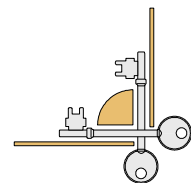
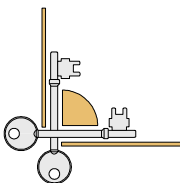


Inhaltsverzeichnis

<i>Kryptografie - Was ist das ?</i>	2
<i>Grundbegriffe der Kryptografie</i>	2
<i>Beispiele</i>	3
<i>Klassische Kryptografie</i>	4
<i>Verschlüsselungsverfahren</i>	4
<i>Caesar-Chiffre</i>	4
<i>Polyalphabetische Verschlüsselung</i>	5
<i>One Time Pad</i>	5
<i>Vigenère-Chiffre</i>	6
<i>Produkt-Chiffre</i>	6
<i>Autokey-Verfahren</i>	7
<i>Summen-Verfahren</i>	7
<i>Enigma</i>	8
<i>Pseudozufallsfolgen</i>	8
<i>Kryptografie in Deutschland</i>	9
<i>Ein Beispiel der Kryptografie: Die Geheimfolie</i>	9
<i>Die wichtigsten Begriffe auf einen Blick</i>	11
<i>Quellenverzeichnis</i>	13





Kryptografie - Was ist das ?

Bei der Kryptografie geht es um die Idee, wichtige Informationen vor anderen Personen zu verbergen. Dabei bedient man sich der Chiffrierung, also der Verschlüsselung. Man codiert die Informationen und gibt den Schlüssel nur an Personen weiter, welche diese Informationen lesen dürfen. Nur anhand dieses Schlüssels ist es möglich, die Codierung wieder rückgängig zu machen und so die ursprünglichen Daten zu erhalten.

Im Laufe der Jahrzehnte wurden unzählige Verfahren zur sicheren Verschlüsselung entwickelt. Keines hat sich bis heute als sicher bewiesen, immer ist es gelungen, die Informationen durch systematisches ausprobieren, durch zufälliges Mithören oder sei es einfach nur durch Glück zu knacken. Sehr oft erledigen Computer diese Arbeit. In einigen Wettbewerben hat man dazu mehrere tausend Computer zusammengeschlossen und diese auf den Schlüssel angesetzt. Nach 3 oder 4 Monaten haben diese dann die Informationen offenbart, die eigentlich als absolut sicher galten. In letzter Zeit jedoch scheint man Systeme gefunden zu haben, die nicht zu entschlüsseln sind, wenn man nicht den passenden Schlüssel hat. Der Unterschied zu den herkömmlichen Verfahren ist, daß hier nirgendwo der Schlüssel gespeichert oder übermittelt wird.

Grundbegriffe der Kryptografie

Verschlüsseln

Kodieren (= encode, encrypt)
Der zugehörige Schlüssel (key) heie V (fr Verschlsseln)

Entschlsseln

Dekodieren (= decode, decrypt)
Der zugehrige Schlssel (key) heie E (fr Entschlsseln)

Symmetrische Verschlsslung

Aus V lt sich E berechnen

Asymmetrische Verschlsslung

Aus V lt sich E nicht berechnen

Beispiele

Beispiel für Symmetrische Verschlüsselung

Wir denken uns die Nachricht als eine endliche Folge von Zahlen. Verschlüsselt wird, indem jede Zahl dieser Folge mit einer festen Zahl (z. B. 3) multipliziert wird. V sei also 3, dann ist $E = 1/3$!

Die Symmetrische Verschlüsselung besitzt folgende typische Eigenschaften:

- Aus V lässt sich E , und aus E lässt sich V berechnen
- V und E lassen sich beliebig vertauschen, ohne dass dies eine Auswirkung auf die Verschlüsselung hat (hier also $V = 1/3$ und $E = 3$)

Beispiel für Asymmetrische Verschlüsselung

Verwenden wir hier zur Verdeutlichung das Beispiel der Symmetrischen Verschlüsselung. Allerdings nehmen wir an, es sei uns nicht möglich, aus $V = 3$ den Schlüssel $E = 1/3$ zu berechnen. Wir tun also so, als wären wir nicht in der Lage, zu dividieren.

Die Asymmetrische Verschlüsselung besitzt folgende Eigenschaften:

- Aus V lässt sich **nicht** E , und aus E lässt sich **nicht** V berechnen
- V und E lassen sich beliebig vertauschen, ohne dass dies eine Auswirkung auf die Verschlüsselung hat)
- Weil sich aus V der Schlüssel E nicht berechnen lässt, kann man V ohne Vorsichtsmaßnahmen verteilen. V heißt daher Öffentlicher Schlüssel (Public Key). E heißt übrigens Privater Schlüssel (Secret Key, Private Key)

Verschlüsselt wird mit ganzen Zahlen von 100 und mehr Dezimalstellen. Diese Zahlen lassen sich also nicht in der Form "... x 10 ^ ..." ausdrücken, müssen also mit Integer Arithmetik behandelt werden. Die Standard Integer Arithmetik kennt nur Zahlen bis zur Länge von 32 Bit, also etwas über 4 Milliarden (10-stellige Zahlen). Die Rechenzeit im Umgang mit 100-stelligen Zahlen liegt schnell im Bereich mehrere Stunden, womit diese Art der Verschlüsselung nur für kurze Nachrichten brauchbar ist.

Klassische Kryptografie

Voraussetzungen für eine geheime Übermittlung sind, dass

- der Empfänger den Schlüssel kennt, den der Sender verwendet hat
- niemand sonst den Schlüssel kennt
- es ohne Kenntnis des Schlüssels unmöglich oder zumindest außerordentlich schwierig ist, den Klartext zurückzugewinnen

Die Schwierigkeiten liegen darin, dass Sender und Empfänger

- einen gemeinsamen Schlüssel vereinbaren müssen, bevor sie geheime Botschaften austauschen können
- den Schlüssel geheimhalten müssen
- ein sicheres Verschlüsselungsverfahren finden müssen

Verschlüsselungsverfahren

Caesar-Chiffre

Gegeben sei ein Alphabet mit 26 Buchstaben (A ... Z). Der Klartext **Abendzeit** soll verschlüsselt werden. Die einfachste Form der Verschlüsselung ist, jeden Buchstaben des Klartextes durch z. B. den übernächsten Buchstaben im Alphabet zu ersetzen (gemäß der alphabetischen Reihenfolge und zyklisch, d.h. auf Z folgt wieder A). Das Ergebnis ist der Geheimtext **Cdgpfbgkv** !

Mathematisch entspricht diese Verschlüsselung einer buchstabenweise "Addition" des Textes CCCCCCCC zum Klartext. Werden die Buchstaben entsprechend der alphabetischen Reihenfolge von 0 bis 25 numeriert, so ergibt sich die Summe zweier Buchstaben aus der Summe dieser Nummern modulo 26.

	C	C	C	C	C	C	C	C	C
+	A	B	E	N	D	Z	E	I	T
	C	D	G	P	F	B	G	K	V

Der Empfänger kann aus dem Geheimtext den Klartext wieder zurückgewinnen. Er muss dazu wissen, mit welchem Algorithmus die Verschlüsselung vorgenommen wurde (hier: Addition), und er muss den Schlüssel C kennen. Durch Umkehrung des Verschlüsselungsalgorithmus (also hier: Subtraktion) unter Verwendung des richtigen Schlüssels ergibt sich wieder der Klartext

	C	D	G	P	F	B	G	K	V
-	C	C	C	C	C	C	C	C	C
	A	B	E	N	D	Z	E	I	T

Dieses Verschlüsselungsverfahren bezeichnet man als Caesar-Chiffrierung !



Die Entschlüsselung des Geheimtextes ohne Kenntnis des Schlüssels bezeichnet man als Kryptanalyse.

Im einfachsten Fall gelingt die Kryptanalyse durch Ausprobieren aller Möglichkeiten. Im Falle der Caesar-Chiffre gibt es nur 26 verschiedene Schlüssel. Woher will man aber wissen, dass $k = C$ und der Klartext Abendzeit, nicht jedoch $k = D$ und der Klartext Zadmcydhs ist? Dies liegt offenbar an der sogenannten Redundanz der Sprache. In unserer Sprache sind nicht alle Zeichenfolgen gleich wahrscheinlich, sondern die Zeichenfolge Abendzeit z. B. ist sehr wahrscheinlicher als Zadmcydhs!

Aufgrund der Wahrscheinlichkeit ergibt sich ein Ansatzpunkt für die Entschlüsselung von Wörtern. Wählt man für den Algorithmus f anstelle einer Verschiebung um i Symbole im Alphabet eine beliebige Permutation (Vertauschung) des Alphabets, so gibt es hierfür $26! \approx 10^{26}$ Möglichkeiten. Diese kann man natürlich nicht alle ausprobieren. Des Weiteren kann man nun die Wahrscheinlichkeit bestimmter Buchstaben einer Sprache hinzuziehen. E ist der häufigste Buchstabe in der deutschen Sprache. Nimmt man nun den am meisten vorkommenden Buchstaben im Geheimtext (G) und verschiebt diesen auf E, so erhält man bereits den Schlüssel C. Die nächsthäufigsten Buchstaben sind N, I, S, R, A und T. Oft kann man aufgrund dieser Entsprechungen den Klartext bereits erraten.

Kann für die Kryptanalyse lediglich der Geheimtext herangezogen werden, wird dies als **Ciphertext-only-attack** bezeichnet. Ist auch ein Teil des Klartextes bekannt, so wird die Kryptanalyse **Known-plaintext-attack** bezeichnet.

Häufig ist es auch möglich, den Klartext zu erraten. So ist es z. B. wahrscheinlich, dass in einem kirchlichen Text das Wort "Amen" häufiger vorkommt oder dass eine persönliche eMail mit dem Wort "Hallo" beginnt!

Im Falle der Caesar-Chiffre genügt die Kenntnis eines einzigen Klartextzeichens zusammen mit dem entsprechenden Geheimtextzeichen, um den Schlüssel k bestimmen zu können. Bei Verschlüsselung mit einer beliebigen Zuordnung von Buchstaben zu anderen Buchstaben (z. B. $A \Rightarrow D$; $B \Rightarrow V$, usw.) benötigt man einen Klartext, in dem die wichtigsten Buchstaben mindestens einmal vorkommen. Dadurch kann man die Zuordnung zu den entsprechenden Geheimtextzeichen ermitteln. Die restlichen Buchstaben ergeben sich aus dem Sinnzusammenhang.

Polyalphabetische Verschlüsselung

One Time Pad

Werden bei der Verschlüsselung die Buchstaben des Klartextes nicht immer durch denselben Buchstaben ersetzt, also beispielsweise A nicht immer durch C, sondern mal durch Z, mal durch E, mal durch B usw., so ist eine statistische Analyse nach obigem Muster nicht möglich. Eine solche Verschlüsselung bezeichnet man als **polyalphabetische Verschlüsselung**.

	T	X	E	D	U	B	N	H	W
+	A	B	E	N	D	Z	E	I	T
	T	Y	I	Q	X	A	R	P	P



Ist der Schlüssel eine gleich verteilte Zufallsfolge von Buchstaben, so ist dieses Verschlüsselungsverfahren sogar absolut sicher. Dies liegt daran, dass es genauso viele mögliche Schlüssel wie mögliche Klartexte gibt, jeder Schlüssel gleichwahrscheinlich ist und somit auch jeder aus dem Geheimtext rekonstruierte Klartext gleich wahrscheinlich ist. Niemand kann sagen, ob der Schlüssel Txedubnhw oder Ykrephypi war. Im einen Falle wird der Geheimtext Tyiqxarpp zu Abendzeit entschlüsselt, im anderen Fall zu Vormittag.

Eine Verschlüsselung durch Addition einer Zufallsfolge heißt **Vernam-Chiffre** oder **One-Time-Pad**.

Vigenère-Chiffre

Eine weitere Methode der Verschlüsselung ist, einen periodischen Schlüssel zu verwenden, der durch Aneinanderreihung eines kurzen Wortes entsteht, z. B. das Wort „Zebra“. Diese Art der Verschlüsselung wird **Vigenère-Chiffre** genannt.

	Z	E	B	R	A	Z	E	B	R
+	A	B	E	N	D	Z	E	I	T
	Z	F	F	E	D	Y	I	J	K

Auch bei diesem Verfahren wird z. B. das E mal auf F und mal auf I abgebildet, so dass eine statistische Analyse nicht zum Ziel führt.

Dennoch ist bei periodischen Schlüsseln eine statistische Kryptanalyse möglich. Bei einem Schlüsselwort der Länge 2 beispielsweise müssen 2 Statistiken erhoben werden – eine für die ungeraden und eine für die geraden Positionen des Geheimtextes. Die Länge des Schlüsselwortes wird durch Ausprobieren ermittelt.

Produkt-Chiffre

Die Periode des Schlüssels lässt sich verlängern, indem der Schlüssel in Teilschlüssel der Länge 2, 3, 5, 7, 11 ... zerlegt wird und der Klartext nacheinander mit diesen Teilschlüsseln verschlüsselt wird. Dies ist gleichbedeutend damit, dass aus den Teilschlüsseln zunächst ein Produktschlüssel gewonnen wird, mit dem dann der Klartext verschlüsselt wird. Die Periode des Produktschlüssels ist das Produkt der Teilschlüssellängen, die Schlüssellänge selbst ist aber nur gleich der Summe der Teilschlüssellängen. Bereits mit einem Schlüssel der Länge $77 = 2 + 3 + 5 + 7 + 11 + 13 + 17 + 19$ lässt sich ein Produktschlüssel der Periode 10^7 erzeugen.

Beispiel

Der Schlüssel sei **Woistreval**, Teilschlüssel sind demzufolge Wo, ist und Reval. Der Produktschlüssel hat die Periode 30. Er errechnet sich wie folgt:

	W	O	W	O	W	O	W	O	W	O	W	O	W	O	W	O	W	O		
+	I	S	T	I	S	T	I	S	T	I	S	T	I	S	T	I	S	T	I	S
+	R	E	V	A	L	R	E	V	A	L	R	E	V	A	L	R	E	V	A	L
	V	K	K	W	Z	Y	I	B	P	H	F	L	Z	G	A	N	S	C	E	R



(Aus Platzgründen sind hier nur die ersten 20 Zeichen aufgeführt)

Autokey-Verfahren

Die Idee beim Autokey-Verfahren ist, einen kurzen Schlüssel durch den Klartext selber zu verlängern.

Beispiel

Der Schlüssel sei **Argo**

	A	R	G	O	E	I	N	G	E	H	E	I	M
+	E	I	N	G	E	H	E	I	M	T	E	X	T
	E	Z	T	U	I	P	R	O	Q	A	I	F	F

Dieses Verfahren ist natürlich gegenüber einer known-plaintext-attack extrem unsicher. Aber auch durch statistische Analyse des Geheimtextes lässt sich der Klartext rekonstruieren. Der am häufigsten vorkommende Buchstabe im Geheimtext (im obigen Beispiel das I) entspricht an den meisten Positionen der Kombination E und E. Ist die Länge s des Schlüssels bekannt, so lässt sich ausgehend von diesen Positionen jedes s -te Klartextzeichen entschlüsseln.

Summen-Verfahren

Eine ähnliche Methode wie die des Autokey-Systems wird bei dem Summen-Verfahren angewandt. Jeder Klartextbuchstabe wird durch die Summe der s vorhergehenden Buchstaben und des Buchstabens selber verschlüsselt. Dadurch sollen die unterschiedlichen Buchstabenhäufigkeiten über einen Bereich der Länge $s + 1$ gemittelt werden, so dass eine statistische Analyse zu keinem Ergebnis führt. Die so vorhergehenden Buchstaben des ersten klartextbuchstabens werden wiederum durch einen Schlüssel der Länge s gebildet.

Beispiel

Der Schlüssel sei Key

	K	E	Y	E	I	N	G	E	H	E	I	M	T
+	E	Y	E	I	N	G	E	H	E	I	M	T	E
+	Y	E	I	N	G	E	H	E	I	M	T	E	X
+	E	I	N	G	E	H	E	I	M	T	E	X	T
	Q	O	X	F	F	E	V	X	F	R	R	G	N



Enigma

Wenn die Periode des Schlüssels sehr lang wird, ist eine Entzifferung schwierig oder sogar unmöglich. Das Problem liegt jedoch darin, dass sehr lange Schlüssel in der Praxis schwer zu handhaben sind. Als Lösung wird versucht, einen langen Schlüssel aus einem kurzen zu erzeugen, aber nicht durch bloße Aneinanderreihung des kurzen Schlüssels, sondern auf komplizierte Art und Weise. In der im Zweiten Weltkrieg verwendeten deutschen Verschlüsselungsmaschine **Enigma** befinden sich drei Rotoren, die sich ähnlich wie ein Kilometerzähler bei jedem Buchstaben weiterdrehen. In jedem Rotor ist eine Permutation des Alphabets fest verdrahtet. Die Permutationen aller drei Rotoren sind hintereinander geschaltet. Auf diese Weise entsteht eine große Zahl unterschiedlicher Kombinationen und jedes Symbol des Klartextes wird mit einer anderen Permutation verschlüsselt. Als Parameter dieses Verschlüsselungsverfahrens war lediglich die Anfangsstellung der Rotoren zu übermitteln.

Lediglich aus Kenntnis des Geheimtextes ist dieser Code nicht zu entschlüsseln. Das Problem ist jedoch, dass nicht nur der Schlüssel, sondern insbesondere die Rotoren geheimzuhalten sind. Außerdem ist dieses Verfahren ebenfalls nicht gegenüber einer known-plaintext-attack sicher. Der Enigma wurde übrigens von den Polen sowie den Engländern recht schnell geknackt.

Pseudozufallsfolgen

Die zuletzt erläuterten Verfahren haben alle das Problem, dass aus einem relativ kurzen Schlüssel ein langer erzeugt wird. Gelingt es, die Systematik der Schlüsselgenerierung herauszufinden, so ist der lange Schlüssel nicht sicherer als der kurze.

Nur wenn der lange Schlüssel keiner Systematik unterliegt, wie dies beim *One-Time-Pad* der Fall ist, ist das Verfahren absolut sicher. Der Nachteil ist, wie bereits erwähnt, der lange Schlüssel, der hierfür notwendig ist.

Naheliegender ist daher die Idee, anstelle der beim *One-Time-Pad* verwendeten Zufallsfolge eine Pseudozufallsfolge zu verwenden. Sender und Empfänger verwenden denselben Zufallszahlengenerator. Sie brauchen nur den Startwert des Zufallszahlengenerators zu vereinbaren und können somit dieselbe Zufallsfolge erzeugen. Das Problem des Austauschs eines langen Schlüssels entfällt !

Allerdings beinhaltet eine Pseudozufallsfolge, auch wenn sie zufällig aussieht, eine sehr starke Systematik, nämlich die des Zufallszahlengenerators. Schon wenige Zeichen des Klartextes zusammen mit dem entsprechenden Geheimtext reichen aus, um diese Systematik zu durchschauen und alle weiteren und vorhergehenden Zufallszeichen zu erzeugen.



Kryptografie in Deutschland

Zwischen dem Interesse des Einzelnen und dem des Staates an Geheimhaltung besteht ein – eigentlich natürlicher – Gegensatz: der Einzelne will seine Informationen und Daten vor der Einsicht anderer Personen schützen, der Staat hingegen will jede Information mitlesen können, um die Gesellschaft vor Verbrechen zu schützen.

Der Anspruch des Staates erscheint unberechtigt und sowieso nicht durchsetzbar. Es gibt eine Verschlüsselung der Verschlüsselung, also Verfahren, mit denen eine geheime Information innerhalb einer frei einsehbaren Nachricht – z. B. einem Bilddokument – versteckt wird. Die Wissenschaft, die sich mit dieser Art der Verschlüsselung befasst, heißt Steganographie. Zu den typischen Vorreitern gehört die „unsichtbare“ Tinte aus Milch oder Weinessig, die erst unter Wärmezufuhr sichtbar wird.

Ein Beispiel der Kryptografie: Die Geheimfolie

Ein sehr gutes Beispiel für die Verschlüsselung von Daten wurde in der diesjährigen Juli-Ausgabe des Magazins „Spektrum der Wissenschaft“ beschrieben. Hierbei geht es um die sogenannte „Geheimfolie“.

Empfänger und Sender besitzen jeweils eine Folie, die aus schwarzen und weißen, kleinen Quadraten besteht. Die Folie des Senders enthält den Chiffretext, die Folie des Senders das Muster zum Entschlüsseln der überbrachten Informationen. Nur durch übereinanderlegen dieser beiden Folien ist es möglich, den Klartext zu erhalten. Eine Manipulation der Daten irgendwo auf dem Wege zwischen Sender und Empfänger ist nicht möglich, ohne dass es dem Empfänger sofort auffällt, da das Muster der beiden Folien zu keinem korrekten Ergebnis führt.

Die Idee dieser neuen Art der Verschlüsselung basiert darauf, dass Computer zwar jede Art der Rechenoperation durchführen können, aber nicht über solche Fähigkeiten wie Sehen verfügen. Die zu überbringende Information wird durch ein Bild übermittelt. Selbst einen Text kann man ohne Probleme als Bild darstellen. Man nimmt hierfür ein Schwarz-Weiß-Bild, welches genau wie beim Computer oder Fernseher in kleine Quadrate (Pixel) aufgeteilt ist. Diese Pixel sind entweder schwarz oder weiß. Zur Erstellung des Schlüssels werden diese Quadrate in jeweils 4 weitere Quadrate, sogenannte Subpixel, aufgeteilt. Von diesen 4 Subpixeln werden nun jeweils 2 weiß und zwei schwarz gefärbt. Hierfür gibt es genau 6 Möglichkeiten, welche entscheidet immer der Zufall. Aus der Entfernung betrachtet ergibt die gesamte Folie ein gleichmäßig graues Bild, da genau die Hälfte schwarz ist und schwarz und weiß gleichmäßig verteilt sind.





Die 6 Möglichkeiten der unterschiedlichen Färbung der Subpixel

Aus Klartext und Schlüssel ergibt sich der verschlüsselte Text nach folgendem System:

- Ist das Klartextpixel weiß, so wird das zugehörige Pixel des Schlüssels, welches sich an der gleichen Position auf der anderen Folie befindet und aus den vorher beschriebenen 4 Subpixeln besteht, unverändert in den Chiffretext übernommen
- Ist der Klartext an dieser Stelle schwarz, so werden Schwarz und Weiß des Schlüsselpixels vertauscht.

Als Ergebnis ist der Chiffretext jetzt wieder ein Bild, welches aus lauter halb-schwarzen Pixeln besteht und auf die Entfernung betrachtet ein genauso graues Bild ergibt wie der Schlüssel. Selbst aus der Nähe betrachtet gibt dies für Außenstehende nicht mehr als eine eher zufällige Anordnung von schwarzen und weißen Kästchen.

Wie wird nun die Information wieder entschlüsselt ?

Bringt man nun beide Informationsteile, Chiffretext und Schlüssel, auf Folien und legt diese exakt übereinander auf einen Overhead-Projektor, so erscheint das ursprüngliche Bild. An den Stellen, wo im Klartext ein weißes Pixel war, kommen in den Subpixeln von Schlüssel und Chiffretext schwarz auf schwarz sowie weiß auf weiß. Durch die Hälfte des gesamten Quadrats dringt also nun das Licht des Projektors. Dies ergibt für das menschliche Auge einen grauen Punkt. Bei einem schwarzen Klartextpixel trifft dagegen Weiß auf Schwarz und umgekehrt. An dieser Stelle dringt also kein Licht hindurch, der Punkt erscheint schwarz. Aus einem ursprünglich schwarzweißen Bild wird ein schwarzgraues. Dies ist jedoch für das menschliche Auge kein Problem, da das Sehsystem Unterschiede in der Gesamthelligkeit automatisch ausgleicht.

Rückschlüsse und Berechnungen des Ursprungsbilds oder des Klartextes anhand des Chiffretextes ist unmöglich, denn der Chiffretext besitzt alle Merkmale einer Zufallsfolge.

Nehmen wir an, es geht um die Übermittlung einer Preisangabe zwischen dem Käufer und dem Verkäufer. Eine Zwischenstelle will nun eine Manipulation der Daten, sagen wir eine Erhöhung der Preises machen. Die Art der Verschlüsselung ist allgemein bekannt und nicht sonderlich kompliziert. Die Zwischenstelle könnte also nun eine neue Preisangabe erzeugen und diese einschleusen. Der Empfänger würde dies nicht bemerken. Deswegen ist es besser, wenn dem Empfänger ein ihm geläufiges Bild übermittelt wird, welches er auf Anhieb erkennt und den Sender als echt authentifiziert. Außerdem kann man mehrere Folien übermitteln, von denen eine angibt, an welcher Position der nächsten Folie sich die korrekte Preisangabe befindet.



Die wichtigsten Begriffe auf einen Blick

Algorithmus

Bei der Datenverschlüsselung beschreibt der Algorithmus das Verfahren, mit dem die Daten codiert werden. Je ausgeklügelter dieser Algorithmus ist, desto sicherer ist die Verschlüsselung.

Brute Force

Übersetzt bedeutet der Begriff soviel wie „rohe Gewalt“. Hier werden sämtliche Schlüssel- bzw. Passwortkombinationen ausprobiert, bis die richtige gefunden ist. Brute Force kommt meist erst zum Einsatz, wenn alle anderen Verfahren erfolglos waren. Denn diese Methode kann extrem zeitaufwendig sein, je nachdem, welche Rechnerleistung zur Verfügung steht und wie lang das Passwort ist. Geht man von 92 möglichen Zeichen aus (Großbuchstaben + Kleinbuchstaben + Zahlen + gängige Sonderzeichen), ist die Anzahl der möglichen Passwörter 92^n , wobei n die Passwortlänge ist. Auf einem Pentium-166-MHz-PC testeten einige Entschlüsselungsprogramme bis zu 13.000 Passwörter pro Sekunde. Während ein dreistelliges Passwort unter diesen Voraussetzungen relativ schnell aufgespürt wird – in rund einer Minute –, dürfte der Vorgang bei einem siebenstelligen Kennwort bis zu 181 Jahre dauern. Um mit der Brute-Force-Methode ein achstelliges Passwort bis zum Jahr 2000 herauszufinden, hätte ein Neandertaler den Pentium-Rechner aktivieren müssen!

Geheimtextanalyse

Die Geheimtextanalyse (*cyphertext only attack*) ist eine statistische Methode, das Passwort zu finden. Beispiel: der häufigste Buchstabe in deutschen Texten ist das kleine „e“. Das Programm sucht die am häufigsten vorkommende Sequenz im chiffrierten Text und geht davon aus, dass sie dem „e“ entspricht. Wurde ein simpler Algorithmus zur Verschlüsselung eingesetzt, lässt sich dann ein Teil des Schlüssels errechnen. Dieses Verfahren funktioniert jedoch nicht, wenn das Dokument zu wenig oder gar keinen Text enthält.

Klartextanalyse

Bei der Klartextanalyse (*known plain text attack*) ist dem Hacker ein Teil des unverschlüsselten Textes bekannt, oder es wird vermutet, dass bestimmte Satzteile im Dokument vorkommen. Besonders häufig werden etwa Standardeinleitungen oder Grußformeln probiert. Indem man den Klartext mit dem chiffrierten Text vergleicht, lässt sich so bei einem simplen Algorithmus der Schlüssel errechnen. Auch die Dateistruktur kann als „Klartext“ dienen. Denn sie ist in jedem Dokument eines bestimmten Formats die gleiche und daher allgemein bekannt.

RC4

Der Verschlüsselungs-Algorithmus RC4 bietet durch seine variable \Rightarrow Schlüssellänge ein annehmbares Maß an Sicherheit. Bei Produkten aus den USA ist die Schlüssellänge jedoch oft auf 40 Bits beschränkt.

Schlüssellänge

Mit dem Schlüssel, der normalerweise aus einem Passwort generiert wird, werden die Daten codiert. Die Schlüssellänge hängt ab vom \Rightarrow *Algorithmus*. Je länger der Schlüssel, desto schwieriger ist es, die codierten Daten zu knacken.

Wörterbuch-Suche

Die Wörterbuch-Suche ist eine schnelle Variante der \Rightarrow *Brute-Force-Methode*. Hier wird unterstellt, dass zur Verschlüsselung ein natürliches Wort benutzt wurde – also keine beliebige Buchstabenkombination. Nacheinander werden daher Wörter aus einem Lexikon ausprobiert. Im Internet gibt es Wörterbuch-Dateien in vielen Sprachen, die sich dazu einsetzen lassen. Vorsicht: Hacker erweitern Wörterbücher gerne um Begriffe, die aus dem näheren Umfeld der Person stammen, die die Datei verschlüsselt hat. Dazu zählen etwa Namen von Familienmitgliedern oder Automarken.

Quellenverzeichnis

PC-Welt 10/98 Seite 256 / 275
(Artikel: Software – Kennwortverschlüsselung im Test)

Spektrum der Wissenschaft – Juli 1998 Seite 10 – 114
(Artikel: Mathematische Unterhaltungen – Die Geheimfolie)

Internet-Adressen:

<http://yi.com.home/BaumannJoachim/>

Cliparts:

Die große CD-ROM der Cliparts für Windows – Vemag Computer Bibliothek