revidierter alter und ergänzter Beitrag zur

Kryptographie?

2 Einführung

Francis Bacon (1561 - 1626) schrieb in seinen "Essayes" von 1597: Denn Wissen ist Macht (For knowledge itself is power). Schon immer haben die Mächtigen dieser Welt das Wissen daher gebraucht, um ihre Macht zu erhalten und zu stärken. Auch die Krypta der Grabmale (Katakomben) weist in diese Richtung. Der entsprechende Wortursprung ist griechisch: krypte bedeutet unterirdischer, geheimer Gang, Gewölbe, Gruft; kryptein verbergen, verstecken, verhüllen.

Die uns bekannten, ältesten Verfahren der Geheimhaltung verwendeten vor ca. 2500 Jahren die Herrscher von Sparta. Der Absender und der Empfänger von geheimen Nachrichten besaßen zylindrische Körper (sog. Skytale) von genau gleichem Durchmesser. Der Absender wickelte einen schmalen Streifen aus Pergament um seinen Zylinder und schrieb dann die Nachricht längs auf das Band. Nur das abgewickelte Pergament wurde durch einen Boten zum Empfänger gebracht. Der wickelte es um seinen Zylinder und konnte so den Inhalt lesen.

Auch Julius Caesar (100 bis 44 v. Chr.) benutzte ein Verfahren zur Verschlüsselung seiner vertraulichen Briefe. Dabei wurde jeder Buchstabe durch einen anderen ersetzt. Die Regel hierfür mutet heute geradezu simpel an: Im Alphabet wird jeweils um drei Stellen weiter gegangen. So wird aus A → D, aus B → E usw. Die letzten Buchstaben des Alphabets werden mit dem Anfang verknüpft, d.h. X → A, Y → B und Z → W (Bild 1)

Seitdem sind natürlich weitaus leistungsfähige Verfahren (komplexere Chiffren) entstanden, die fast alle auf einen Algorithmus, also eine Rechnung beruhen. Sie wurden zunächst mit mechanischen Maschinen realisiert. Eines der bekanntesten Geräte ist die 1926 in Berlin-Wannsee entwickelte Rotorchiffriermaschine ENIGMA. Sie wurde im zweiten Weltkrieg vieltausendfach von der deutschen Seite verwendet. Der ENIGMA-Code wurde jedoch schon vor Kriegsausbruch von polnischen Mathematikern geknackt und später an Briten und Franzosen weitergegeben. So konnten die Alliierten bis Kriegsende geheime deutsche Funksprüche entschlüsseln und dem Gegner folgenschwere Verluste zufügen.

Die traditionellen Einsatzgebiete der Verschlüsselung bisher im militärischen Bereich. Mit dem rasanten Aufschwung der elektronischen Datenverarbeitung gewinnen kryptographische Verfahren auch für zivile Anwendungen zunehmend an Bedeutung. Einen wichtigen Schub erlebte die Kryptographie in den siebziger Jahren, als in den USA der erste Verschlüsselungs-Standard (DES) verabschiedet und das Prinzip der öffentlich-bekannten Schlüssel entdeckt wurde.

3 Struktur und Funktion

Das Ziel der Kryptographie besteht stets darin, eine Nachricht während der Übertragung vor Beeinträchtigungen zu schützen (Bild 2). Vor und nach der Übertragung befindet sich eine Botschaft im sicheren Bereich der Kommunikationspartner. Ein zum Chiffrieren vereinbarter Schlüssel muss ebenfalls sicher, z.B. durch persönliche Übergabe, ausgetauscht werden. Während der Übertragung kann die Nachricht Angriffen ausgesetzt sein, der Nachrichtenkanal (z.B. Telefon, Briefpost, Rechnernetz usw.) gilt als unsicher.

Funktionell gilt dabei: Sender und Empfänger müssen (gemeinsam) einen Schlüssel (engl. key) festlegen und austauschen. Er sei K_S für den Sender und K_e für den Empfänger. Später wird sich zeigen, dass beide nicht identisch, wohl aber sorgfältig aufeinander abgestimmt sein müssen. Dann verschlüsselt (C = codiert) der Sender seinen Klartext, die Nachricht N mit diesem Schlüssel und es entsteht der Geheimtext $G = C(K_s,N)$. Er wird über den öffentlichen Kanal übertragen und gelangt so zum Empfänger. Dort wird er dechiffriert (D = decodiert) und es entsteht wieder der Klartext. Also gilt $N = D(K_e,G)$. Für die beiden Schlüssel muss folglich $N = D\{K_e,C(K_s,N)\}$ gelten.

Es werden grundsätzlich zwei Arten der gegnerischen Beeinträchtigung unterschieden:

- *Abhören* (passiver Angriff): Hierbei versucht ein "Lauscher" den Inhalt einer Nachricht zu erfahren.
- *Manipulation* (aktiver Angriff): Der Angreifer versucht die Nachricht zu verändern. Dazu zählen auch das Löschen oder das Wiedereinspielen von Teilen der Nachricht.

Wird der erste Punkt weiter gefasst, so sind dort auch die Vorhaben der Suche nach den Außerirdischen einzuordnen. Sie werden jedoch wahrscheinlich die Nachrichten so codieren, dass wir sie besonders leicht verstehen können. Wie schwierig so etwas sein kann, zeigt *unsere* Botschaft an die Außerirdischen, welche am 16.11.74 vom 300 m-Teleskop in Arecibo ins Weltall gesandt wurde (Bild 3). Stellen sie sich einmal vor, wie sie den Text erkennen würden, wenn die zusätzlichen Aussagen links daneben fehlen.

4 Leistungsmerkmale

Je nach Art und Zweck einer Nachricht müssen die verwendeten kryptographischen Verfahren unterschiedliche Dienste erbringen. Im Laufe der Zeit hat sich eine Anzahl verschiedenartiger Anwendungen und Methoden herausgebildet, bei denen die Schutzwürdigkeit der Übertragung durch fünf wesentliche Sicherheitsattribute beschrieben werden kann:

- Unter *Vertraulichkeit* wird verstanden, dass der Inhalt einer Nachricht gegenüber Nicht-Eingeweihten verborgen werden muss.
- Die *Integrität* einer Nachricht bedeutet, dass ihr Inhalt nicht verändert werden darf, bzw. Mittel zur Verfügung stehen, mit denen Änderungen festgestellt werden können.
- Die *Authentizität* verlangt, dass der Empfänger und/oder der Sender feststellen kann, ob er auch wirklich mit dem gewünschten Partner in Verbindung steht. Sonst könnte es ja möglich sein, dass der Partner ein Gegner ist, der sich nur in den Kanal eingeschlichen hat.

- Die *Nicht-Abstreitbarkeit* entspricht dem Einschreiben mit Rückantwortschein. Der Sender und/oder Empfänger bestätigen durch sie verbindlich die Sendung oder den Empfang einer Nachricht. In dieses Gebiet gehört z.B. eine Anwendung der elektronischen Unterschrift.
- Die *Anonymität* ist ein Sonderfall der elektronischen Kommunikation. Allgemein bekannt und garantiert ist sie bei den öffentlichen Wahlen und vielen soziologischen Umfragen. Ähnliche Fälle treten auch bei der elektronischen Kommunikation auf. Wenn z.B. ein Forschungsinstitut in einer Datenbank recherchiert, so könnte ein Gegner aus den recherchierten Dokumenten ableiten, womit sich die Forschung gerade beschäftigt. Auch für automatisierte statistische Erhebungen sollte sie gewährleistet sein.

5 Grundprinzipien

Für die Kryptographie besteht jeder Text - also sowohl Klar- als auch Geheimtext aus einer Abfolge von Zeichen. Diese Zeichen werden nacheinander gesendet und empfangen. Für eine Verschlüsselung gibt es zwei Prinzipien:

- *Strom*-Chiffren betrachten den Text als Zeichenfolge und wenden die Chiffrierung auf jedes Zeichen einzeln an
- *Block*-Chiffren unterteilen den Text in Blöcke gleicher Länge und verschlüsseln jeden Block nach gleichem Schema

Die Chiffrierung selbst setzt sich immer aus den zwei Grundtechniken *Substitution* (Ersetzung) und *Transposition* (Umstellung) zusammen. Für beide Techniken wurden zunächst getrennte Verfahren entwickelt. Moderne Verschlüsselungsverfahren, wie der DES oder IDEA, mischen beide Techniken und bewirken damit eine enorme Komplexität. Im folgenden werden diese Techniken vorgestellt und die wichtigsten Ansätze zum Knacken solcher Codes aufgezeigt.

6 Einfache Ersetzungschiffren

Im einfachsten Fall der Ersetzungchiffren wird jedes Zeichen k_i des Klartextes durch genau ein anderes g_i des Geheimtextes ersetzt. Die anfangs erwähnte Caesar-Chiffre kann mittels des Bild 1 mechanisch erklärt werden. Es gibt zwei Kränze, die mit dem Alphabet belegt sind. Nun kann der innere Kranz gegenüber dem äußerem um drei Positionen verdreht werden. So stehen im inneren Teil die Zeichen des Klartextes und im äußeren Kranz die des Geheimtextes. Es sei ein einfaches Beispiel gewählt:

Klartext: die stadt rom liegt auf sieben huegeln
Geheimtext: GLH VWDGW URP OLHJW DXI VLEHEQ KXHJHOQ

Mathematisch kann der Zusammenhang durch die Vorschrift $g_i = k_i + 3$ (MOD 26) ausgedrückt werden. Natürlich kann jede der 25 möglichen Positionen des inneren Kreises zur Verschlüsselung vereinbart werden.

Eine Verbesserung dieses Prinzips kann dadurch erreicht werden, daß zusätzlich ein Schlüsselwort (mit lauter verschiedenen Buchstaben) verwendet wird. Die ersten Buchstaben des Klartextalphabet werden dann gemäß dieses Schlüsselwortes ersetzt. Die restlichen Buchstaben werden alphabetisch mit den fehlenden Buchstaben aufgefüllt. Lautet das Schlüsselwort beispielsweise "KEYWORD", so entsteht die folgende Zuordnungstabelle:

Ausgangs-Alphabet: abcdefg hijklmnopqrstuvwxyz
Ersetzungs-Alphabet: *KEYWORD* ABCFGHIJLMNPQSTUVXZ

Das obige Beispiel lautet dann:

Klartext: die stadt rom liegt auf sieben huegeln
Geheimtext: WBO PQKWQ NJH GBODQ KSR PBOEOI ASODOGI

Nach dieser Methode lassen sich weitaus mehr Schlüssel erzeugen.
Die **Kryptoananlyse**, also das Knacken dieser simplen Austauschchiffren ist relativ einfach. In jeder Sprache existiert nämlich eine charakteristische Häufigkeitsverteilung der Buchstaben. Für einen üblichen Text gilt z.B. die Tabelle 1.
Tabelle 1 Nach Häufigkeit in % sortierte Buchstaben eines typischen deutschen Textes.

e	17,40	d	5,08	o	2,51	p	0,79
n	9,78	h	4,76	b	1,89	v	0,67
i	7,55	u	4,35	w	1,89	j	0,27
s	7,27	l	3,44	f	1,66	y	0,04
r	7,00	c	3,06	k	1,21	x	0,03
a	6,51	g	3,01	z	1,13	q	0,02
t	6,15	m	2,53				

Der Geheimtext wird nach der Häufigkeit der Buchstaben untersucht. Geschieht dies für die obige Chiffrierung mit KEYWORD, so ergibt sich für die 32 Zeichen bereits folgende Statistik, wobei die Vergleichswahrscheinlichkeiten auf ganze Prozente gerundet wurden:

Zeichen	Anzahl	Häufigkeit	Vergleich
o	6	18,75	(e) 17,4
q	4	12,50	(t) 6,15
b	3	9,37	(i) 7,55
d, i, k, p, s, w	2	6,25	(g, n, a, s, u, d): 3; 10; 7 ;7 ;4; 5
a, e, g, h, j, n, r	1	3,13	(h, b, l, m, o, r, f): 5; 2; 3; 3; 3; 7; 2

Auch wenn hier im Nachhinein die Zuordnung schon brauchbar erscheint, wird ein so kurzer Text kaum zu korrekt zu knacken sein. Mit der Länge des Texten wird jedoch die Annäherung immer besser, und bereits bei etwa tausend Zeichen ist die Zuordnung fast fehlerfrei.
Diese Methode der Dechiffrierung hat auch auf anderen Gebieten Bedeutung. Der historisch bedeutsamste Fall entstand mit dem Stein von Rosette (Bild 4). Er wurde am unteren Nil in Rosette 1799 von Boussard gefunden und befindet sich heute im Britischen Museum zu London. Er enthält gleiche Texte in Hieroglyphen, demotisch und griechisch. J. F. Campollion entzifferte hieraus mittels statischer Analysen das Hieroglyphische. Die erste Veröffentlichung dazu von 1822 gilt heute als Beginn der Ägyptologie.

7 Polyalphabetische Ersetzung
Die wesentliche Schwäche der einfachen Ersetzungschiffren liegt in der ähnlichen Häufigkeitsverteilung von Klar- und Geheimtext. Daher entstanden die polyalphabetischen Ersetzungen. Hierzu vereinbaren Sender und Empfänger

1. mehrere Ersetzungstabellen (Alphabete) und
2. wann und wie zwischen ihnen gewechselt werden soll.

Im einfachsten Fall werden zwei Alphabete benutzt und zwar das erste für alle Klartext-Buchstaben an geradzahliger Position, das zweite für die ungeradzahligen Stellen:

Klartext: 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
Ersetzung 1: M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
Ersetzung 2: *L K J I H G F E D C B A Z Y X W V U T S R Q P O N M*

Klartext: dieser satz ist verschluesselt
Geheimtext: P*DQTQU* T*MSL* U*TF H*H*DTOEX*R*QTEHX*S

Im Beispiel werden das häufige 'e' und das seltene 'v' je nach Lage auf die Geheimtextbuchstaben 'H' oder 'Q' abgebildet. Während 'e' im Klartext noch fünfmal so oft vorkommt als 'v', tritt deren geheimer Widerpart 'H' und 'Q' jetzt gleich häufig auf. Ein Rückschluss auf die Klartextbuchstaben scheint nicht mehr möglich. Um die Häufigkeiten der Geheim-Textsymbole noch stärker anzugleichen, können weitere Alphabete hinzugezogen werden. Je mehr verschiedene Alphabete eingesetzt werden, desto gleichmäßiger wird die Verteilung. Der Verschlüsselungs-Klassiker hierfür ist das in Bild 5 gezeigte Vignere-Quadrat. Es stammt von dem französischen Diplomaten Blaisse de Vignere (1523-1596). Es enthält 26 verschiedene Ersetzungs-Alphabete, die durch Schlüsselwortbuchstaben referenziert werden. Besaß das Schlüsselwort z.B. 7 Buchstaben, so wird der Klartext zyklisch mit sieben verschiedenen Alphabeten chiffriert.

Für die Krypto-*Analyse* sind drei Schritte zu realisieren

- Zunächst muß die Anzahl der verwendeten Alphabete bestimmt werden.
- Dann sind die Regeln für ihre Anwendung zu finden.
- Schließlich ist der Geheimtext in die Teile für die einzelnen Alphabete zu zerlegen und dafür die statistische, monoalphabetische Analyse durchzuführen.

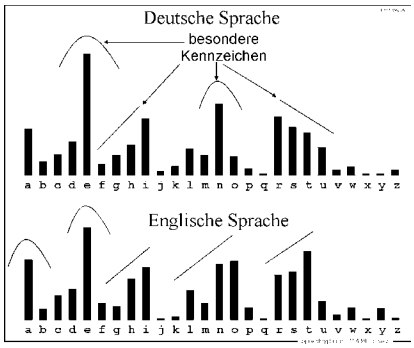
Für die Erkundung der Anzahl der Alphabete sollen zwei Prinzipien beschrieben werden. Das wohl älteste Verfahren geht auf den preußischen Major Kasiski zurück. Es nutzt die Tatsache, daß es in jeder Sprache häufige Buchstaben-*Kombinationen* gibt, wie z.B. im Deutschen die Digramme "st", "en" "in" und die Trigramme "ung", "ein", "ing" usw. Jede einzelne Kombination wird im Geheimtext natürlich unterschiedlich codiert und zwar je nachdem mit welchen Alphabet bei ihm begonnen wurde. Dadurch wiederholen sich gleiche Codierungen an bestimmten Positionen im Text. Nach der Periodizität dieser Positionen ist zu suchen. Daraus ergibt sich dann mit großer Wahrscheinlichkeit die Anzahl der verendeten Alphabete.

Ein weiteres Maß zur Bestimmung der Alphabet-Anzahl bringt die Betrachtung der Buchstabenverteilung im Geheimtext. Dabei wird untersucht, wie stark die Häufigkeit jedes einzelnen Buchstabens vom durchschnittlichen Vorkommen aller Buchstaben abweicht. Aus der gewichteten Summe aller Abweichungen wird die sog. Standardabweichung errechnet:

$$\frac{1}{26}\sum_{i=1}^{26}\left|x_i - \frac{1}{26}\right|$$

mit x_1 = a, x_2 = b ... x_{26} = z. Sie gibt die durchschnittliche Abweichung eines Buchstabens vom arithmetischen Mittel an. Haben alle Buchstaben gleiches Vorkommen, so ist die Standardabweichung Null. In deutschsprachigem Text streuen die Buchstaben jedoch stark um das mittlere Aufkommen (siehe Tabelle 1). Die entsprechende Verteilung weist starke Schwankungen auf. Durch polyalphabetische Ersetzung wird die Anzahl häufiger und seltener Buchstaben angeglichen,

somit wird die Standardabweichung kleiner. Als Beispiel wurden die Buchstaben des vorliegenden Artikels mit ein, zwei und drei Alphabeten ersetzt. Für jede Alphabetanzahl ergibt sich eine typische Abweichung (siehe Bild 6).
Die Streuung der Buchstabenhäufigkeiten hilft also dem Kryptoanalytiker, unter Berücksichtigung des Textumfangs, die Anzahl der verwendeten Alphabete zu erraten.



8 Unknackbar: Der Vernam Chiffre
Es gibt jedoch Ersetzungschiffren, die jeder statistischen Analyse trotzen und erwiesenermaßen nicht geknackt werden können: Die Einmalschlüssel. Sie wurden 1917 von dem amerikanischen Ingenieur Gilbert S. Vernam entdeckt und oft nach ihm benannt. Die Vernamchiffren sind dadurch gekennzeichnet, daß der Schlüssel nur einmal verwendet werden darf. Außerdem muss er mindestens so lang sein wie die Botschaft und darf keine Regelmäßigkeiten enthalten, also rein zufällig sein.
Das Verfahren selbst ist trivial: Zum Chiffrieren wird der Klartext einfach mit dem Schlüssel bitweise addiert und beim Entschlüsseln wieder abgezogen. Die Stärke des Einmalschlüssels: Durch die Verknüpfung von Geheimtext mit der Zufallszahl nimmt der Geheimtext selbst zufälligen Charakter an. Vernams Chiffren haben jedoch auch gravierende Nachteile:

- Für jede Botschaft muss vorher ein Schlüssel sicher übermittelt werden
- Da die Schlüssel mindestens so lang sind wie die Nachricht, könnte diese auch gleich statt des Schlüssels übertragen werden
- Das Erzeugen echter Zufallsfolgen ist technisch aufwendig

Obgleich sich die Einmalschlüssel aus den o.g. Gründen nicht durchsetzen konnten, wurden sie lange Zeit im militärischen und diplomatischen Bereich eingesetzt. So ist bekannt dass Fidel Castro und Che Guevara Vernam-chiffrierte Nachrichten austauschten. Für den heißen Draht zwischen Washington und Moskau werden sie noch immer eingesetzt.

9 Umstellungschiffren
Ein Raster mit Buchstaben kann man horizontal und vertikal lesen. Beispielhaft sind hierfür die Kreuzworträtsel oder in Perfektion die berühmten Textgestaltungen, die eine gewisse Ähnlichkeit mit den Magischen Zahlenquadraten besitzen:

HASE
ABEL
SEIL
ELLE

Wer einmal solche Rätsel gebastelt hat, weiß wie schwer das ist. Hierauf beruhen viele Umstellungchiffren. Es sei vom Klartext

DIESER TEXT HAT FUENF SPALTEN

ausgegangen. Er wird zunächst ohne Leerzeichen in gleich lange Zeilen - Im Beispiel der Länge 5 geteilt - und ergibt so:

DIESE
RTEXT
HATFU
ENFSP
ALTEN

Jetzt wird er spaltenweise senkrecht gelesen und es folgt der Geheimtext:

DRHEAITANLEETFTSXFSEETUPN

Dies lässt sich mehrmals wiederholen. Nun wird der eben erhaltene Geheimtext in Zeilen der Länge 7 aufgeschrieben:

DRHEAIT
ANLEETF
TSXFSEE
TUPN

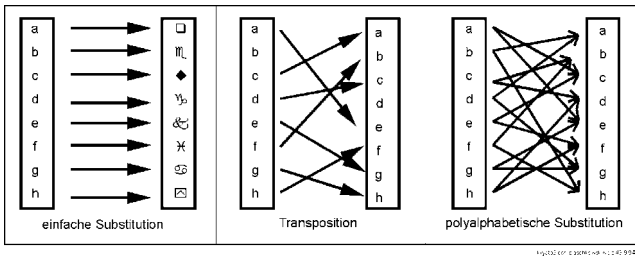
und wiederum spaltenweise senkrecht gelesen.

DATTRNSUHLXPEEFNAESITETFE

Dieses Verfahren kann auf vielfältige Weise wiederholt werden. So entsteht ein völliges "Durcheinander" der Zeichen. Alle verschiedenen Möglichkeiten einen Text der Länge n umzustellen betragen $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. Für die nur 26 Zeichen unseres Mustertextes sind das bereits $26! \approx 4 \cdot 10^{26}$ Möglichkeiten. Wollte man alle Varianten auf einen Rechner durchprobieren und setzt dabei für jeden Versuch nur 1 µs an, so ergeben sich mehr als tausend Jahre Rechenzeit. Dieser Weg ist also für umfangreichere Texte völlig hoffnungslos.
"Knackpunkt" der Kryptoanalyse sind wieder die häufigen Buchstabengruppen. Zunächst werden die Einzelsymbole gezählt, um zu prüfen, ob überhaupt eine Transposition vorliegt. Davon kann ausgegangen werden, falls alle Buchstaben mit ihren normalen Häufigkeiten vorkommen. Danach werden die Geheimtext-Buchstaben betrachtet, die im Klartext oftmals in Gruppen vorkommen (z.B. in Di- oder Trigrammen). Stellt man zwischen solchen Zeichen besonders häufige Abstände fest, so kann man z.B. auf die Spaltenanzahl schließen. Insbesondere dann, wenn der Angreifer zu einem Geheimtext Teile des Klartextes besitzt oder ahnt, erleichtert es ihm die Suche nach dem Umstellungsmuster. Hat sich dieses Muster für einen Teil der Botschaft bestätigt, so ist es wahrscheinlich auch für den Rest gültig.

10 Kriterien für gute Chiffren

Wann ist ein Verschlüsselung-Algorithmus ausreichend sicher? Was macht eine Chiffre "gut genug" für eine spezielle Anwendung? Substitutionen verbergen die Buchstaben des Klartextes; polyalphabetische Ersetzungen lassen eine hohe Streuung der Buchstabenhäufigkeiten entstehen; Transpositionen schichten den Text um und erzeugen ein scheinbar undurchsichtiges Durcheinander (vgl. Bild 7). Alle diese Verfahren für sich besitzen jedoch Schwächen, die einen erfolgreichen Angriff ermöglichen. Insbesondere nach den fatalen Dechiffrierungen in den beiden Weltkriegen wurden Gütekriterien entwickelt, an denen Kryptosysteme gemessen werden. Die wichtigsten Forderungen sind:

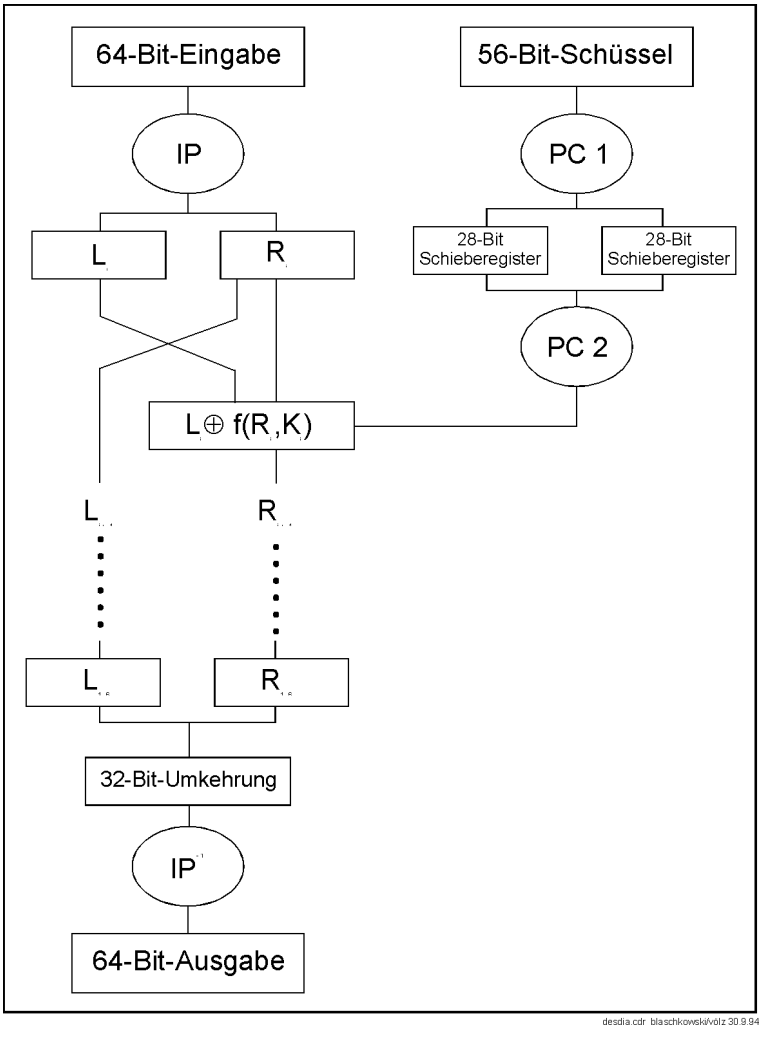


- Der benötigte Grad der Geheimhaltung soll über den Aufwand des Verfahrens entscheiden **(Skalierbarkeit).**
- Die Sicherheit des Systems darf nicht von der Geheimhaltung des benutzten Algorithmus abhängen **(Öffentlichkeit des Verfahrens).**
- Die verwendeten Schlüssel müssen (relativ) kurz und frei wählbar sein. **(Freie Schlüsselwahl).**
- Eine Teildechiffrierung darf nicht auf den ganzen Klartext schließen lassen **(Konfusion)**.
- Eine gegnerische Änderung im Klartext sollte viele Teile des Geheimtextes beeinflussen **(Diffusion)**.

Bei der Implementierung

- sollte die Implementation das Verfahrens so einfach wie möglich sein **(Schnelligkeit),**
- sollten Verarbeitungsfehler sich nicht auf Folgeinformationen auswirken dürfen **(Fehlerfortpflanzung).**

Was also fehlte, war ein Algorithmus, der die Stärken von Substitution und Transposition vereint, leicht zu implementieren ist und dessen Sicherheit einer öffentlichen Prüfung standhält. Weiterhin sollte dieser Algorithmus standardisiert sein, so dass potentielle Kommunikationspartner nur noch ein Verfahren unterstützen mussten. Im Jahr 1974 annoncierte das Standardisierungs-Kommitee der amerikanischen Regierung eine öffentliche Ausschreibung, in der nach einem solchen Algorithmus gesucht wurde. Einer der eingesandten Vorschläge war eine Weiterentwicklung des im Bankwesen eingesetzten Chiffre "Lucifer" der Firma International Business Machines (IBM). Nach 18-monatiger öffentlicher Diskussion, die keine Sicherheitslücken aufdeckte, wurde der Algorithmus als bundesweiter Standard DES (Data Encryption Standard) 1977 verabschiedet. Die große Zahl von Hard- und Softwareimplementierungen machten den DES seither zum weltweit bedeutendsten Verschlüsselungs-Standard.



11 Der DES-Algorithmus

Ebenso wie die traditionelle Kryptographie, verschlüsselt auch der DES-Algorithmus durch Transposition und Substitution. Während früher jedoch einfache Algorithmen mit langen Schlüsseln verwendet wurden, verhält es sich beim DES genau umgekehrt.
Als Vertreter der sogenannten Produkt-Chiffren bewirkt der DES bei kurzem Schlüssel eine hohe Komplexität. Produkt-Chiffren, wie der DES, verwenden zyklisch immer die gleichen Ersetzungs- und Umstellungsmuster. Das Ergebnis eines vorherigen Durchlaufs wird dabei mit dem Schlüssel verknüpft und dient als Eingabe für den kommenden Zyklus. Der Trick dabei ist, dass der Schlüssel in jedem Zyklus teilweise auch "auf sich selbst einwirkt", da die vorliegenden Daten ja im letzten Zyklus mit seiner Hilfe erstellt wurden. Schon nach wenigen Runden gleichen die Ergebnisse Zufallszahlen.

Der DES-Algorithmus verschlüsselt als Block-Chiffre je 64 Bit. Die Grundoperationen, die der er zum Verschlüsseln verwendet sind Substitution, Transposition und bitweise Addition (XOR). Die Substitutionen werden in einfachen Schaltungen realisiert, den sog. S-Boxen, ebenso die Transpositionen (**P**ermutationen) in den P-Boxen (Bild 8).
Den Kern des Algorithmus bildet eine Schleife, in der die Eingabedaten durch S- und P-Boxen ersetzt, umgestellt und mit dem modifizierten 56-Bit-langem Schlüssel verodert werden. In den 16 Durchläufen der Schleife dient jeweils das Ergebnis der vorherigen Runde als Eingabe der aktuellen Iteration, der Schlüssel wird in jedem Durchlauf vor der XOR-Operation modifiziert.
Einen funktionellen Überblick gibt das Bild 9. Als erstes wird der 64-Bit-Eingabevektor einer initialen Permutation (IP) unterzogen, die unmittelbar vor der Ausgabe wieder rückgängig gemacht wird (IP^{-1}). Als nächstes wird der erste von 16 Schleifendurchläufen abgearbeitet. In jeder Iteration *i* wird die Eingabe in je ein linkes (L_i) und rechtes (R_i) 32-Bit-Feld geteilt, K_i bezeichnet den modifizierten Schlüssel im Durchlauf *i*. Pro Runde werden folgende sechs Schritte ausgeführt:
1. Die linke Ausgabe ist die rechte Eingabe, $L_{i+1} = R_i$.
2. Konstruiert 48-Bit-Vektor *E* durch Transposition und Verdoppelung von R_i.
3. Verknüpft *E* und K_i durch exklusives Oder (XOR).
4. Leitet das Ergebnis durch die S-Boxen.
5. Leitet das Ergebnis durch eine P-Box.
6. Verknüpft das Ergebnis aus 5. mit der linken Eingabe durch exklusives Oder (XOR).

Der in 3. aufgeführte Runden-Schlüssel K_i wird für jede Iteration neu berechnet. Dazu wird der 56-Bit-Schlüssel ähnlich wie in der initialen Permutation umgestellt (PC1) und in Schieberegistern je nach Runde um ein oder zwei Stellen bitweise nach links geschoben und erneut umgestellt (PC2). Auf diese Weise erhält jede Runde einen modifizierten Arbeits-Schlüssel.
Nach dem 16. Durchlauf werden die linke und rechte Hälfte vertauscht, und der bereits erwähnten Permutation IP^{-1} zugeführt. Die Ausgabe ist der verschlüsselte 64-Bit-Block.
Die hohe Sicherheit des DES wird im wesentlichen von den Substitutionen in den S-Boxen getragen. Ihr Aufbau ist zwar wohlbekannt, nicht jedoch die Entwurfskriterien, die zur Auswahl der Ersetzungsmuster geführt haben. Diese blieben bis heute das wohlgehütete Geheimnis der Entwickler und des US-amerikanischen Sicherheitsdienstes. Zwar konnte nachgewiesen werden, dass S-Boxen anderen Inhalts die Sicherheit des DES schwächen können, dies brachte jedoch keinen Hinweis auf die Systematik der standardisierten S-Boxen. Kritiker vermuten, dass im Design der S-Boxen eine unerkannte Hintertür verborgen ist, durch welche eingeweihte Regierungsbehörden einen DES-Code leichter knacken können.
Wie alle Block-Chiffren ist der DES-Algorithmus sehr empfindlich gegen Manipulationen eines Text-Blocks. Wie aber wird erkannt, ob nicht ein ganzer Block unbefugt gelöscht oder eingefügt wurde? Zu diesem Zweck wird die Block-Verschlüsselung im sog. cipher-block-chaining-modus (Verkettungsmodus) betrieben. In diesem Modus wird die Ausgabe einer Block-Verschlüsselung verwendet, um den nächsten Eingabe-Block zu modifizieren. Der erste Block wird normal chiffriert (Bild 10). Vor dem Verschlüsseln des nächsten Blocks, wird dieser mit dem Chiffrat des ersten Blocks bitweise addiert. Dieses Verfahren wird nun sukzessive bis zum letzten Block angewandt. Beim Dechiffrieren werden die Blöcke in umgekehrter Reihenfolge entschlüsselt und bitweise voneinander abgezogen. Ein Löschen oder Hinzufügen von Blöcken würde die voneinander abhängige Kette der Blöcke zerstören und das Entschlüsseln weiterer Blöcke unmöglich machen.

12 Symmetrische Verschlüsselung versus ...
Alle bisher betrachteten Verschlüsselungs-Algorithmen fallen in die Klasse der symmetrischen Chiffren. Diese zeichnen sich dadurch aus, dass zum Ver- und Entschlüsseln jeweils der gleiche Schlüssel benutzt wird. Dabei treten jedoch zwei wichtige Probleme auf:

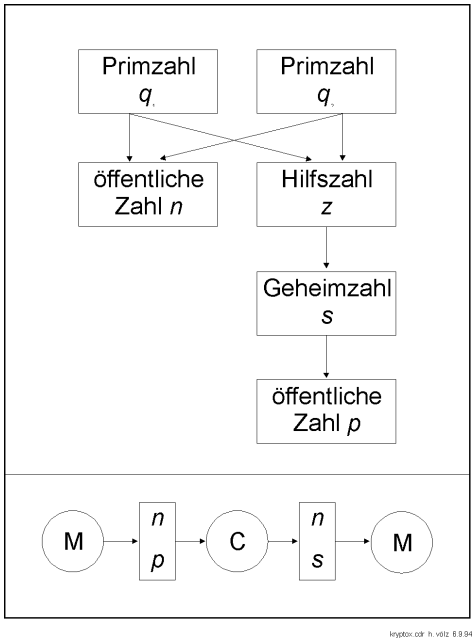
- Vor der Nachrichtenübermittlung müssen Sender und Empfänger einen geheimen Schlüssel vereinbaren. Dazu muss dieser über einen sicheren Kanal übertragen werden, was in der Regel aufwendig ist (z.B. Übermittlung durch Boten)
- Mit jeder neuen Kommunikationsbeziehung muss auch ein neuer Schlüssel generiert werden.

Die vielen Schlüssel müssen verwahrt und ggf. verschiedenen Personen(-Gruppen) bekannt gemacht werden. Dadurch steigen Verwaltungsaufwand und Sicherheitsrisiko.
In einer spektakulären Veröffentlichung wiesen 1976 die amerikanischen Wissenschaftler Diffie und Hellman einen eleganten Weg aus dem Dilemma: Sie entdeckten das Prinzip der öffentlichen Schlüssel.

13 ... Asymmetrische Verschlüsselung
Die beiden Kryptologen schlugen vor, bei jedem Teilnehmer sowohl einen Verschlüsselungsalgorithmus mit öffentlichen Schlüssel als auch einen Entschlüsselungsalgorithmus mit geheimen Schlüssel einzusetzen. Ver- und Entschlüsselungsalgorithmus sind allgemein bekannt. Jeder Teilnehmer wählt einen geheimen Schlüssel und generiert dazu einen öffentlichen Schlüssel. Den öffentlichen Schlüssel macht er bekannt, den geheimen Schlüssel behält er für sich.
Möchte nun ein *Sender* dem *Empfänger* eine geheime Botschaft zukommen lassen, so verschlüsselt er die Nachricht mit dem *öffentlichen Schlüssel des Empfängers*. Nach der Übertragung entschlüsselt der Empfänger diese mit seinem geheimen Schlüssel (siehe Bild 11)
Nur derjenige, der den geheimen Schlüssel kennt, kann den mit dem öffentlichen Schlüssel chiffrierten Text entziffern. Entscheidend ist dabei, dass der zum Verschlüsseln notwendige öffentliche Schlüssel leicht aus dem geheimen berechnet werden kann, nicht aber umgekehrt der geheime aus dem öffentlichen. Der Clou des Verfahrens liegt also darin, dass der Teilnehmer mit dem öffentlichen Schlüssel nur ein Teil seines Geheimnisses preis gibt: Gerade genug zum Verschlüsseln, aber nicht zum Entschlüsseln. Somit ist auch das Problem der Schlüsselverteilung gelöst, da der Schlüssel zum Chiffrieren einmal veröffentlicht wird und von jedermann nachgeschlagen werden kann.

14 Einwegfunktionen

In der DDR gab es einen Witz. Ein Junge fragt seinen Vater, was der Unterschied einer Kritik von unten und von oben sei. Der Vater nimmt einen Topf mit Wasser begibt sich in damit ans Fenster der Wohnung im ersten Stock und gießt das Wasser über den Jungen auf der Straße aus. Er erklärt, dies ist Kritik von oben und nun mache dasselbe von unten. Der Jungen wird bei dem Versuch, das Wasser aus dem Topf nach seinem Vater hochzuschütten nur noch nasser. Ja und das ist Kritik von unten!



Es gibt vielfältige Prozesse, die in analoger Weise nur schwer umkehrbar sind. Sie sind in der Mathematik als Einwegfunktionen bekannt und bilden die Grundlage für die Anwendung moderner Krytographieverfahren mit öffentlichen und geheimen Schlüssel. Als vereinfachtes mathematisches Beispiel sei die Potenzfunktion

$$x = p^s$$

gewählt. Es ist ein leichtes aus p und s den Wert von x zu berechnen. Weitaus schwieriger ist es aber s aus x und p zu bestimmen

$$s = \log(x)/\log(p).$$

Für die Übertragung (von Zahlen) existiere nun ein öffentliches Verzeichnis, in dem jeder Teilnehmer seinen Schlüssel (K = Key) einträgt. Wenn nun der Sender A an den Empfänger B eine Botschaft m (von message) übertragen will, findet er dort die Schlüsselzahl $p = K_pB$ (p für Public = öffentlich). Kennt er außerdem die Geheimzahl s (von Secret), so kann er leicht x berechnen und damit aus der Botschaft m, den Geheimtext c (von Code) erzeugen und an B senden. Ein Angreifer kennt also p als den öffentlichen Schlüssel von B und den Code c. Um ihn zu entschlüsseln muss er zunächst das s und dann x finden. Hierfür ist der Aufwand ersichtlich groß.
In der Praxis durchgesetzt hat sich jedoch ein Verfahren, das nach seinen Entdeckern Rivest, Shamir und Adleman als RSA-Chiffre bekannt wurde. Es basiert auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen. Um das öffentlich-geheime Schlüsselpaar zu erstellen, vollzieht ein Teilnehmer folgende Schritte: (Bild 12)

1. Er wählt zwei große Primzahlen q_1 und q_2 mit $q_1, q_2 > 10^{100}$.
2. Er berechnet die öffentliche Zahl $n = q_1 \cdot q_2$.
3. Er berechnet eine Hilfszahl $z = (q_1 - 1) \cdot (q_2 - 1)$.
4. Er wählt seine Geheimzahl s, die teilerfremd zu z sein muß.
5. Er findet die zugehörige öffentliche Zahl p aus $p \cdot s = 1$ MOD z.

Der öffentliche Schlüssel besteht aus dem Paar (z, n). Hiermit werden die Botschaften M an ihn zum Code gemäß

$$C = M^p (\text{MOD } n)$$

erzeugt. Die Entschlüsselung erfolgt dann nach der Umkehrung

$$M = C^s (\text{MOD } n).$$

Ein Angreifer müsste das geheime s kennen. Um es zu bestimmen, muss er die Primzahlzerlegung der großen Zahl n realisieren. Dies ist mit einem so großem Rechenaufwand verknüpft, dass es Großrechner für lange Zeit beschäftigt. Die Kenntnis der geheimen Primfaktoren und somit die Berechnung des geheimen Schlüssels s öffnet dem Empfänger die Hintertür durch diese Einwegfunktion.
Auch hier soll ein kleines Beispiel der Veranschaulichung dienen:
Es sei $q_1 = 3$ und $q_2 = 11$, $n = 33$ und $z = 20$. Als Wert für s wird 7 gewählt, da $s = 7$ und $z = 20$ keine gemeinsamen Teiler besitzen. Aus diesen Werten kann p berechnet werden: $7p = 1$ (MOD 20) $\rightarrow p = 3$. Unsere Nachricht bestehe aus dem Namen "ANNE". Zur numerischen Codierung dienen die Alphabetpositionen:

Zeichen	Zahl	q_1^3	Chiffretext C= q_1^3(MOD 33)	$C^s=C^7$	C^7(MOD 33)	Zeichen
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

15 Digitale Unterschrift mit öffentlichen Schlüsseln
Fast alle Verträge und wichtigen Dokumente werden heute noch handschriftlich unterschrieben. So alt wie diese Tradition sind die beiden Fälle des Missbrauchs:

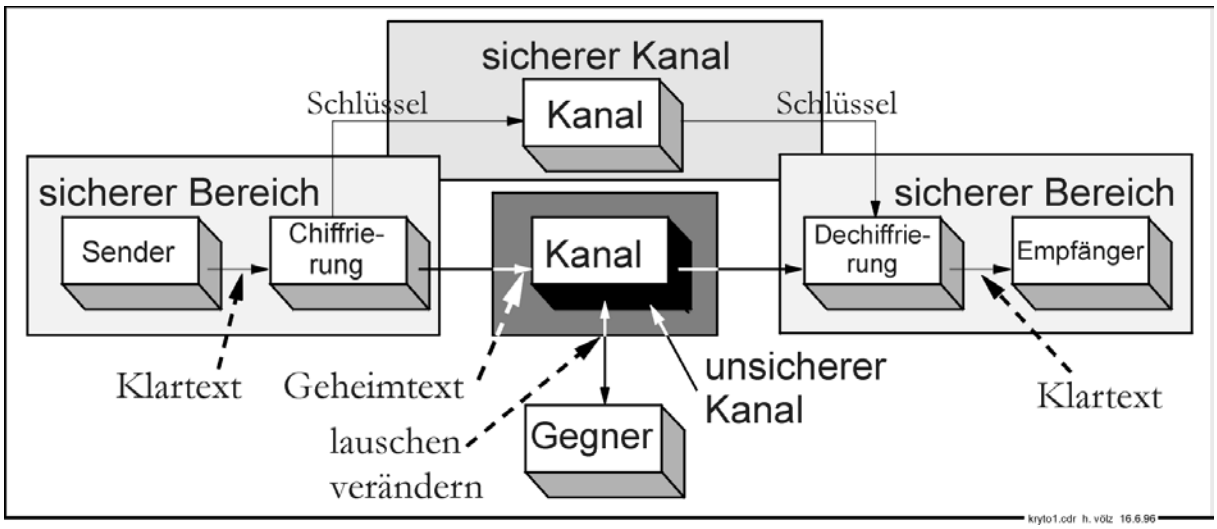
- Die Unterschrift wird von einem Dritten gefälscht. Dabei wird häufig geschickt eine Handschrift nachgeahmt.
- Der Inhalt des unterschriebenen Dokuments wird modifiziert. Dazu zählen Löschen und Hinzufügen von Text, Umdatierung, Abänderungen usw.

Das elektronische Äquivalent zur herkömmlichen Unterschrift, die digitale Signatur, schließt beide Vergehen grundsätzlich aus. Es basiert auf dem Prinzip der öffentlichen Verschlüsselung und wirkt sowohl personen- als auch dokumentbezogen. Obwohl bei der elektronischen Unterschrift die gleichen Verschlüsselungstechniken wie bei den vorgestellten public-key Verfahren zum Einsatz kommen, dient die Chiffrierung hier nicht der Geheimhaltung des Nachrichteninhalts sondern der

Authentifikation des Verfassers. Aus diesem Grund verschlüsselt der Sender ein Dokument mit seinem geheimen Schlüssel. Wegen $C = K_s(P)$ und $P = K_p(C)$ kann nun jeder mit Hilfe des öffentlichen Schlüssels K_p des Senders das Dokument lesen.

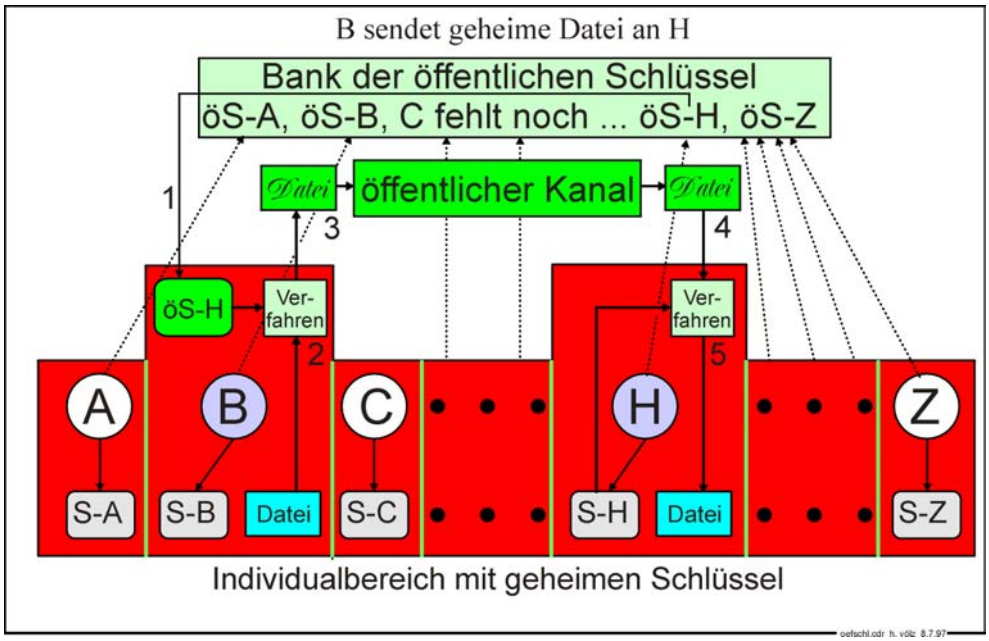
Maßgeblich jedoch ist, dass nur Besitzer eines geheimen Schlüssels einen Text generieren kann, der mit dem zugehörigen öffentlichen Schlüssel entziffert ein sinnvolles Dokument ergibt. Eine Manipulation würde nach dem Dechiffrieren mit hinreichender Sicherheit nur unleserlichen Datenmüll verursachen.

In der Praxis wird allerdings nicht das ganze Dokument unterschrieben, also öffentlich verschlüsselt, da dies bei längeren Texten zu rechenaufwendig wäre (vgl. Bild 13). Stattdessen bildet man über das Dokument eine Art Prüfsumme fester Länge (den digitaler Fingerabdruck), die den Inhalt des Dokuments eindeutig indentifiziert. Es muss dabei gewährleistet sein, dass kein anderer Text die gleiche Prüfsumme vorweist, zumindest muss es unmöglich sein einen solchen zu finden. Übertragen werden das unverschlüsselte Dokument und der verschlüsselte Fingerabdruck als digitale Unterschrift. Der Empfänger bildet nun auch die Prüfsumme über die empfangene Nachricht und entschlüsselt danach den digitalen Fingerabdruck mit dem öffentlichen Schlüssel des Senders. Stimmen beide Zahlen überein, so ist die Botschaft unverfälscht.



16 Ausblick

Von der Geheimwissenschaft zum Jedermann-Werkzeug entwickelt, bieten kryptographische Verfahren in vielen Bereichen unserer Informationsgesellschaft den einzig praktikablen Datenschutz. Insbesondere im schnell expandierenden Kommunikationsmarkt, wo durch die angekündigte "Daten-Autobahn" eine massive Kommerzialisierung der Datennetze bevorsteht, wird der Verschlüsselungs-Technik eine "Schlüssel"-Rolle zukommen. Zwar ist fast keine Chiffre ganz sicher und die z.T. spektakulären Erfolge der Code-Knacker, wie im Fall der Pay-CD, lassen grundsätzliche Bedenken an der Kryptographie laut werden. Jedoch steht im zivilen Einsatz der Verschlüsselungs-Technik der Aufwand des unbefugten Entzifferns meist in keinem Verhältnis zum Nutzen: Wer gibt schon einige Milliarden US$ zum Knacken einer chiffrierten Pizza-Bestellung aus?



Text im “Gold bug” von Edgar Ellen Poe

Um den Schatz des vor 150 Jahren gehängten Seeräubers zu finden muß er eine Zettel mit Geheimschrift entziffern

Führt zu folgenden Häufigkeiten

53##+305))6*;4826)4#.)4#);806*;48+8|60))85;;]8*;:#*8+83(88)5*+;46(;88
96?;8)*#(;485);5*+2:*#(;4956*2(5*-4)8|8*;4069285);6+8)4##;1(#9;48
081;8:8#1;48+85;4)485+528806*81(#9;48;(88;4(#?34;48)4#;161;:188;#?;

Anzahl	33	26	19	15	15	14	12	11	9	8	7
Zeichen	8	;	4	#	)	*	5	6	(	+	1
Anzahl	6	5	5	4	4	3	2	1	1	1	
Zeichen	0	2	9	:	3	?	|	-	.	]	

Die “8” muß also das e sein; Verstärkt da doppel e im englischen häufig. Weiter ist das häufigste Wort “the”, es entspricht also “;48”. Daher gilt

53##+305))6**;48**26)4#.)4#);806**;48**+8|60))85;;]8*;:#*8+83(**88**)5*+;46(;**88**
96?;8)*#(;485);5*+2:*#(;4956*2(5*-4)8|8*;4069285);6+8)4##;1(#9**;48**
081;8:8#1**;48**+85;4)485+52**88**06*81(#9**;48**;(**88**;4(#?34**;48**)4#;161;:1**88**;#?;

Weitere Lösungen sind dann

5	+	8	3	4	6	*	#	(	;
a	d	e	g	h	i	n	o	r	t

“A good glass in the bishop’s hostel in the devil’s seat - twenty-one degrees and thirteen minutes - northeast and north - main branch seventh limb east side - shoot from the left eye of the death’s head - a bee line from the tree through the shot fitly feet out”

```
         012345678901234567890123 45

A        abcdefghijklmnopqrstuvwxyz  0
B        bcdefghijklmnopqrstuvwxyza  1
C        cdefghijklmnopqrstuvwxyzab  2
D        defghijklmnopqrstuvwxyzabc  3
E        efghijklmnopqrstuvwxyzabcd  4
F        fghijklmnopqrstuvwxyzabcde  5
G        ghijklmnopqrstuvwxyzabcdef  6
H        hijklmnopqrstuvwxyzabcdefg  7
I        ijklmnopqrstuvwxyzabcdefgh  8
J        jklmnopqrstuvwxyzabcdefghi  9
K        klmnopqrstuvwxyzabcdefghij 10
L        lmnopqrstuvwxyzabcdefghijk 11
M        mnopqrstuvwxyzabcdefghijkl 12
N        nopqrstuvwxyzabcdefghijklm 13
O        opqrstuvwxyzabcdefghijklmn 14
P        pqrstuvwxyzabcdefghijklmno 15
Q        qrstuvwxyzabcdefghijklmnop 16
R        rstuvwxyzabcdefghijklmnopq 17
S        stuvwxyzabcdefghijklmnopqr 18
T        tuvwxyzabcdefghijklmnopqrs 19
U        uvwxyzabcdefghijklmnopqrst 20
V        vwxyzabcdefghijklmnopqrstu 21
W        wxyzabcdefghijklmnopqrstuv 22
X        xyzabcdefghijklmnopqrstuvw 23
Y        yzabcdefghijklmnopqrstuvwx 24
Z        zabcdefghijklmnopqrstuvwxy 25
```