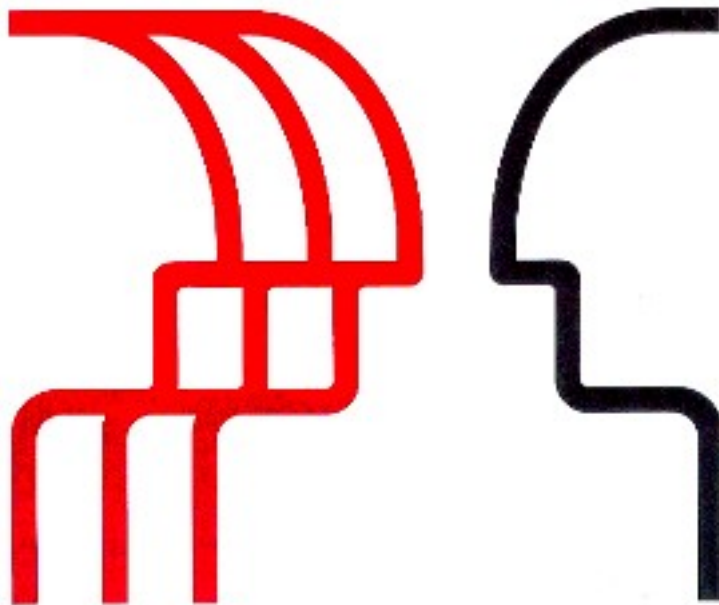




Facharbeit Kryptographie von [Brian Pfretzschner](#) steht unter einer [Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland Lizenz](#).

Fachoberschule am Beruflichen Schulzentrum e. o. Plauen



Facharbeit

in der Fachrichtung Informatik

Kryptographie

Brian Pfretzschner
Klasse FOS T 08 LB

Betreuer: Herr Neidel

Seiten: 20

Ort, Datum: Zeulenroda, 27. März 2009

Inhaltsverzeichnis

1	Einführung	3
1.1	Was ist Kryptographie	3
1.2	Geschichte	4
1.3	Abgrenzung	5
1.3.1	Signaturverfahren	5
1.3.2	Steganographie	5
2	Verfahren	5
2.1	symmetrische Kryptosysteme	6
2.1.1	Verschiebechiffre	6
2.1.2	Homophone Verschlüsselung	7
2.1.3	DES	8
2.1.4	RC6	8
2.1.5	AES	9
2.1.6	A5	9
2.2	asymmetrische Kryptosysteme	10
2.3	hybride Kryptosysteme	12
3	Angriffstechniken	13
3.1	Häufigkeitsanalyse	13
3.2	Brute Force	13
3.3	Known Plaintext	13
3.4	chosen-plaintext attack (Angriff mit frei wählbarem Klartext)	13
4	Kryptographie und Recht	14
5	Ausblick	14
6	Literaturverzeichnis	15
7	Selbständigkeitserklärung	20
8	Anlagen	21

1 Einführung

1.1 Was ist Kryptographie

(griechisch: *kryptós*, „verborgen“ und *gráphein*, „schreiben“)

Die Kryptographie beschäftigt sich mit der Verschlüsselung von Informationen. Verschlüsselung bedeutet, dass ein klar lesbarer Text (Klartext) durch ein Verschlüsselungsverfahren in eine „unleserliche“ Zeichenfolge (Geheimtext) umgewandelt wird.

Ein Verschlüsselungsverfahren besteht aus einem oder mehreren *Algorithmen* und einem oder mehreren *Schlüsseln* (teilweise vergleichbar mit Passwörtern).

Die Kryptographie wird natürlich nicht nur für (menschen-)lesbaren Text benutzt, sondern auch für binäre Daten, wie zum Beispiel Dokumente, Bilder, etc.

Die 4 Ziele der Kryptographie sind:

- *Zugriffsschutz* (Nur die berechtigten Gegenstellen können den Geheimtext entschlüsseln und somit interpretieren.)
- *Integrität* (= Änderungsschutz; Hiermit wird sichergestellt, dass kein Mittelman heimlich und unbemerkt die Daten manipuliert.)
- *Authentizität* (= Fälschungsschutz; Es kann eindeutig geprüft werden, wer die Daten abgesendet hat.)
- *Verbindlichkeit* (= Auch Dritten gegenüber, muss sichergestellt werden, dass der Sender und die empfangenen Daten eindeutig zugeordnet werden können.¹⁾)

Dabei muss nicht jedes Verschlüsselungsverfahren alle 4 Ziele abdecken.

Die *Kryptographie* ist mit der *Kryptoanalyse* unter der Bezeichnung *Kryptologie* zusammengefasst.

Der Gesamtbereich der Kryptologie beschäftigt sich mit der Informationssicherheit.

Dabei ist die Kryptographie das Teilgebiet, das sich mit der Verschlüsselung der Daten beschäftigt. Die Kryptoanalyse hingegen versucht an die Informationen aus verschlüsselten Daten zu kommen, ohne den Schlüssel zum entschlüsseln zu kennen.²⁾

1 <http://wapedia.mobi/de/Kryptographie>

2 <http://de.wikipedia.org/wiki/Kryptographie>

1.1 Geschichte

Die erste Verwendung eines kryptographie-ähnlichen Verfahrens ist auf die Ägypter im dritten Jahrtausend v.u.Z. zurückzuführen. Sie benutzten die sogenannte Altägyptische Kryptographie. Dabei veränderte man die Darstellungsform des hieroglyphischen Schriftsystems, sodass nur eine kleine Gruppe die Informationen lesen konnte.

Die Verschiebechiffre wurde durch Gaius Julius Caesar (römischer Staatsmann, Feldherr und Autor) sehr bekannt. Er benutzte sie für seine militärische Kommunikation.¹

Mehr zur Verschiebechiffre unter 2.1.1 Verschiebechiffre.

Im Amerikanischen Bürgerkrieg (1861-1865) wurde die Telegrafie zur Kommunikation genutzt. Allerdings investierte man wenig in die Verschlüsselung der eigenen, bzw. Entschlüsselung der gegnerischen Kommunikation. Dennoch gelang die Entschlüsselung dank der schwachen Verschlüsselungsverfahren auf beiden Seiten häufig.

Ende des 19. Jahrhunderts formulierte Auguste Kerckhoffs von Nieuwenhof das *Kerckhoffs' Prinzip*. Dieses sagt aus, dass ein Verschlüsselungssystem durch die Geheimhaltung des Algorithmus keinen Sicherheitszuwachs erfährt, sondern nur durch die Geheimhaltung der Schlüssel.

Bis heute, ist es das Grundgesetz der Kryptographie.²

Im Ersten Weltkrieg wurde die Kryptoanalyse erstmals intensiv genutzt. So entschlüsselte ein französischer Artillerie-Offizier das damals von den Deutschen eingesetzte Verschlüsselungsverfahren ADFGX. Laut Historikern und Kryptologen konnte auch dadurch die Einnahme von Paris verhindert werden.

Im Zweiten Weltkrieg wurden, wenn möglich, Maschinen zur Ver- und Entschlüsselung eingesetzt. So ist auf deutscher Seite u.a. die Enigma zu nennen, die aber von den Briten entschlüsselt werden konnte.

Auf Amerikanischer Seite nutzte man zwei verschiedene Maschinen: Die M-209 und die SIGABA. Die SIGABA war wesentlich sicherer als die M-209 und wurde nur für wichtige Nachrichten benutzt. Nach heutigem Wissensstand, konnten die Deutschen die SIGABA nie brechen.

In den siebziger Jahren konnten durch die Erfindung des Computers neue und sicherere

1 <http://de.wikipedia.org/wiki/C%C3%A4sar-Chiffre>

2 http://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip

Algorithmen entwickelt werden. Ein Beispiel dafür ist das 1976 entwickelte Verschlüsselungssystem DES (mehr dazu unter 2.1.3 DES) oder die Entdeckung von Public-Key-Verfahren (siehe 2.2 asymmetrische Kryptosysteme).

1991 veröffentlichte der amerikanische Physiker Phil Zimmermann das PGP-Verfahren, das besonders für Privatpersonen ausgelegt war.¹

1.2 Abgrenzung

1.2.1 Signaturverfahren

Signaturverfahren nutzen asymmetrische Verschlüsselungsverfahren (siehe 2.2 asymmetrische Kryptosysteme). Diese werden aber nicht eingesetzt um den Nachrichteninhalte zu verschlüsseln, sondern um eine Signatur zu erzeugen die der Nachricht angehängt wird. Mittels dieser Signatur kann der Absender der Nachricht eindeutig bestimmt werden.²

1.2.2 Steganographie

Das Ziel der Steganographie ist ebenfalls die Übertragung von Daten und Informationen ohne das Unberechtigte mitlesen können. Dabei werden die Daten nicht verschlüsselt sondern in einem Datenstrom versteckt, sodass Dritte die Übertragung nicht bemerken. Natürlich gibt es auch Mischformen bei denen die Daten verschlüsselt werden und anschließend versteckt versendet oder auch gespeichert werden.³

2 Verfahren

Es gibt zwei grundlegende Vorgehensweisen:

- *Blockverschlüsselung*

Die Daten werden Blockweise verschlüsselt. Es werden also nacheinander Blöcke mit typischerweise 128, 168, 192 oder 256 Bit Länge⁴ verarbeitet.

Der Verschlüsselungsvorgang kann erst beginnen, wenn die zu verschlüsselnden Daten in Blöcke zerteilt wurden. Sollte der letzte Block nicht komplett gefüllt sein weil nicht mehr genug Zeichen übrig sind, wird dieser mit Füllzeichen aufgefüllt. Beim

1 http://de.wikipedia.org/wiki/Geschichte_der_Kryptographie

2 <http://de.wikipedia.org/wiki/Signaturverfahren>

3 <http://de.wikipedia.org/wiki/Steganographie>

4 <http://de.wikipedia.org/wiki/Blockchiffre>

Entschlüsseln müssen die Füllzeichen unbedingt wieder entfernt werden!

- *Stromverschlüsselung*

Diese Art eignet sich besonders für die Echtzeit-Verschlüsselung, denn jedes Klartext-Bit kann sofort verschlüsselt und übertragen werden. Somit wird Bit für Bit verarbeitet, egal wie viele noch übrig sind bzw. noch dazu kommen werden.

2.1 symmetrische Kryptosysteme

Symmetrische Verschlüsselungssysteme zeichnen sich durch gleiche Schlüssel zum Ver- bzw. Entschlüsseln aus. Deshalb muss der Schlüssel der zum Verschlüsseln benutzt wurde zum Empfänger übertragen werden. Dritte müssen an dieser Stelle nur den Schlüssel und den Geheimtext abfangen und können somit die Daten entschlüsseln.

Bei manchen Verfahren muss der Schlüssel nach dem Verschlüsseln noch transformiert werden, damit man den Geheimtext entschlüsseln kann.

Vorteile:

- kaum rechenintensiv → schnell

Nachteile:

- unsicher
- geheimer Schlüssel muss übertragen werden
- für jeden Kommunikationspartner wird ein eigener Schlüssel benötigt¹

2.1.1 Verschiebechiffre

Auch bekannt als Caesar-Verschlüsselung, Caesar-Verschiebung oder „Einfacher Caesar“². Es ist ein sehr einfacher Vertreter für eine monoalphabetische Substitution, also das Ersetzen von Zeichen durch ein festgelegtes Alphabet. Caesar benutzte meistens den Schlüssel C, d.h. er verschob das Alphabet um 3 Stellen (C ist der dritte Buchstabe im Alphabet).

Das Geheimalphabet nach Caesar sieht als wie folgt aus:

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

1 http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem

2 <http://de.wikipedia.org/wiki/Verschiebechiffre>

(Es ist üblich, Klartextbuchstaben klein und Geheimtextbuchstaben groß zu schreiben. Das hat allerdings keine Auswirkungen auf die Verschlüsselung.)

Bevor man mit der Verschlüsselung beginnt, entfernt man meistens noch die Leerzeichen. Danach verschiebt man die Buchstaben des Textes. Aus dem Text „Test der Verschiebechiffre“ wird verschlüsselt:

Klar: TestderVerschiebechiffre

Geheim: WhvwghuYhuvfklhehfkliiuh

Die Verschiebechiffre ist nicht sicher, da es nur 25 verschiedene Schlüssel gibt. Man kann den verwendeten Schlüssel durch probieren (siehe 3.2 Brute Force) oder durch eine Häufigkeitsanalyse (siehe 3.1 Häufigkeitsanalyse) herausfinden. Die Häufigkeitsanalyse macht Gebrauch von der ungleichmäßigen Buchstabenhäufigkeit in der Sprache (siehe Anlage 1: grafische Darstellung der Buchstabenhäufigkeit). So ist das E in der deutschen Sprache mit Abstand der häufigste Buchstabe.

In unserem Beispiel sind die Buchstaben im Geheimtext wie folgt verteilt:

Geheimtextbuchstabe	H	U	K	L	V	W	I	F	Y	E	G
Anzahl	6	3	2	2	2	2	2	2	1	1	1

Daraus ergibt sich, dass das Geheimtext-H höchstwahrscheinlich das Klartext-E ist. Die Differenz von E (5. Buchstabe im Alphabet) und H (8. Buchstabe im Alphabet) ergibt 3. Also ist der Text mit dem Schlüssel C verschlüsselt.

2.1.2 Homophone Verschlüsselung

Die homophone Verschlüsselung ist der Verschiebechiffre sehr ähnlich, ist aber wesentlich sicherer weil man die Häufigkeitsanalyse nicht nutzen kann. Klartextbuchstaben können durch mehrere Geheimtextzeichen ersetzt werden, nicht wie bei der Verschiebechiffre nur durch einen Geheimtextbuchstabe. Die Buchstabenhäufigkeit ist in der deutschen Sprache wie folgt verteilt:

	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
%	6	2	2	5	17	2	3	5	8	1	1	3	2	10	2	1	1	7	7	6	4	1	1	1	1	1

So wird z.B. der Buchstabe E durch 17 verschiedene Zeichen ersetzt werden, bzw. das O durch 2, usw. Dadurch wird erreicht, dass jedes Geheimtextzeichen eine Häufigkeit von nur 1% hat, somit kann man keine Häufigkeitsanalyse mehr durchführen. Man müsste stattdessen auf eine Analyse der Bigramme (Zeichenpaare), Trigramme oder Tetragramme¹ zurückgreifen. Das

¹ http://de.wikipedia.org/wiki/Homophone_Verschl%C3%BCsslung

heißt, man sucht nach häufig auftretenden Zeichenpaaren wie CH, CK, EN, ER, ... Dazu werden allerdings lange Texte benötigt. Ein kurzer Text ist also relativ gut geschützt.

2.1.3 DES

1975 veröffentlichte IBM den Data Encryption Standard, der im Auftrag der NSA (National Security Agency, USA) entwickelt wurde, denn zu dieser Zeit gab es kaum Verschlüsselungssysteme die für die nicht-militärischen Bereiche zur Verfügung standen.

DES arbeitet als Blockchiffre mit Blockgrößen von 64 Bit. Der Schlüssel ist ebenfalls 64 Bit lang, allerdings gehen 8 Bit für den Paritäts-Check (= dient zur Erkennung von Fehlern bei der Übertragung oder Speicherung) verloren. Das heißt es gibt 2^{56} , also ca. 72 Milliarden verschiedene Schlüssel.

1976 wurde dieses Verfahren offizieller Standard für die US-Regierung und international vielfach eingesetzt. Im Juni 1997 wurde erstmals eine verschlüsselte Nachricht geknackt (= ohne Kenntnis des Schlüssels entschlüsselt).

1999 wurde die Sicherheit des einfachen DES nicht mehr bestätigt. Stattdessen gilt 3DES als sicher. Bei 3DES wird die Nachricht mit 3 voneinander unabhängigen und unterschiedlichen Schlüsseln verschlüsselt. Zuerst wird der Klartext mit dem Schlüssel S1 verschlüsselt, danach wird der Geheimtext mit Schlüssel S2 entschlüsselt und schließlich mit dem Schlüssel S3 verschlüsselt.²

2.1.4 RC6

RC6 ist die aktuelle Version der RC Verschlüsselungssysteme. Sie wurden alle von Ronald Rivest entwickelt.

RC6 ist die Weiterentwicklung von RC5. Es behebt die bekannten Schwachstellen des RC5 Verfahrens. RC6 wurde vom amerikanischen National Institute of Standards and Technology (NIST) als hinreichend sicher eingestuft.

RC6 arbeitet mit variablen Schlüssellängen, Blockgrößen und Runden. Der Schlüssel kann 0 – 2040 Bits lang sein, 0 – 255 Runden werden unterstützt und als Größe der Blöcke werden üblicherweise 128 Bit verwendet.¹

2 http://de.wikipedia.org/wiki/Data_Encryption_Standard

1 <http://de.wikipedia.org/wiki/RC6>

2.1.5 AES

Der Advanced Encryption Standard (AES) ist der offizielle Nachfolger von DES bzw. 3DES. Er wurde vom National Institute of Standards and Technology (NIST) im Oktober 2000 festgelegt.

Um einen möglichst guten Algorithmus zu finden, wurde 1997 ein offener Wettbewerb ausgerufen. 1998 standen schließlich 5 Algorithmen im Finale, u.a. RC6 und Rijndael. Rijndael gewann schlussendlich, denn es konnte besonders durch seine überdurchschnittliche Geschwindigkeit und durch die Einfachheit des Algorithmus überzeugen.

Bei AES ist die Blocklänge auf 128 Bit beschränkt, bei den Schlüssellängen steht die Wahl zwischen 128, 192 oder 256 Bits. Durch die unterschiedlichen Schlüssellängen spricht man auch von AES-128, AES-192 und AES-256.

AES wird heute in der Verschlüsselung des WLAN-Funkverkehrs (WPA2), für die Übertragung der Daten bei SSH und Ipsec, bei mehreren VoIP Protokollen und in vielen anderen Anwendungsfällen genutzt.²

2.1.6 A5

A5 ist ein Stromchiffreverfahren, d.h. die anfallenden Klartext-Daten können Bit für Bit verschlüsselt und weitergegeben werden.

Es gibt bedeutend weniger Stromchiffre- als Blockchiffreverfahren³, deshalb möchte ich hier nur auf A5 eingehen.

A5 wird für die Kommunikation zwischen Mobiltelefon und Sendemast eingesetzt. Da es in manchen Ländern Beschränkungen für Verschlüsselungssysteme gibt, ergeben sich daraus nachfolgende verschiedene Varianten des A5 Systems:

- *A5/0*
Die Übertragung der Daten erfolgt unverschlüsselt (unter anderen eingesetzt in Frankreich, Libyen).
- *A5/1*

² http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

³ http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie

Die normale Variante der A5 Verschlüsselung.

- A5/2

Eine abgeschwächte Version des A5/1 Verfahrens (wird z.B. in Australien eingesetzt).

A5/1 wird nicht mehr als sicher betrachtet. Deshalb wurde der Nachfolger A5/3 entwickelt. Es unterscheidet sich allerdings grundlegend vom Vorgänger, denn A5/3 ist eine Blockchiffre.¹

2.1 asymmetrische Kryptosysteme

Bei der asymmetrischen Verschlüsselung besitzt jeder Kommunikationspartner 2 Schlüssel: einen privaten (private key) und einen öffentlichen (public key). Der öffentliche Schlüssel kann beliebig weitergegeben und verbreitet werden. Der Private hingegen darf unter keinen Umständen jemand anderem bekannt sein! Die beiden Schlüssel hängen voneinander ab, es ist aber nicht möglich durch den öffentlichen auf den privaten Schlüssel zu schließen.

Wenn Person S (Sender) einen geheimen Text an Person E (Empfänger) senden möchte, braucht Person S den öffentlichen Schlüssel von Person E. Dieser kann problemlos und in Klartext ausgetauscht werden, denn er darf jedem bekannt sein. Person S verschlüsselt den Text mit dem öffentlichen Schlüssel und sendet den Geheimtext an Person E. Dieser Geheimtext kann nur durch den privaten Schlüssel entschlüsselt werden. Man kann nicht durch den öffentlichen Schlüssel auf den Klartext oder den privaten Schlüssel schließen.

Asymmetrische Kryptosysteme sind extrem sicher, es dauert Monate bis Jahre um eine verschlüsselte Nachricht zu knacken. Bei ausreichenden Schlüssellängen ist es zur Zeit noch komplett unmöglich. Eine Nachricht die mit einem 193-stelligen Schlüssel verschlüsselt wurde, konnte erst nach einem Jahr Rechenarbeit gebrochen werden – üblich sind heute 300-stellige Schlüssel!

Der größte Nachteil der asymmetrischen Verschlüsselung ist der hohe Rechenaufwand. Im Vergleich zur symmetrischen Verschlüsselung ist die asymmetrische ca. 1000-mal langsamer. Ein weiteres Problem tritt auf, wenn eine Nachricht an mehrere Empfänger gesendet werden soll, denn sie muss für jeden Empfänger mit dessen öffentlichen Schlüssel verschlüsselt werden.

Vorteile:

- keine Übertragung von privaten Schlüsseln
- Nutzbar als digitale Unterschrift/Signatur
- sicher

¹ [http://de.wikipedia.org/wiki/A5_\(Algorithmus\)](http://de.wikipedia.org/wiki/A5_(Algorithmus))

Nachteile:

- sehr rechenintensiv → langsam

Es gibt verschiedene asymmetrische Systeme, aber alle ähneln sich in ihrer Funktionsweise. Abgesehen von den mathematischen Unterschieden sind sie größtenteils gleich. Deshalb möchte ich hier nur das bedeutendste Verfahren - RSA - vorstellen, dafür aber mit dem mathematischen Formeln und Abläufen.¹

RSA wurde 1977 von Ronald L. Rivest, Adi Shamir und Leonard Adleman entwickelt. Es war die erste öffentlich nutzbare asymmetrische Verschlüsselung.

Das Verfahren basiert darauf, dass es sehr aufwendig ist eine große Zahl zu faktorisieren, d.h. in zwei Primzahlen zu zerlegen, bei deren Multiplikation, mit sich selbst, das Ergebnis die ursprüngliche Zahl ist.

Schlüsselerzeugung:

1. Erzeugung oder Auswahl von zwei voneinander unabhängigen Primzahlen p und q . Umso größer diese sind, umso sicherer ist der Schlüssel (größere Schlüssellänge).

2. Berechnung des RSA-Moduls:

$$N = pq$$

3. Berechnung der Eulerschen φ -Funktion von N :

$$\varphi(N) = (p-1)(q-1)$$

4. Auswahl einer zu $\varphi(N)$ teilerfremden Zahl e , für die gilt:

$$1 < e < \varphi(N)$$

5. Berechnung von d , als Kehrwert von e :

$$ed \cdot \text{mod } \varphi(N) = 1^2$$

Nach dem Berechnen der Schlüssel werden nur noch die Zahlen N , e und d benötigt. Alle anderen müssen sicher entfernt werden. N und e sind der öffentliche Schlüssel, N und d der Private.

Man kann diese Verschlüsselung nur auf Zahlen anwenden. Da alle digitalen Informationen als Bit-Folge vorliegen, kann man einfach eine bestimmte Anzahl von Bits als Zahl interpretieren. Der Empfänger entschlüsselt den Geheimtext und kann die daraus resultierende Bit-Folge beliebig interpretieren.

1 <http://www.philippbauer.de/info/info/asymmetrische-verschluesselung/>

2 <http://www.kryptologie.tk/>

Eine Klartextzahl K kann man durch folgende Formel in die entsprechende Geheimtextzahl G umwandeln: $G = K^e \cdot \text{mod } N$ (e ist Teil des öffentlichen Schlüssels).

Die Entschlüsselung der Geheimzahl G in die Klartextzahl K wird schließlich mit folgender Formel durchgeführt: $K = G^d \cdot \text{mod } N$ (d ist Teil des privaten Schlüssels).

RSA kann auch zum Signieren von Nachrichten verwendet werden. Dazu verschlüsselt der Absender einen definierten Datenblock mit dem privaten Schlüssel. Der Datenblock besteht u.a. aus einem Hash der Nachricht um Manipulationen zu entdecken. Der Empfänger kann dann mit dem öffentlichen Schlüssel prüfen, ob die Nachricht von dem angegebenen Absender gesendet wurde und ob sie zwischenzeitlich manipuliert wurde – vorausgesetzt der private Schlüssel ist niemand anderem bekannt.

RSA hat eine große Rolle in der Verschlüsselung eingenommen. Es dient zur Schlüsselübertragung bei wichtigen Protokollen wie z.B. SSH, Ipsec, TLS oder auch zu eMail Verschlüsselung durch PGP oder S/MIME (siehe 2.3 hybride Kryptosysteme)¹.

2.1 hybride Kryptosysteme

Hybride Verschlüsselungssysteme vereinen die Vorteile von asymmetrischen und symmetrischen Systemen. Symmetrische Verfahren sind ressourcensparend aber unsicher, da zur Ver- und Entschlüsselung der gleiche Schlüssel benutzt wird. Somit muss der Gegenstelle der Schlüssel bekannt sein. Bei hybriden Verfahren wird dieser Schlüssel asymmetrisch verschlüsselt und kann somit sicher an die Gegenstelle gesendet werden. Die eigentlichen Daten werden dann, mit dem gerade vereinbarten Schlüssel, symmetrisch verschlüsselt und übertragen.

3 Angriffstechniken

3.1 Häufigkeitsanalyse

Diese Angriffstechnik habe ich schon unter 2.1.1 Verschiebechiffre beschrieben.

Sie funktioniert nur mit monoalphabetischen Verschlüsselungssystemen, denn die Häufigkeitsanalyse basiert darauf, dass manche Zeichen in einem Geheimtext eine größere Häufigkeit haben als andere. Daraus lässt sich, abhängig von der Sprache, der Schlüssel erkennen (siehe Anlage 1: grafische Darstellung der Buchstabenhäufigkeit).

¹ <http://de.wikipedia.org/wiki/RSA-Kryptosystem>

3.2 Brute Force

Bei Brute Force Angriffen werden alle Möglichkeiten durchprobiert. Deswegen ist es eine sehr einfache aber aufwendige Art einen Geheimtext zu knacken. Da aber moderne PCs bzw. Server viel Rechenpower haben, wird die Methode wieder populärer.

Vor Brute Force Attacken kann man sich relativ einfach durch längere Schlüssel und somit mehr Möglichkeiten schützen¹.

3.3 Known Plaintext

Wie der Name schon sagt, ist dem Angreifer ein Teil der Nachricht sowohl als Geheim- als auch als Klartext bekannt. Somit kann man den verwendeten Schlüssel berechnen. Dabei ist zu beachten, dass bereits häufig verwendete Textbausteine als Angriffspunkte dienen können (z.B. „Mit freundlichen Grüßen“ oder berechenbare Protokoll-Daten)².

3.4 chosen-plaintext attack (Angriff mit frei wählbarem Klartext)

Diese Attacke funktioniert im Prinzip wie ein Known Plaintexte Angriff, mit dem Unterschied das der Angreifer die Klartexte frei wählen kann und Zugriff auf die resultierenden Geheimtexte hat. Damit können die Zusammenhänge zwischen Klar- und Geheimtext effizienter und schneller berechnet werden.³

4 Kryptographie und Recht

In vielen Ländern gibt es Beschränkungen in der Nutzung von Verschlüsselungssystemen, denn es werden nicht nur legale Daten verschlüsselt. Auch Kriminelle nutzen die Kryptographie um Informationen geschützt zu übertragen.

Unverschlüsselte eMails sind z.B. vergleichbar mit Postkarten. Jeder kann sie ohne große Probleme lesen, ohne dass der Empfänger etwas davon mitbekommt. Deshalb sollten wichtige Nachrichten gut verschlüsselt werden. Das Bundeswirtschaftsministerium und das Bundesinnenministerium haben die Entwicklung von GnuPG (Freies Verschlüsselungssystem, dass besonders zur eMail-Verschlüsselung eingesetzt wird.) sogar unterstützt.¹

1 <http://www.kuno-kohn.de/crypto/crypto/analysis.htm>

2 http://www.mathe.tu-freiberg.de/~dempe/schuelerpr_neu/analyse.htm

3 http://de.wikipedia.org/wiki/Adaptive_Chosen_Ciphertext

1 <http://www.sueddeutsche.de/computer/20/320889/text/>

Ganz anders sieht es in manchen anderen Ländern aus: In Großbritannien ist man verpflichtet das Passwort bzw. den Schlüssel auszuhändigen, wenn dies verlangt wird. Das bestätigt ein aktuelles Urteil vom Oktober 2008². In den USA fallen Verschlüsselungssysteme sogar unter das Waffengesetz und dürfen nicht ohne weiteres exportiert werden³.

5 Ausblick

Die Forschung an der Quantenkryptographie ist weit fortgeschritten. Es kann damit gerechnet werden, dass diese Technik in den nächsten Jahren zum Einsatz kommt. Damit ist es erstmals möglich den geheimen Schlüssel absolut abhörsicher zu übertragen. Dazu nutzt man die physikalischen Gesetze aus.⁴

Die eigentliche Verschlüsselung muss aber weiterhin von einem möglichst starken Verschlüsselungssystem durchgeführt werden. Sobald die Quantenkryptographie soweit ausgereift ist, dass jeder sie nutzen kann, werden die asymmetrischen Systeme den Großteil ihres Nutzens verlieren, denn der Vorteil von asymmetrischen Verschlüsselungen ist, dass kein geheimer Schlüssel übertragen werden muss. Da die Schlüsselübertragung durch die Quantenkryptographie aber absolut sicher wird, entfällt der größte Vorteil der asymmetrischen Systeme.

Ich denke dass in den nächsten Jahren ein komplexeres und natürlich sichereres symmetrisches System entwickelt wird. Dank Quantenkryptographie ist die Kommunikation damit nahezu komplett sicher.

6 Literaturverzeichnis

- [1] Billen, Kai: SHA-2 Familie und SHA-3 - ravenhorst
<http://blog.kairaven.de/archives/1700-SHA-2-Familie-und-SHA-3.html>
- [2] Bölz, Tobias M.: RSA

2 <http://www.gulli.com/news/gro-britannien-neues-urteil-2008-10-19/>

3 <http://wapedia.mobi/de/Kryptographie?t=5>.

4 http://daily-innovation.de/50226711/quantenkryptografie_die_zukunft_der_abharsicheren_verschlasselung.php

- <http://www.scribd.com/doc/7147/RSA>
- [3] Christ, Jochen: [kryptologie.tk](http://www.kryptologie.tk)
<http://www.kryptologie.tk/>
- [4] Esslinger, Prof. Bernhard: CrypTool - Lernprogramm für Kryptographie und Kryptoanalyse
<http://www.cryptool.com/>
- [5] Ewald, Gerd: Regenechsen :: Ideas come true | Einleitung
http://www.regenechsen.de/phpwcms/index.php?krypto_einleitung
- [6] Firma RSA Laboratories: Kryptographie FAQ: Frage 4: Was sind die Vor- Nachteile von asymmetrischer Verschlüsselung im Vergleich mit symmetrischer Verschlüsselung?
<http://www.iks-jena.de/mitarb/lutz/security/cryptfaq/q4.html>
- [7] Glaser, Gerhard M.: Verschlüsselung (symmetrisch, asymmetrisch, hybrid)
<http://www.tcp-ip-info.de/security/verschluesselung.htm>
- [8] Hauer, Philipp: Asymmetrische Verschlüsselung/Public-Key-Verfahren. Das Verfahren. Die Vorteile/Pro und Nachteile/Kontra.
<http://www.philippbauer.de/info/info/asymmetrische-verschluesselung/>
- [9] Henkel, Kareen; Helbig, Susanne; Kriener, Jan: Sichere Datenübertragung - 5 Kryptoanalyse
http://www.mathe.tu-freiberg.de/~dempe/schuelerpr_neu/analyse.htm
- [10] Killeen, Ronan: Possible Attacks on RSA
http://members.tripod.com/irish_ronan/rsa/attacks.html
- [11] Kremer, Annika: gulli: Großbritannien: Neues Urteil bestätigt Pflicht zur Herausgabe von Passwörtern
<http://www.gulli.com/news/gro-britannien-neues-urteil-2008-10-19/>
- [12] Kremer, Annika: gulli: IT-Sicherheit: Neuer Hash-Algorithmus soll die SHA-Familie ersetzen
<http://www.gulli.com/news/it-sicherheit-neuer-hash-2008-10-30/>
- [13] Krippgans, Robert: Daily Innovation: Quantenkryptografie - die Zukunft der abhörsicheren Verschlüsselung
http://www.daily-innovation.de/50226711/quantenkryptografie_die_zukunft_der_abhorsicheren_verschluesselung.php

- [14] Kröner, Tim: Ausblick und Entwicklung
<http://www.voip-information.de/security/ausblick-entwicklung.php>
- [15] Laga, Dr. iur. Gerhard: Sicherheit im E-Mail Verkehr, Fernmeldegeheimnis
<http://www.rechtsprobleme.at/doks/diss-exkurs.html>
- [16] Malzacher, Peter: Ziele der Kryptographie
<http://www-aix.gsi.de/~peter/Kryptographie/sld009.htm>
- [17] o.V.: Paritätsbit – Wikipedia
<http://de.wikipedia.org/wiki/Parit%C3%A4tsbit>
- [18] o.V.: A5 (Algorithmus) – Wikipedia
[http://de.wikipedia.org/wiki/A5_\(Algorithmus\)](http://de.wikipedia.org/wiki/A5_(Algorithmus))
- [19] o.V.: Kryptoanalyse – Wikipedia
<http://de.wikipedia.org/wiki/Kryptoanalyse>
- [20] o.V.: Sezessionskrieg – Wikipedia
<http://de.wikipedia.org/wiki/Sezessionskrieg>
- [21] o.V.: GNU Privacy Guard – Wikipedia
http://de.wikipedia.org/wiki/GNU_Privacy_Guard
- [22] o.V.: Gaius Iulius Caesar – Wikipedia
http://de.wikipedia.org/wiki/Julius_Caesar
- [23] o.V.: Monoalphabetische Substitution – Wikipedia
http://de.wikipedia.org/wiki/Monoalphabetische_Substitution
- [24] o.V.: Monographisch – Wikipedia
<http://de.wikipedia.org/wiki/Monographisch>
- [25] o.V.: Atbash – Wikipedia
<http://de.wikipedia.org/wiki/Atbash>
- [26] o.V.: Data Encryption Standard – Wikipedia
http://de.wikipedia.org/wiki/Data_Encryption_Standard
- [27] o.V.: Advanced Encryption Standard – Wikipedia
http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

- [28] o.V.: Enigma (Maschine) – Wikipedia
[http://de.wikipedia.org/wiki/Enigma_\(Maschine\)](http://de.wikipedia.org/wiki/Enigma_(Maschine))
- [29] o.V.: Homophone Verschlüsselung – Wikipedia
http://de.wikipedia.org/wiki/Homophone_Verschl%C3%BCsselung
- [30] o.V.: Rabin-Kryptosystem – Wikipedia
<http://de.wikipedia.org/wiki/Rabin-Kryptosystem>
- [31] o.V.: Merkle-Hellman-Kryptosystem – Wikipedia
<http://de.wikipedia.org/wiki/Merkle-Hellman>
- [32] o.V.: RSA-Kryptosystem – Wikipedia
<http://de.wikipedia.org/wiki/RSA-Kryptosystem>
- [33] o.V.: Briefgeheimnis – Wikipedia
<http://de.wikipedia.org/wiki/Briefgeheimnis>
- [34] o.V.: Hybride Verschlüsselung – Wikipedia
<http://de.wikipedia.org/wiki/Hybridverschl%C3%BCsselungsverfahren>
- [35] o.V.: Needham-Schroeder-Protokoll – Wikipedia
<http://de.wikipedia.org/wiki/Needham-Schroeder-Protokoll>
- [36] o.V.: RC6 – Wikipedia
<http://de.wikipedia.org/wiki/RC6>
- [37] o.V.: RC5 – Wikipedia
<http://de.wikipedia.org/wiki/RC5>
- [38] o.V.: RC2 (Verschlüsselungsverfahren) – Wikipedia
[http://de.wikipedia.org/wiki/RC2_\(Verschl%C3%BCsselungsverfahren\)](http://de.wikipedia.org/wiki/RC2_(Verschl%C3%BCsselungsverfahren))
- [39] o.V.: Asymmetrisches Kryptosystem – Wikipedia
http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem
- [40] o.V.: WPA2 – Wikipedia
<http://de.wikipedia.org/wiki/WPA2>
- [41] o.V.: Twofish – Wikipedia
<http://de.wikipedia.org/wiki/Twofish>
- [42] o.V.: Blockverschlüsselung – Wikipedia

- <http://de.wikipedia.org/wiki/Blockchiffre>
- [43] o.V.: Symmetrisches Kryptosystem – Wikipedia
http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem
- [44] o.V.: Verschiebechiffre – Wikipedia
<http://de.wikipedia.org/wiki/Verschiebechiffre>
- [45] o.V.: Stromverschlüsselung – Wikipedia
<http://de.wikipedia.org/wiki/Stromchiffre>
- [46] o.V.: Wikipedia:WikiProjekt Kryptologie – Wikipedia
http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie
- [47] o.V.: Wapedia - Wiki: Kryptographie
<http://wapedia.mobi/de/Kryptographie?t=5>.
- [48] o.V.: -
www.w3l.de/w3lmedia/W3L/Medium107200/Leseprobe9783937137896.pdf
- [49] o.V.: Briefgeheimnis für eMails? - jswelt - Forum (Javascript, PHP, MySQL, AJAX, Webdesign)
<http://forum.jswelt.de/internet-and-recht/13175-briefgeheimnis-f-r-emails.html>
- [50] o.V.: Verschiebechiffre – Wikipedia
<http://de.wikipedia.org/wiki/C%C3%A4sar-Chiffre>
- [51] o.V.: Signatursystem – Wikipedia
<http://de.wikipedia.org/wiki/Signaturverfahren>
- [52] o.V.: Steganographie – Wikipedia
<http://de.wikipedia.org/wiki/Steganographie>
- [53] o.V.: Altägyptische Kryptographie – Wikipedia
http://de.wikipedia.org/wiki/Alt%C3%A4gyptische_Kryptographie
- [54] o.V.: Geschichte der Kryptographie – Wikipedia
http://de.wikipedia.org/wiki/Geschichte_der_Kryptographie
- [55] o.V.: Verschlüsselung – Wikipedia

- <http://de.wikipedia.org/wiki/Verschl%C3%BCsslung>
- [56] o.V.: Hybride Verschlüsselung – Wikipedia
<http://de.wikipedia.org/wiki/Hybridverschl%C3%BCsslungsverfahren>
- [57] o.V.: Wapedia - Wiki: Kryptographie
<http://wapedia.mobi/de/Kryptographie>
- [58] o.V.: Kryptologie – Wikipedia
<http://de.wikipedia.org/wiki/Kryptologie>
- [59] o.V.: Kryptographie – Wikipedia
<http://de.wikipedia.org/wiki/Kryptographie>
- [60] Pommerening, Klaus: Kryptographische Protokolle: Hybride Verschlüsselung
<http://www.staff.uni-mainz.de/pommeren/DSVorlesung/KryptoProt/Hybrid.html>
- [61] Schneider, Iris; Christ, Jürgen: E-MAIL: Das verlorene Briefgeheimnis - Medien - FOCUS Online
http://www.focus.de/kultur/medien/e-mail-das-verlorene-briefgeheimnis_aid_173849.html
- [62] Thöing, Christian: Kryptographie - Kryptoanalyse
<http://www.kuno-kohn.de/crypto/crypto/analysis.htm>
- [63] Verlag DATACOM Buchverlag GmbH: Stromchiffre :: stream cipher :: Definition :: IT-Lexikon
<http://www.itwissen.info/definition/lexikon/Stromchiffre-stream-cipher.html>
- [64] Verlag Heinz Heise GmbH & Co. KG: heise online - 08.12.03 - RSA-576 geknackt
<http://www.heise.de/newsticker/RSA-576-geknackt--/meldung/42719>
- [65] Verlag süddeutsche: Verschlüsselte E-Mails - Das elektronische Briefgeheimnis - Computer - sueddeutsche.de
<http://www.sueddeutsche.de/computer/20/320889/text/>

7 Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst

und keine anderen Hilfsmittel als angegeben habe. Insbesondere versichere ich, dass ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken als solche kenntlich gemacht habe.

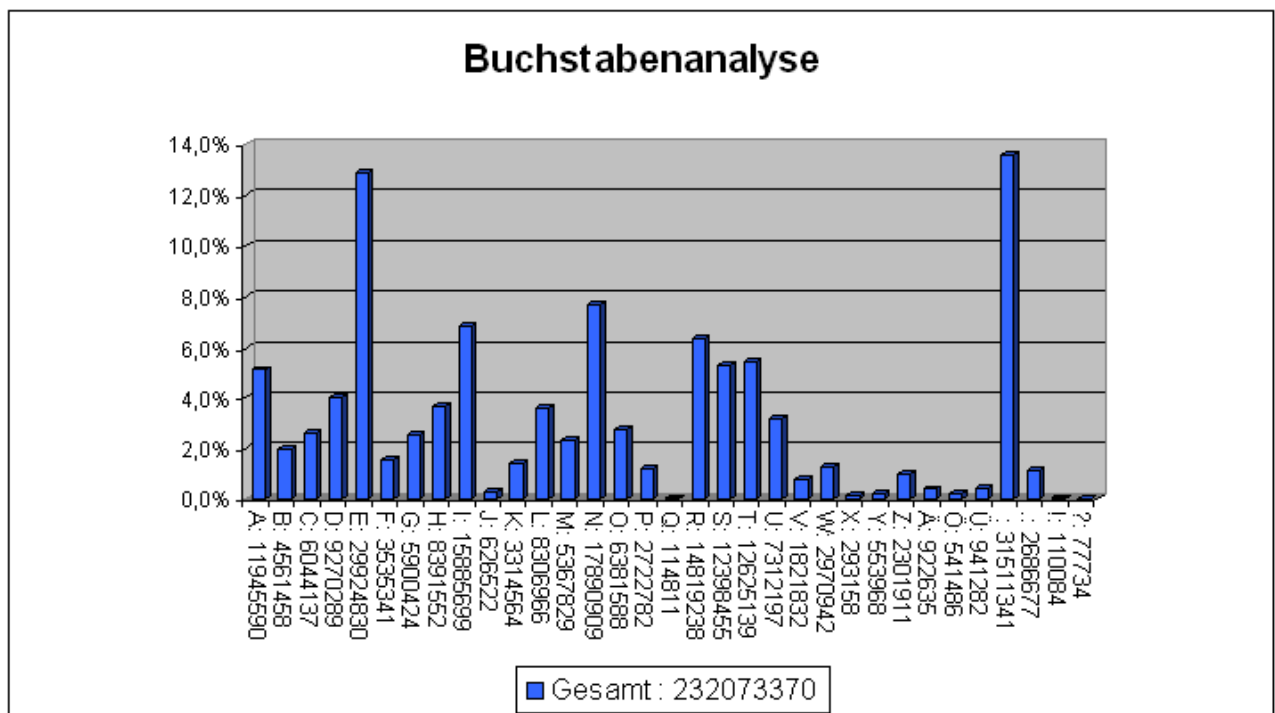
Ort:

Datum:

Unterschrift:

8 Anlagen

Anlage 1: grafische Darstellung der Buchstabenhäufigkeit



Quelle: [http://de.wikipedia.org/w/index.php?](http://de.wikipedia.org/w/index.php?title=Bild:Alphabet_hufigkeit.png&filetimestamp=20040616203300)

[title=Bild:Alphabet_hufigkeit.png&filetimestamp=20040616203300](http://de.wikipedia.org/w/index.php?title=Bild:Alphabet_hufigkeit.png&filetimestamp=20040616203300)

Author: Arbeitsgruppe EBUSS (Potsdam, Mosbach) 2004