Um hier zu gewährleisten, dass wirklich nur der rechtmäßige Empfänger die Nachricht liest, muss diese kryptographisch verschlüsselt werden.

3 Geschichtliche Entwicklung

Die Möglichkeit, geheime Nachrichten verschicken zu können, beschäftigt die Menschen schon sehr lange. Den ersten Ansatz eines kryptographischen Verfahrens nutze man wahr-

scheinlich in Sparta vor etwa 2500 Jahren mit der sogenannten Skytale. Ihr Prinzip ist sehr einfach: Der zu verschlüsselnde Text wird auf einen Streifen Papier geschrieben und dieser um eine Rolle gelegt. Liest man nun die Buchstaben ≫quer≪, ergibt sich eine andere, scheinbar sinnlose, Reihenfolge. Verfügt der Empfänger über eine Rolle des gleichen Durchmessers, kann der die Nachricht umgekehrt wieder entschlüsseln.

Auch der römische Kaiser Julius Caesar soll in seinen Briefen kryptographische Methoden verwandt haben. Er verwendete dabei sogenannte Schiebechiffren, wobei jedem Buchstaben des Klartext-Alphabetes genau ein anderer Buchstabe zugeordnet wurde. Im einfachsten Fall legt man einfach zwei Reihen identischer Alphabete untereinander und verschiebt die unterste Reihe um k Stellen. So erhält man eine simple Verschlüsselungstabelle. Die verschiedenen Varianten dieser Verschlüsselung werden auch als Cäsaren bezeichnet.

Der Franzose Blaise de Vigenère veröffentlichte 1586 eine neue Art der Chiffrierung. Hierbei wird zur Verschlüsselung statt wie bei Caesar einer einzelnen Zahl eine sich wiederholende Zeichenfolge als Schlüssel verwendet. Mit Hilfe des sogenannten Vigenère-Quadrats, das alle 26 Verschiebungen des Alphabets enthält, wird dann Buchstabe für Buchstabe chiffriert. Das Vigenère-Verfahren gilt auch heute noch als sicher, sofern der Schlüssel genauso lang ist wie der Klartext (One-Time-Pad). Die Vigenère-Chiffre zählt zu den polyalphabetischen Chiffrierungen.

Abbildung 1: Die Enigma

In den 1920er-Jahren wurden mit sog. Rotormaschinen Verfahren entwickelt, um die Verschlüsselung zu automatisieren. Die Maschine bestand aus verschiedenen Walzen und Rotoren, deren Anordnung ständig geändert wurde. Auch die im Zweiten Weltkrieg eingesetzte Chiffriermaschine ENIGMA gehörte zu dieser Art.

Doch bereits Ende des 19. Jahrhunderts begründete der niederländische Philologe Kerckhoffs von Nieuwenhof die moderne Kryptographie, indem er bekundete, dass sich die Sicherheit eines Verfahrens nicht auf die Geheimhaltung des Algorithmus, sondern ausschließlich auf die Geheimhaltung des Schlüssels gründen darf. Diese Erkenntnis ist bis heute gültig.

Ende der 1970er Jahre wurde der Data Encryption Standard (DES) veröffentlicht, der darauf beruht, nicht nur einzelne Zeichen, sondern ganze Blöcke zu chiffrieren. Durch ein einigermaßen geplantes Durcheinanderwürfeln (Substitution) ist eine recht unknackbare Verschlüsselung möglich.

In ihrer Arbeit ≫New directions in cryptography≪ thematisierten die Wissenschaftler W. Diffie und M. Hellman 1976 die Suche nach Alternativen zu bestehenden Verfahren und erfanden mit der Public-Key-Kryptographie ein asymmetrisches Verfahren zur Verschlüsselung. Mehr dazu im Abschnitt über asymmetrische Kryptoverfahren weiter unten.

4 Grundlegende Begriffe

Klartext Der Klartext bezeichnet den ursprünglichen Text, der die zu übertragende Information beinhaltet. Der Inhalt des Textes ist für jeden ersichtlich.

Geheimtext Wird der Klartext durch ein Kryptosystem verschlüsselt, entsteht als Resultat der Geheimtext. Durch die Verschlüsselung ist der Inhalt dieses Textes nicht zu erkennen. Durch entsprechende Verfahren wird der Geheimtext beim Empfänger der Nachricht wieder entschlüsselt. Der Empfänger hat dann wieder den Klartext vorliegen.

Schlüssel Bei der Mehrzahl der Verschlüsselungsverfahren gibt der Schlüssel an, wie der Klartext chiffriert bzw. der Geheimtext dechiffriert werden soll. Nur mit Hilfe des Schlüssels kann eine Ver- oder Entschlüsselung stattfinden. Welche Schlüssel konkret zum Einsatz kommen wird im letzten Abschnitt beschrieben.

symmetrische Verfahren Bei den symmetrischen Verschlüsselungsverfahren wird für die Ver- und Entschlüsselung der gleiche Schlüssel benutzt. Sender und Empfänger müssen also im Besitz des Schlüssels sein, aber gleichzeitig sicherstellen, dass kein Dritter den Schlüssel kennt. Ein einfaches symmetrisches Krypto-Verfahren ist jenes, welches bereits Cäsar nutzte und nach ihm benannt wurde.

asymmetrische Verfahren Bei den asymmetrischen oder Public-Key-Verfahren werden für Ver- und Entschlüsselung jeweils unterschiedliche Schlüssel verwendet. Dieser Ansatz geht davon aus, dass jede Person, die verschlüsselte Nachrichten empfangen will, zwei Schlüssel besitzt: einen privaten und einen öffentlichen. Möchte nun jemand einen Text an diese Person schicken, verschlüsselt er diesen mit dem öffentlichem Schlüssel des Empfängers. Dieser kann den Text dann mit seinem privaten Schlüssel dechiffrieren. Der private Schlüssel ist dabei nur dem Empfänger bekannt. So ist es möglich, dass jeder Texte an diese Person verschlüsseln, aber nur diese Person allein sie auch wieder entschlüsseln kann. Ein sehr wichtiges asymmetrisches Verfahren ist RSA.

5 Sicherheitsanforderungen an Kryptosysteme

1. Die Sicherheit eines Systems darf nicht von dessen Geheimhaltung, sondern ausschließlich von der Schlüssellänge abhängen
2. Der Krypto-Algorithmus sollte nachvollziehbar sein (offene Quellen)
3. Die Länge des Schlüssels sollte so groß wie möglich sein
4. Der geheime Schlüssel darf nicht weitergegeben werden
5. Die Echtheit des Senders muss zweifelsfrei feststehen (digitale Signatur), um der Nachricht vertrauen zu können

6 Allgemeine Funktion von Kryptosystemen

6.1 symmetrische Verfahren

Symmetrische Verfahren tragen ihren Titel, weil zur Ver- und Entschlüsselung der gleiche Schlüssel benutzt wird – Ver- und Entschlüsselung laufen quasi symmetrisch zueinander ab.

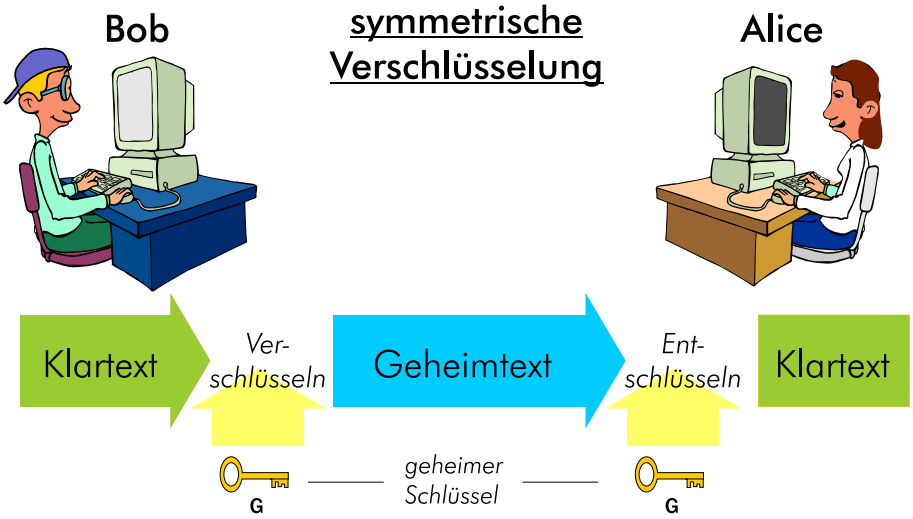

Abbildung 2: Prinzip symmetrischer Krypto-Verfahren

Soll eine Nachricht über ein symmetrisches Verfahren codiert werden, so müssen zunächst Sender (üblicherweise »Bob«) und Empfänger (»Alice«) einen geheimen Schlüssel (in der Regel eine Text- oder Bitfolge) vereinbaren, den sonst niemand kennen darf. Nun verschlüsselt der Sender (Bob) seine Nachricht mit eben diesem geheimen Schlüssel und sendet sie an den Empfänger. Dieser wiederum ist mit dem Schlüssel in der Lage, die Information wieder zu entschlüsseln. Dritten, die nicht im Besitz des Schlüssels sind, bleibt der Inhalt der Kommunikation zwischen Alice und Bob verborgen.

Ein Schwachpunkt bei der symmetrischen Verschlüsselung ist der sichere Austausch der Schlüssel: Bevor etwas sicher übertragen werden kann, muss der Schlüssel sicher übertragen werden...

6.2 asymmetrische Verfahren

Asymmetrische Verfahren beruhen auf dem Prinzip, dass für Ver- und Entschlüsselung unterschiedliche Schlüssel benutzt werden. In der Praxis bedeutet dies, das jede Person zwei Schlüssel besitzt: einen öffentlichen, der an jeden weitergegeben werden kann, der an diese Person eine verschlüsselte Nachricht senden will. Außerdem exisitiert ein zweiter, privater Schlüssel, der auf jeden Fall geheim gehalten werden muss. Möchte Bob nun eine Nachricht an Alice versenden, verschlüsselt er sie mit Alice' öffentlichem Schlüssel (den ja jeder kennen darf). Diese Nachricht kann nun nur noch mit dem privaten Schlüssel von Alice entschlüsselt werden. So ist sichergestellt, dass nur Alice als rechtmäßige Empfängerin den Text lesen kann.

Umgekehrt müsste Alice eine Nachricht an Bob mit seinem öffentlichen Schlüssel verschlüsseln, anschließend könnte Bob diese Nachricht mit seinem privaten Schlüssel wieder dechiffrieren.

Sinn dieser sogenannten Public-Key-Kryptographie ist die Möglichkeit, Daten verschlüsselt an Personen senden zu können, die man zuvor nicht getroffen hat und somit auch keinen geheimen Schlüssel austauschen konnte. Kein Wunder also, dass Public-Key-Verfahren besonders im E-Mail-Verkehr eingesetzt werden, wo sich die Kommunikationspartner u.U.

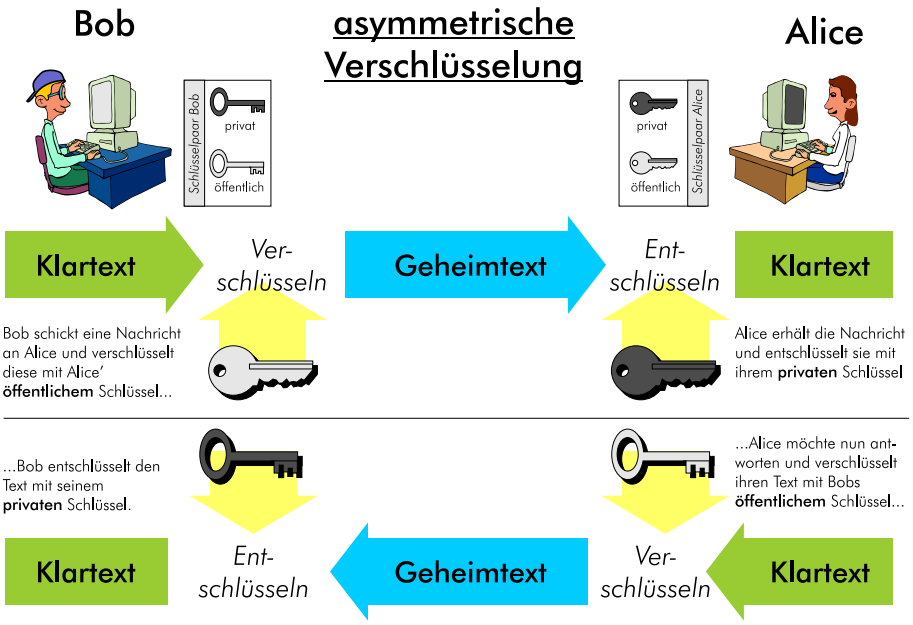

Abbildung 3: Prinzip asymmetrischer Krypto-Verfahren

auf unterschiedlichen Kontinenten befinden und sich der sichere Austausch eines geheimen Schlüssels entsprechend schwierig gestalten würde.

7 Ausgewählte Kryptosysteme

7.1 Cäsar

Wir unterscheiden zwischen zwei Verfahren: Dem Alphabetischen Cäsar und dem Buchstaben-Cäsar. Bei ersterem Verfahren verschlüsselt man einen beliebigen Text, in dem man das komplette Klartextalphabet aufschreibt und es darunter wiederholt, jedoch um k Stellen verschoben:

Klartextalphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

In dem Beispiel wurde das Geheimtextalphabet um 4 Stellen verschoben. Man chiffriert nun die Nachricht, in dem man den Klartextbuchstaben oben durch den entsprechenden Buchstaben aus dem Geheimtextalphabet ersetzt. So würde zum Beispiel aus KRYPTOGRAPHIE die Folge GNULPKCLWLDEA. Mit den Kenntnis von k kann der Empfänger die Nachricht wieder dechiffrieren, k ist also unser Schlüssel. Jedoch ist dieses Verfahren durch bloßes Ausprobieren aller 25 Schlüssel sehr leicht zu umgehen.

Einen Schritt weiter geht der Buchstaben-Cäsar, der zur Gruppe der monoalphabetischen Chiffrierungen gehört. Hierbei wird das Geheimtext-Alphabet nicht nur verschoben, sondern komplett neu zusammengesetzt. Voraussetzung ist lediglich, dass jedem Klartextbuchstaben genau ein Geheimbuchstabe zugeordnet ist und umgekehrt.

Klartextalphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimtextalphabet	Q	A	Y	W	S	X	E	D	C	R	F	V	T	G	B	Z	H	N	U	J	M	I	K	O	L	P

KRYPTOGRAPHIE würde in diesem Beispiel zu FNLZJBENQZDCS. Gegenüber den Verschiebechiffren gibt es hier breits etwa $4 \cdot 10^{26}$ Möglichkeiten der Verschlüsselung. Dem Empfänger muss als Schlüssel zur Dechiffrierung das komplette Geheimtextalphabet oder zumindest die Vorschrift zu dessen Bildung bekannt sein. Auch monoalphabetische Chiffrierungen sind nicht sicher, da durch Häufigkeitsanalyse der Zeichen relativ leicht das Geheimtextalphabet nur aus dem vorliegenden Geheimtext geschlussfolgert werden kann.

7.2 Data Encryption Standard DES

Im Jahre 1977 wurde der von IBM unter Einfluss der National Security Agency (NSA) entwickelte Verschlüsselungsalgorithmus zum Data Encryption Standard (DES) erklärt. Der DES-Algorithmus mischt vereinfacht gesagt die Bits derartig kräftig durch, dass es unmöglich wird, aus dem Geheimtext den Klartext oder den Schlüssel schlussfolgern zu können.

Der DES verschlüsselt immer Blocks von je 64 Bit Länge, daher zählt er auch zu den Blockchiffren. Zur Verschlüsselung wird ein Schlüssel von 64 Bit Länge verwendet, von dem aber nur 56 Bit wirklich wirksam sind. Eine wichtige Rolle spielen im Verlauf des Algorithmus Permutationen, d.h. die Bits werden nach einer festen Vorschrift umgeordnet - z.B. Bit 34 kommt an die Stelle von Bit 2, dieses an die Stelle 14, das dortige Bit auf 1 und so weiter. Den prinzipiellen Ablauf des DES zeigt die Abbildung, er besteht aus der Eingangspermutation, der Schlüsseleinteilung, dem zentralen Block (der 16mal durchlaufen wird) und schließlich der Ausgangspermutation.

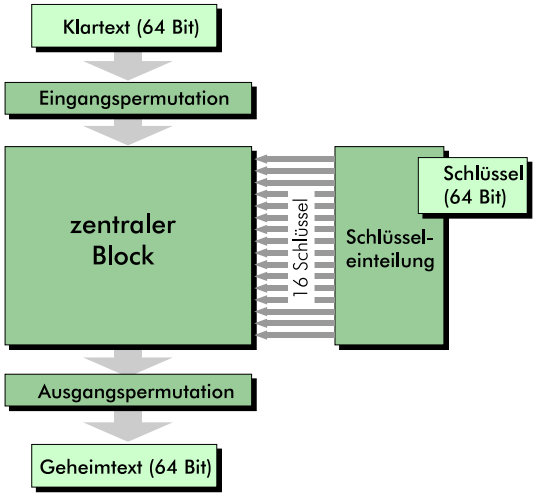

Abbildung 4: Funktionsprinzip des DES

Zunächst wird der zu codierende 64-Bit-Block in der Eingangspermutation komplett umgeordnet. Außerdem werden im Schlüsseleinteilungs-Teil aus dem Original-Schlüssel 16 weitere Schlüssel erzeugt, die später bei der Verschlüsselung im zentralen Block eine Rolle spielen. Zunächst wird dabei der 64 Bit lange Schlüssel auf 56 Bit reduziert, indem jedes achte Bit weggelassen wird. Anschließend werden u.a. durch Linksverschiebung dieser 56 Bit nacheinander 16 verschiedene Schlüssel erzeugt, die von dem Originalschlüssel abhängig sind. Diese Schlüssel werden dann jeweils nochmal auf 48 Bit reduziert, indem bestimmte Bits ignoriert werden.

Sind die Schlüssel generiert und hat der Datenblock die Eingangspermutation hinter sich, beginnt die Ausführung des zentralen Blocks. Hierbei wird der 64-Bit-Datenblock in einen linken und einen rechten Teil geteilt, die jeweils 32 Bit groß sind. Der rechte Teil wird nun durch sog. Expansionsmutation auf 48 Bit erweitert, indem einzelne Bits dupliziert werden. Anschließend wird er mit dem ersten Schlüssel (der ja ebenfalls 48 Bit lang ist) bitweise XOR-verknüpft (≫Exklusives Oder≪). Auf diese Operation folgt die sogenannte S-Box-Substitution. DES

definiert 8 verschiedene S-Box-Tabellen, die die Substitutionen beschreiben. Jede dieser S-Boxen nimmt 6 Bit Eingabe entgegen und gibt nach der Umstellung 4 Bit Ausgabe zurück. Aus den 48 Bit Daten werden nun 8 Blöcke zu je 6 Bit gebildet, die den jeweiligen S-Boxen übergeben werden. Diese liefern 8 mal 4 Bit zurück, wir erhalten also wieder 32 Bit an Daten. Auf diesen 32-Bit-Block wird eine weitere Permutation P angewandt, die Bits werden nochmals umgeordnet, bevor sie mit der linken Hälfte des ursprünglichen 64-Bit-Datenblocks XOR-verknüpft werden. Anschließend wird die rechte mit der linken Hälfte getauscht und der zentrale Block beginnt von vorn, dann aber mit dem zweiten Schlüssel. Dies wiederholt sich so lange, bis alle 16 Schlüssel zur Anwendung kamen.

Sind die 64 Bit verschlüsselt aus dem zentralen Block herausgekommen, werden sie nochmals einer Ausgangspermutation unterzogen, die die Umkehrung der Eingangspermutation darstellt. Die Entschlüsselung lässt sich durchführen, indem man die Permutationstabellen umgekehrt anwendet und die Schlüsselerzeugung auch ≫rückwärts≪ durchlaufen lässt. Sowohl Ver- als auch Entschlüsselung sind durch ihre bitorientierte Arbeitsweise auf Computern sehr schnell durchführbar.

DES in seiner ursprünglichen Form kommt wegen der geringen Schlüssellänge heute kaum noch zur Anwendung, stattdessen greift man auf sog. Triple-DES zurück.

7.3 RSA

Der RSA-Algorithmus, benannt nach seinen Erfindern Ron Rivest, Adi Shamir und Leonard Adleman, dürfte den meisten wohl zumindest namentlich bekannt sein: es handelt sich um die zur Zeit sicherlich bekannteste und meistbenutzte asymmetrische Chiffre.

Die Sicherheit von RSA liegt in der Schwierigkeit begründet, (sehr) große Zahlen zu faktorisieren. Es ist leicht möglich, das Produkt zweier Primzahlen zu berechnen, jedoch weitaus schwieriger, aus diesem Produkt wieder die Faktoren zu bestimmen. Bei sehr großen Primzahlen wird dies unmöglich. RSA verwendet also eine Art ≫Falltür-Funktion≪, die nur in eine Richtung funktioniert.

Schlüsselerzeugung

Da RSA ein asymmetrisches Verfahren ist, benötigen wir ein Schlüsselpaar, bestehend aus dem öffentlichen und dem geheimen Schlüssel einer Person. Diese Schlüssel müssen jedoch zunächst einmal generiert werden. Dabei kommt prinzipiell folgender Ablauf zum Tragen (nach [5]):

- Es werden zwei Primzahlen p und q gewählt, die jeweils etwa 1000 bis 2000 Bits lang sein sollten.
- Die Zahl n ist das Produkt dieser Primzahlen: $n = p \cdot q$
- Es wird eine Zahl e gesucht die kleiner ist als n und relativ prim (keine gemeinsamen Faktoren) zu $(p-1) \cdot (q-1)$
- Berechnung der Zahl d:

$$d = \frac{1 \bmod (p-1) \cdot (q-1)}{e}$$

Diese Gleichung kann z.B. mit Hilfe des Erweiterten Euklidschen Algorithmus gelöst werden (auf dessen Komplexität ich hier nicht eingehen will)

- Öffentlicher Schlüssel bestehend aus e und n
  Privater Schlüssel bestehend aus d und n

p und q sind für die Verschlüsselung uninteressant und werden nicht gespeichert.

Ver- und Entschlüsselung

Ist nun eine Nachricht zu verschlüsseln, muss der Text zunächst in Blöcke aufgeteilt werden, deren Länge n nicht überschreiten darf. Außerdem werden Buchstaben in Zahlen konvertiert (dies ist aber in der Praxis nicht nötig, da Bits ja letztlich sowieso einen Zahlenwert darstellen). Für die Verschlüsselung mit dem öffentlichen Schlüssel gilt nun:

$$c = m^e \bmod n$$

wobei m das Klartext- und c das verschlüsselte Zeichen darstellt. Die Entschlüsselung geschieht umgekehrt mit dem privaten Schlüssel:

$$m = c^d \bmod n$$

Hierbei ist wieder c das Geheimtext- und m das Klartextzeichen.

Wie bei allen anderen Algorithmen auch hängt die Sicherheit des RSA-Algorithmus vor allem von der Schlüssellänge und der Geheimhaltung des privaten Schlüssels ab.

Literatur

[1] Brockhaus-Enzyklopädie; in 24 Bd. - 19. Auflage; F.A. Brockhaus Verlag GmbH, Mannheim 1990

[2] Kryptographie, Dossier 4/2001, Spektrum der Wissenschaft; ISSN 0947-7934

[3] Christian Thöing: Kryptographie
http://mitglied.lycos.de/cthoeing/krypto/index.htm

[4] Matthew Fischer: How to implement the Data Encryption Standard (DES)
http://www.infoserversecurity.org/files/des-how-to.txt

[5] Carl Duncan: RSA in 7 steps (Newsgroup-Posting in sci.crypt, 30.06.2001)
http://home.t-online.de/home/poisoner/krypto/rsa7stps.txt
http://groups.google.de/groups?selm=3B651D48.E5D47EFE%40invalid.addr