Fachhochschule Köln
University of Applied Science Cologne
Abteilung Gummersbach

Die Geschichte der IT-Sicherheit

Verschlüsselung von Daten über 2500 Jahre hinweg

IT-Sicherheit

Marco Nassenstein

marco@nassenstein.com

11030048

WS 2006 / 2007

INHALTSVERZEICHNIS

Vorwort....3
Monoalphabetische Substitutionschiffren....3
Atbash....3
Polybios-Chiffre....4
Verschiebechiffre....5
Sicherheit monoalphabetischer Chiffren....5
Polyalphabetische Substitutionschiffren....6
Tabula Recta....6
Vigenère-Verschlüsselung....7
Vernam-Verschlüsselung....8
Sicherheit Polyalphabetischer Chiffren....8
Antistatistische Substitutionschiffren....9
Alphabetum Kaldeorum....10
Homophone Verschlüsselung....11
Polygrammsubstitution....11
Playfair-Chiffre....12
Sicherheitseinschätzung....13
Andere klassische Verschlüsselungsmethoden....14
Skytale....14
Zinken....14
Cardan-Gitter....15
Ottendorf-Verschlüsselung....15
TELWA....16
Maschinen....16
Chiffrierscheibe....17
Jefferson-Walze....17
Kryha....18
Enigma....19
Bomba....22
PURPLE....23
NEMA....24
M-209....24
Unknackbare Verschlüsselungen?....25
Fremde Sprachen als Verschlüsselung....25
Schlusswort....26

Vorwort

Seit es Menschen gibt, gibt es Geheimnisse. Während es verschiedene Gründe für Geheimnisse geben kann, ist allen Geheimnissen gemeinsam gegeben, daß sie Informationen enthalten, die nur gewissen Leuten zugänglich sein sollen. Müssen diese Informationen Raum, Zeit und neugierige Augen als Geheimnis überstehen, dann ist ihre Verschlüsselung eine Notwendigkeit.

Die Abbildung eines großen, zu schützenden Geheimnisses auf ein kleineres, das in Form einer bestimmten deterministischen Regel vorliegt, ist der Zweck einer Verschlüsselung. Die Sicherheit von Information soll durch Verfahren oder Schlüssel gewährleistet werden, die nur dem rechtmäßigen Empfänger bekannt sind.

Diese Ausarbeitung soll die Geschichte der Datenverschlüsselung innerhalb der letzten 2600 Jahre aufzeigen: die verschiedenen Ansätze, die simplen, aber nicht weniger genialen Methoden in der Frühzeit, bis hin zu den mechanischen Wunderwerken aus dem zweiten Weltkrieg.

Die unterschiedlichen Verfahren werden nur sekundär chronologisch geordnet, stattdessen primär nach der Methodik, die sie funktionieren lassen.

Monoalphabetische Substitutionschiffren

Die denkbar einfachste Art der Verschlüsselung eines Textes besteht darin, die einzelnen Zeichen nach einem bestimmten Regelwerk gegen andere Zeichen auszutauschen. Da jedem Buchstaben genau ein anderer Buchstabe zugeordnet wird, hat das Chiffrat stets dieselbe Länge wie der Klartext. Wendet man das Regelwerk rückwärts auf das Chiffrat an, erhält man den Klartext, womit das Verfahren der symmetrischen Kryptographie zugeordnet werden muß.

Atbash

Bereits 600 v. Chr wendete man im Palästina das monoalphabetische Substitutionschiffre *Atbash*

an. *Atbash* heißt auf unser Alphabet übertragen in etwa "AZ-BY", was direkt als Hinweis auf die Funktionsweise zu verstehen ist. Zur Verschlüsselung eines Klartextes bestimmt man die Position eines Zeichens im Alphabet und ersetzt es durch das Zeichen, das denselben Abstand im Alphabet hat, allerdings von hinten gezählt. Somit wird ein A durch ein Z ersetzt und ein B durch ein Y.

"IT Sicherheit" würde mit Atbash verschlüsselt also folgendermaßen aussehen:

RG Hrxsvisvrg

In der Bibel wird im Buch Jeremia Kapitel 25 Vers 26 und Kapitel 51 Vers 41 so aus dem Namen Babel (=BBL) der Name Scheschach (=SSK)[1].

Polybios-Chiffre

Das *Polybios-Chiffre*[2] ordnet das Alphabet in einer Matrix an und ersetzt jedes Zeichen durch seine zwei numerischen Koordinaten. Strenggenommen handelt es sich hierbei nicht um eine monoalphabetische Substitution, da ja jedem Buchstabe genau zwei Ziffern zugeordnet werden. Da diese aber ebenso fix sind, wie ein substituierter Buchstabe, sollte das Verfahren trotzdem als solches verstanden werden.

Polybios war ein griechischer Historiker, der dieses Verfahren bereits 100 v. Chr angewandt haben soll, um Nachrichten optisch über große Strecken zu übermitteln. Dabei sollten die Positionen von Fackeln die Koordinaten des zu übermittelnden Buchstabens darstellen. "IT Sicherheit" im Polybios-Chiffre würde sich folgendermaßen darstellen:

2444 43241323154223152444

Die zugehörige Matrix sieht so aus:

	1	2	3	4	5
1	**A**	**B**	**C**	**D**	**E**
2	**F**	**G**	**H**	**I**	**K**
3	**L**	**M**	**N**	**O**	**P**

[1] http://www.linuxfibel.de/krypto.htm

[2] http://de.wikipedia.org/wiki/Polybios-Chiffre

4	**Q**	**R**	**S**	**T**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

Das Polybios-Chiffre fand auch noch, kombiniert mit einer Transposition, im ersten Weltkrieg unter dem Namen *ADFGX*[3] Verwendung.

VERSCHIEBECHIFFRE

Das *Verschiebechiffre* verschiebt ein Zeichen um eine bestimmte Anzahl Stellen im Alphabet. Die Anzahl der Transformationen kann als Schlüssel betrachtet werden. Erfunden und benutzt haben soll dieses Verfahren Julius Caesar[4] zur Überbringung geheimer Informationen an seine Streitmächte. Er präferierte dabei den Schlüssel C (also eine Verschiebung um 3 Stellen. Ein A wurde damit zu einem C und ein B zu einem D und ein Z zu einem B).

Auch heute findet dieses Verfahren in Diskussionsforen im Internet noch Anwendung, wenn bestimmte Textpassagen nicht sofort lesbar sein sollen; in etwa Lösungswörter eines Rätsels oder Plots aus diskutierten Werken wie Filme oder Bücher. Die Anzahl der Verschiebungen ist hier 13, was dem Verfahren den Namen *ROT13* (sprich: Rotation um 13 Zeichen) einbrachte und den Nebeneffekt hat, daß eine weitere Anwendung des Verfahrens erneut den Klartext ausgibt. Dies hängt damit zusammen, daß unser Alphabet 26 Buchstaben hat. So wird bei der ersten Anwendung aus einem A ein N und bei der zweiten daraus wieder ein A. "IT-Sicherheit" mit ROT13 kodiert ergibt:

VG Fvpureurvg

SICHERHEIT MONOALPHABETISCHER CHIFFREN

Die monoalphabetischen Substitutionsschriften sind keineswegs als sicher anzusehen. Sie sind vor allem anfällig für Mustererkennungen: gelingt es einem potentiellen Angreifer ein Wort des

[3] http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/dkoch/ADFGVX.html

[4] http://www.kuno-kohn.de/crypto/crypto/caesar.htm

Chiffrats zu erraten, dann kann er anhand der dort zur Anwendung gekommenen Subsitutionsvorschrift alle anderen Buchstaben im Chiffrat, die im Zielwort genauso vorkommen, ersetzen. Zu findende Wörter wären zum Beispiel typische Floskeln wie "Mit freundlichen Grüßen" oder "Betreff", vor allem aber Wörter mit Doppelbuchstaben oder in der jeweiligen Sprache typische Silben wie "heit", "keit" oder "ung" im Deutschen.

Im 19. Jahrhundert ging der Autor Edgar Allan Poe sogar soweit, daß er seine Leser dazu aufforderte, ihm monoalphabetische Geheimschriften zu schicken. Tatsächlich gelang es ihm auch, sie allesamt zu entschlüsseln. Gemäß seinen theoretischen Arbeiten zur Kryptoanalyse[5] lässt sich erahnen, daß er dafür tatsächlich einen lexikalischen und einen semantischen Ansatz benutzte.

Polyalphabetische Substitutionschiffren

Eine höhere Form der Verschlüsselung stellen die polyalphabetischen Substitutionschiffren dar, die, wie der Name bereits andeutet, mehrere Geheimalphabete kombinieren, um die Sicherheit des Chiffrats zu erhöhen.

Bezogen auf das weiter oben vorgestellte Verschiebechiffre würde das bedeuten, daß jeder Buchstabe nicht um denselben, festen Wert im Alphabet verschoben wird, sondern durch eine Anzahl, die durch irgendeine alternierende Vorschrift erzeugt wird. Zum Beispiel könnte der erste Buchstabe um eine Stelle verschoben werden, der zweite um zwei, der dritte um drei, und so weiter.

Tabula Recta

Die *Tabula Recta*, die vom Benediktinerabt Johannes Trithemius (1462-1516), der die ersten gedruckten Bücher über Kryptographie verfasste, erdacht wurde, vewendet, ähnlich wie das Polybios-Chiffre, eine Matrix. Allerdings enthält hier jede der 24 Zeilen alle Buchstaben des Alphabets (im Falle der Tabula Recta ebenfalls 24, da es im Lateinischen kein J und kein U gibt). Der Unterschied zwischen den Zeilen besteht lediglich darin, daß das Alphabet jeweils später

[5] Edgar Allan Poe, Der Goldkäfer, ISBN 048626875

beginnt (und die ausgelassenen Buchstaben später hinten angehängt werden, um die Zeile zu komplettieren). Er selber schreibt[6] dazu:

In dieser regelmäßigen oder viereckigen Tabelle von Buchstaben findet man durch Veränderung („per mutationem“) oder Umsetzung („transpositionem“) das gebräuchliche Alphabet unserer lateinischen Buchstaben, die in ihrer Gesamtheit Monogramme (einzelne Buchstaben) darstellen, nämlich 24 mal 24, das ergibt die Zahl von 576 und multipliziert man diese mit genauso vielen (24), ergibt sich ein wenig weniger als 14.000.

Die Idee lag nun darin, den ersten Buchstaben des Klartextes mit der ersten Zeile zu verschlüsseln und den zweiten mit der zweiten (vgl. oben angedeutetes Verfahren des Polyalphabets beim Verschiebechiffre). Diese Vorgehensweise selber bezeichnet man als progressive, also voranschreitende, Chiffrierung und kommt in späteren Kapiteln der Geschichte und dieser Ausarbeitung noch mehrfach vor.

VIGENÈRE-VERSCHLÜSSELUNG

Mit der *Vignére Verschlüsselung*, benannt nach dem Diplomaten Blaise de Vigenère (16. Jahrhundert), tauchte das Prinzip eines Passworts zum ersten Mal auf. Dieses geheime Wort wurde so interpretiert, daß die Position seiner Zeichen jeweils die Verschiebung des Alphabets für das entsprechende Zeichen des Klartext ergab[7].

Nehmen wir als zu verschlüsselnden Klartext erneut "IT Sicherheit" an. Passwort soll sein "passwort". In diesem Falle würde das Alphabet um 16 Stellen verschoben werden (da "P" der 16. Buchstabe im Alphabet ist). Das I (Buchstabe Nr. 9 im Alphabet) von "IT Sicherheit" müßte demnach um 16 Stellen auf Position 25 (also ein Y) verschoben werden. Analog würde es mit dem zweiten Buchstaben "T" des Klartextes geschehen, der gemäß des zweiten Buchstabens des Passworts "A" um eine Stelle verschoben werden müßte (U).

Ist das Passwort abgearbeitet, aber der Klartext noch nicht, so hängt man es einfach erneut an, so

[6] http://de.wikipedia.org/wiki/Tabula_recta

[7] http://www.csci.csusb.edu/public/crypto/game/VigenereCipher_Overview.php

daß im Sinne des polyalphabetischen Verfahrens das erste Alphabet das normale ist und das zweite eine Reihenfolge von Buchstaben, die dieselbe Länge hat, wie der Klartext und in unserem Beispiel so aussehen würde: passwortpasswortpasswortpasswortpasswortpas....

VERNAM-VERSCHLÜSSELUNG

Die *Vernam Verschlüsselung*, benannt nach ihrem Erdenker, dem amerikanischen Kryptologen Gilbert Vernam (1890-1960), benutzt dasselbe Prinzip wie die Vignére-Verschlüsselung. Allerdings ist das Passwort genauso lang wie der Klartext[8] und wird nach einmaliger Verwendung nicht mehr benutzt. Unter der Voraussetzung, daß es gewissenhaft angewendet wird und das Einmalpasswort (One Time Pad) tatsächlich aus zufälligen Zeichen besteht, gilt dieses Verfahren als informationstheoretisch sicher und kann nachweislich nicht gebrochen werden.

Zwar erfüllt dieses Verfahren den Anspruch darauf, daß sich die Sicherheit eines Verfahrens nicht auf die Geheimhaltung des Systems (Obscurity) aufbauen darf, sondern einzig durch die Geheimhaltung des Schlüssels, allerdings muß bedacht werden, daß es wohl keinen praktischen Unterschied macht, ob man einen Text mit 100 Zeichen vor fremdem Zugriff schützen muß, oder einen Schlüssel, der ebenfalls 100 Zeichen Länge hat.

SICHERHEIT POLYALPHABETISCHER CHIFFREN

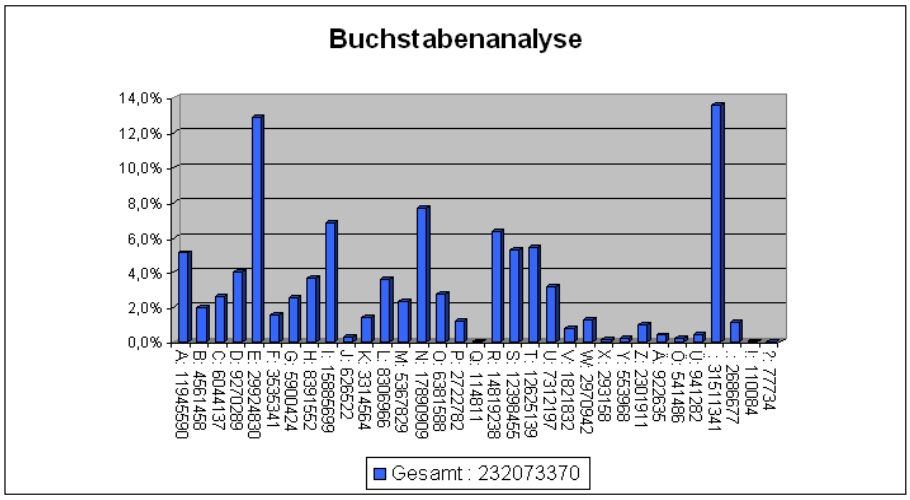
Wie auch die monoalphabetischen Verfahren, bietet der polyalphabetische Ansatz - sehen wir von der Vernam Verschlüsselung mir ihren ganz eigenen Nachteilen ab - keinen ausreichenden Schutz und kann gebrochen werden. Wenn zum Beispiel die Schlüssellänge bekannt ist, so kann man alle Zeichen des Chiffrats, die diesen Abstand haben, mit dem selben Verschiebechiffre substituieren.

Der *Kasiski-Test*, benannt nach dem preußischen Infanteriemajor Friedrich Wilhelm Kasiski (1805 - 1881), soll diese Schlüssellänge ermitteln und macht sich dabei zunutze, daß es durchaus vorkommt, daß Wiederholungen im Klartext (vor allem Silben) mit Wiederholungen des Schlüssels

[8] http://www.kuno-kohn.de/crypto/crypto/otp.htm

aufeinanderfallen. Diese Abstände zwischen den Vorkommnissen müssen demnach wahrscheinlich vielfache der Schlüssellänge oder die Schlüssellänge selber sein. Danach bedarf es nur noch einer Häufigkeitsanalyse.

Wie auch schon beim monoalphabetischen Ansatz, ist eine Häufigkeitsanalyse der Buchstaben, die in der zu entschlüsselnden Sprache vorkommen, ein wunder Punkt des Verfahrens. Jeder Kreuzworträtselfan weiß, daß in der deutschen Sprache vor allem E's und N's häufiger vorkommen, als andere Buchstaben. Siehe dazu die folgende Graphik[9], die das Vorkommen der verschiedenen Zeichen in der deutschen Sprache statistisch aufzeigt:



Vor allem längere Texte nähern sich recht gut dieser Statistik an. Bei kürzeren Texten jedoch besteht die Gefahr, daß sie aus verschiedenen, vorhersagbaren Phrasen oder Textfragmenten bestehen müssen, die den Mindestinformationsgehalt darstellen, den es zu kommunizieren gilt. Somit ist das eine wie das andere der Gefahr der unauthorisierten Entschlüsselung ausgesetzt und die polyalphabetischen Substitutionschiffren können nicht als sicher betrachtet werden (Ausnahme: Vernam).

Antistatistische Substitutionschiffren

Um der Gefahr der statistischen Analyse entgegenzutreten, entwickelte man schon früh (nachgewiesen um das 14. Jahrhundert) Verfahren, die das Häufigkeitsgebirge einebnen sollten:

[9] http://de.wikipedia.org/wiki/Häufigkeitsanalyse

besonders häufig vorkommende Buchstaben sollten durch mehrere unterschiedliche Zeichen ersetzt werden.

Alphabetum Kaldeorum

Die folgende Graphik[10] zeigt das Alphabet dieser Verschlüsselung, wobei sie strenggenommen nicht als Verschlüsselung verstanden werden sollte, da sie nach keiner kryptologischen Systematik funktioniert, sondern lediglich Zeichen des Klartextes durch dem Leser unbekannte Symbole ersetzt. Trotzdessen findet sie innerhalb dieser Arbeit Erwähnung, denn sie weist den Buchstaben g, h, l, o, p und q jeweils zwei unterschiedliche Symbole zu, um die weiter oben erwähnten Ansätze der Häufigkeitsanalysen zu entkräften.

Daß es sich ausgerechnet um diese Buchstaben handelt hängt damit zusammen, daß das Alphabetum Kaledorum, wie der Name bereits impliziert, für die lateinische Sprache entwickelt wurde, die ihrerseits wieder andere statistische Wahrscheinlichkeiten für bestimmte Zeichen besitzt, als die deutsche Sprache. Zusätzlich wurden in das Chiffrat sinnlose Zeichen eingefügt, um eine Entschlüsselung weiter zu erschweren.

Als Urheber gilt Herzog Rudolf IV. von Österreich (1339 - 1365), der dem Alphabetum Kaledarum allerdings einen indischen Ursprung zuschrieb. Das konnte aber nie nachgewiesen werden.

[10] http://de.wikipedia.org/wiki/Alphabetum_Kaldeorum

Homophone Verschlüsselung

Die *homophone Verschlüsselung* (homophon ist griechisch für Gleichklang) geht das Problem mit der statistischen Analysierbarkeit eines Chiffrats logisch an und teilt den Buchstaben des Klartexts eben soviele verschiedene Geheimzeichen zu, wie die jeweilige Häufigkeit des Buchstabens nahelegt.

Der Buchstabe E, der nach der Graphik weiter oben eine Wahrscheinlichkeit von 13% in einem normalen prosaischen Text mit Satzzeichen besitzt, bekommt demnach auch aus der Gesamtmenge an Geheimzeichen 13% zugeschrieben. Wenn also das Geheimalphabet 100 Zeichen vorrätig hat (zum Beispiel mit den Zahlen 00 bis 99), dann stehen allein 13 verschiedene nur für das E.

Dadurch ergibt sich zwangsläufig innerhalb des Geheimtextes eine Zeichenwahrscheinlichkeit von 1%, wodurch eine Häufigkeitsanalyse unmöglich wird[11]. Die einzige Möglichkeit besteht für einen Angreifer nun noch darin, sich auf Silben zu konzentrieren. Dies geht selbstverständlich nur in einem ausreichend langen Text, der weit mehr als 100 Buchstaben besitzt, denn nur so lässt sich eine Regel erkennen. Andersherum gilt, daß Texte mit unter 100 Zeichen als recht gut geschützt abgesehen werden können.

Polygrammsubstitution

Eine Polygrammsubstitution greift nun diese vermeintlich letzte Schwachstelle der antistatistischen Verfahren an und ersetzt immer mehrere Zeichen auf einmal; in der Regel jedoch Zeichenpaare, wodurch man von einem Digraph-Chiffre spricht. Zum einen ergibt sich dadurch wieder eine wesentliche homogenere Verteilung der Geheimtextzeichen, zum anderen wird die Suche nach typischen Buchstabenpaaren wie "er", "ne", "qu" oder "st" dadurch erschwert, denn diese werden ja stets gemeinsam chiffriert. (Allerdings sei direkt an dieser Stelle angemerkt, daß auch diese Silben natürlich eine bestimmte Wahrscheinlichkeit innerhalb eines hinreichend langen Textes besitzen. Von daher sind auch Polygrammsubstitutionen nicht gegen Häufigkeitsanalysen gefeit.)

[11] http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/mzoellner/siebzehn.htm

PLAYFAIR-CHIFFRE

Das Playfair-Chiffre wurde 1854 vom britischen Physiker Charles Wheatstone erfunden und bis zum ersten Weltkrieg eingesetzt. Seine Sicherheit erlangt es vor allem durch die relative Komplexität seines Verfahrens[12]:

Der Klartext wird zunächst von Leer- und Satztzeichen befreit und alle Buchstaben zu Großbuchstaben umgewandelt, außerdem wird J zu I. Zwei aufeinanderfolgende gleiche Buchstaben werden durch einen einzelnen und ein X ersetzt. "Otto" wird damit zu "OT XO". Sollte es sich im Klartext um eine ungerade Anzahl von Zeichen handeln, so wird auch der letzte, einzeln stehende Buchstabe durch ein X ergänzt.

Als Passwort dient ein beliebiger Schlüsselsatz. Seine Buchstaben werden in einer 5x5 Matrix angeordnet, mit jeweils 5 Zeichen pro Zeile (5 Zeilen). Wenn ein Buchstabe bereits vorkam, wird er nicht ein zweites Mal aufgeführt. Die noch freien Felder werden einfach in alphabetischer Reihenfolge der noch nicht vorgekommenen Buchstaben aufgefüllt, wobei das zugrundegelegte Alphabet kein J enthält (um eine 5x5 Matrix zu erreichen). Beim Schlüsselsatz "IT Sicherheit macht tierisch Spass" lautet die zugehörige Matrix also:

	1	2	3	4	5
1	**I**	**T**	**S**	**C**	**H**
2	**E**	**R**	**M**	**A**	**P**
3	**B**	**D**	**F**	**G**	**K**
4	**L**	**N**	**O**	**Q**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

Die Zeichen des Klartexts, der bereits weiter oben vorbereitet wurde, werden nun immer paarweise, in sogenannten Digrammen, verschlüsselt.

Dabei betrachtet man, ob diese beiden Zeichen in der Schlüsselwortmatrix in derselben Zeile liegen. Wenn dem so ist, dann substituiert man sie durch das Zeichen, das jeweils rechts vom Klartextzeichen zu finden ist. Befindet sich rechts kein Zeichen, beginnt man wieder zu Anfang

[12] http://www.egge.net/~savory/playfair.htm

derselben Zeile. "IS" wird im Falle der obigen Matrix also zu "TC" werden.

Liegen die beiden Zeichen jedoch nicht in derselben Zeile, sondern stattdessen in derselben Spalte, dann wählt man, ganz analog, den jeweils darunter zu findenden Buchstaben. "EV" würde im Falle der obigen Matrix damit zu "BI" werden.

Liegen die beiden Buchstaben weder in einer gemeinsamen Spalte, noch in einer gemeinsamen Zeile, dann wählt man die Buchstaben, die die Verbindungspunkte zwischen den Zeilen und Spalten der Klartextzeichen bilden. "TF" würde somit werden zu "SD".

Die Entschlüsselung würde entsprechend ablaufen. Alles, was dazu nötig ist, ist das Schlüsselwort und die Interpretationsgabe, Wörter mit J als solche zu erkennen. "IA HR" bedeutet nämlich "Jahr".

Wie bereits weiter oben angedeutet, lässt sich auch beim Playfair Chiffre anhand der Häufigkeit bestimmter Silben Rückschlüsse auf den Klartext ziehen und dies trägt zu seiner Entschlüsselung bei. Liegen außerdem die Zeichen nicht in derselben Spalte und Zeile, dann würde - im Beispiel "SD" bedeutet "TF" - auch automatisch gelten "DS" bedeutet "FT" und jeweils umgekehrt.

SICHERHEITSEINSCHÄTZUNG

Alle vorgestellten kryptographischen Ansätze haben ihre Schwächen. Vielleicht erscheint das auch nicht unbedingt als Verwunderung, denn der jüngste ist über 100 Jahre alt, der älteste weit über 2000. Man muß bei der Einschätzung ihrer Sicherheit bedenken, daß bestimmte statistische Verfahren zum Brechen der jeweiligen Verschlüsselung nicht ohne weiteres ohne technologische Hilfe, wie zum Beispiel Computer, nachvollziehbar sind. Und obwohl heutzutage gilt, daß Sicherheit niemals durch Unklarheit des zugrundeliegenden Systems erlangt werden soll, werden die Verfahren zum Zeitpunkt ihrer Entwicklung doch einen ausreichenden Schutz geboten haben. Selbst heute gilt eine Verschlüsselung dann als sicher, wenn sie bislang von niemandem geknackt wurde. Dies war sicher auch lange Zeit für das simple Verschiebechiffre der Fall.

Im Rahmen der vorgestellten Verfahren setzt jedoch nur die *homophone Verschlüsselung* auf eine

mathematisch/logische Grundlage ihrer Entwicklung und beeindruckt durch eine, selbst nach heutigen Maßstäben, stattliche Sicherheit bei entsprechend kurzen Texten.

Bevor nun in späteren Artikeln auf die mechanischen Wunderwerke des 20. Jahrhunderts eingegangen wird, möchten wir nochmal den Blick auf andersartige Arten der Verschlüsselung wenden.

Andere klassische Verschlüsselungsmethoden

Die nachfolgend vorgestellten Verschlüsselungsmethoden arbeiten nicht nach einer algorithmisch anmutenden Vorschrift, sondern entstammen eher den geistreichen Ideen von Menschen, die an einer umkomplizierten Art und Weise interessiert waren, um ihre Geheimnisse zu schützen.

Skytale

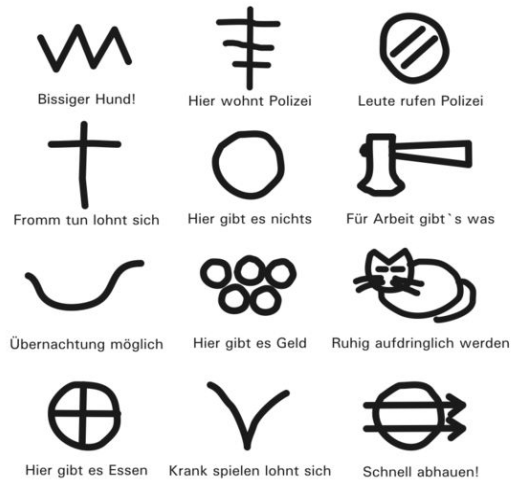
Bereits vor 2500 Jahren haben die Spartaner[13] ihre militärischen Botschaften nicht in Klartext übermittelt, sondern einen langen Streifen Pergament spiralförmig um einen Stock eines ganz bestimmten Durchmessers gewickelt. Danach wurde die Botschaft längs des Stocks entlang aufgeschrieben und das Pergament danach wieder abgewickelt. Die Übermittlung erfolgte nun ohne den Stock. Auf dem Pergament waren lediglich unzusammenhängende Buchstaben zu sehen. Erst der rechtmäßige Empfänger mit einem Stock desselben Durchmessers konnte die Botschaft entziffern. Der Stock(durchmesser) kann in diesem Falle also als Passwort verstanden werden.

Zinken

Exemplarisch für jede Art der Geheimsprache oder -schrift in einer bestimmten sozialen Gruppe seien hier die Zinken erwähnt, die auch unter dem Namen Gaunerzinken besser bekannt sein dürften. Von einer Verschlüsselung im klassischen Sinne kann hier keine Rede sein, dennoch zeigt es, daß Unklarheit im Falle der Kommunikation Geheimnisse unter Umständen angemessen

[13] http://www.it.fht-esslingen.de/~schmidt/vorlesungen/kryptologie/seminar/ws9798/html/krypt_gesch/krypt_gesch-2.html

schützen kann. Das folgende Bild zeigt einige dieser Zinken:



CARDAN-GITTER

Der italienischen Mathematiker Jérôme Cardan erdachte um 1550 das nach ihm benannte *Cardan Gitter*[14]. Auf ein Blatt Papier wird ein Gitter gemalt und bestimmte, zufällig erwählte Felder werden ausgeschnitten. Durch diese Löcher hindurch schreibt man nun die Zeichen des Klartexts auf ein darunterliegendes Papier. Danach entfernt man das Cardan-Gitter und füllt den Rest des zweiten Papiers mit sinnlosen Buchstaben aus. Nur mit dem Cardan-Gitter kann diese Botschaft erneut gelesen werden.

Eine Variation ist ein Cardan-Gitter, das auf eine Seite eines beliebigen Buches gelegt wird und an der Stelle Löcher geschnitten bekommt, unter der sich die benötigten Buchstaben befinden. Nun braucht ein Entschlüssler nicht nur das Gitter, sondern auch das entsprechende Buch und die Seite.

OTTENDORF-VERSCHLÜSSELUNG

Die Ottendorf-Verschlüsselung basiert ebenfalls auf Büchern: man überträgt dem Empfänger lediglich Seiten- und Zeilenzahl, sowie gegebenenfalls noch die Position des Wortes, das dieselbe Bedeutung trägt, wie die Aussage, die man dem Empfänger zukommen lassen möchte.

Das Chiffrat besteht dann Beispielsweise aus der Zeichenfolge 56/21/9, was bedeutet, daß man (in

[14] http://de.wikipedia.org/wiki/Cardan-Gitter

einem vorher festgelegten Buch) Seite 56 aufschlagen und in Zeile 21 das neunte Wort benutzen muß, um die Nachricht zu rekonstruieren.

TELWA

Exemplarisch für eine Substitutionsschrift aus dem zweiten Weltkrieg, die aufgrund mathematischer Methodik (s.o.) geknackt wurde, soll hier das sogenannte TELWA Verfahren[15] genannt werden, das von den Alliierten eingesetzt wurde und von den Deutschen entschlüsselt werden konnte. Der Name ergibt sich, weil alle Botschaften mit Buchstaben in Fünfergruppen chiffriert waren und mit der Zeichenfolge TELWA begannen.

Die Zeichenfolge "RYKFI" stand dabei zum Beispiel für eine sich öffnende Klammer oder UZUSP für das englische Wort "signed". Es gab also eine eindeutige Entsprechung zwischen Bedeutung und Fünfergruppe.

Die deutschen Kryptologen entdeckten innerhalb der abgefangenen Funksprüche, daß die Buchstaben in den Fünfergruppen jeweils voneinander abhängig waren, wahrscheinlich, so wurde gemutmaßt, um Übertragungsfehler identifizieren zu können. Daraufhin gelang es sogar, eine mathematische Formel anzufertigen, anhand welcher sich auch Fehler bei der Abhörung feststellen liessen. Durch statistische Analysen konnten 75% des TELWA Codes von den Deutschen dechiffriert werden.

MASCHINEN

Das 20. Jahrhundert war die Hochzeit der mechanischen Verschlüsselungsmaschinen, allen voran die berühmte Enigma der deutschen Wehrmacht. In diesem Kapitel wird sie, sowie einige ähnliche Maschinen aus anderen Ländern, vorgestellt. Außerdem werden zu Anfang zwei Mechaniken genannt, die bereits 500, bzw. 200 Jahre vor der Enigma gute Dienste zur Verschlüsselung leisteten.

[15] http://www.heise.de/tp/r4/artikel/18/18371/1.html

CHIFFRIERSCHEIBE

Die Chiffrierscheibe, bereits im 15. Jahrhundert durch den italienischen Architekten Leone Alberti entwickelt[16], automatisiert das weiter oben ausgeführte Verschiebechiffre, indem man zwei Scheiben, eine etwas größer als die andere, aneinandersetzt. An einer mittig gelegenen Achse können sich nun beide unabhängig voneinander drehen. Eine bestimmte Stellung steht dann für die Verschiebung um eine bestimmte Anzahl von Buchstaben, wenn am Rande der inneren Scheibe beispielsweise das Geheimalphabet und an der äußeren das Klartextalphabet angebracht ist.

Natürlich konnte man die Stellung der Scheiben zueinander nach einer vorher festgelegten Gesetzmäßigkeit während der Chiffrierung verändern, wodurch ein echtes polyalphabetische Substitutionschiffre entstand.

An dieser Stelle sei angemerkt, daß eine Chiffrierscheibe dem Computerspiel "Monkey Island" in den frühen 90er Jahren beigelegt war und als Kopierschutz diente.

JEFFERSON-WALZE

Die Jefferson-Walze wurde vom berühmten amerikanischen Erfinder und Mitverfasser der Unabhängigkeitserklärung Thomas Jefferson entwickelt. Sie funktionierte dem Prinzip der Chiffrierscheibe sehr ähnlich, bot jedoch bereits mehr Komfort, indem sie gleich 26 Scheiben enthielt, an deren Rändern jeweils die 26 Buchstaben des Alphabetes aufgetragen waren. Dies mußte nicht in der Reihenfolge des Alphabetes sein, aber zumindest mußten Empfänger und Sender dieselben Buchstabenreihenfolgen benutzen, wodurch sich gegenüber anderen Besitzern von Jeffernson Walzen eine zusätzliche Sicherheit ergab. Man stellte die Scheiben nun so zueinander, daß an ihnen entlang innerhalb einer Zeile der Klartext zu lesen war. Dieser durfte maximal 26 Buchstaben lang sein, aufgrund der 26 Scheiben.

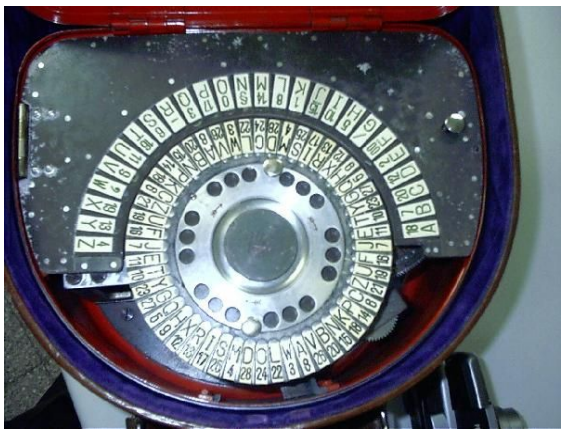
[16] http://www.mathe.tu-freiberg.de/~dempe/schuelerpr_neu/chiffsch.htm

Der Sender übertrug nun eine beliebige andere Zeile (z.B. die direkt darunter) an den Empfänger, der diese erneut auf seine Maschine anwendete und nun in den anderen 25 Zeilen nach der suchte, die Sinn ergab.

Ein Mitarbeiter der französischen Regierung erfand die Jefferson Walze um 1890 herum neu und dann, kurz vor dem ersten Weltkrieg, ebenso ein Offizier der U.S. Armee. Zwischen 1922 und dem Anfang des zweiten Weltkrieges wurde sie dort unter dem Namen M-94 benutzt[17].

KRYHA

Der Kryha Kryptograph wurde durch Alexander von Kryha im Jahre 1924 entwickelt[18]. Im Prinzip handelte es sich hierbei um einen Mechanismus, der die variiernden Stellungen einer Chiffrierscheibe automatisieren konnte.



Im Jahre 1933 gelang es einigen Kryptologen, eine mit der Kryha verschlüsselten Botschaft mit

[17] http://www.monticello.org/reports/interests/wheel_cipher.html/

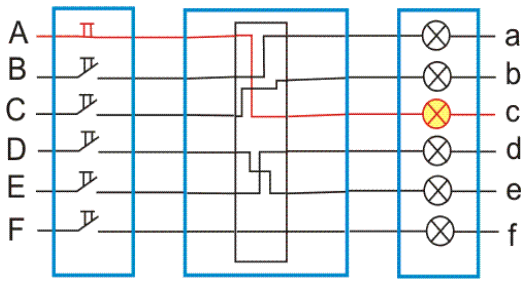
[18] http://www.jproc.ca/crypto/kryha_mech.html

1135 Zeichen in unter 3 Stunden zu entziffern. Trotz dieser Schwäche wurde sie bis in die 1950er Jahre hinein benutzt.

Enigma

Die Enigma, wohl die bekannteste Verschlüsselungsmaschine, wurde bereits im Jahre 1918 durch den deutschen Elektroingenieur Arthur Scherbius (1878–1929) zum Patent angemeldet. Enigma ist Griechisch und bedeutet passenderweise „Geheimnis“. Sie arbeitet ähnlich wie eine Schreibmaschine mechanisch, benötigt aber auch Strom für die Verschlüsselung und besteht im Wesentlichen aus drei Einheiten: der Tastatur für die Eingabe des Klartextes, dem Verschlüsselungsmechanismus und einem Lampenfeld, das bei Betätigung einer Taste den entsprechenden Buchstaben des Chiffrats aufleuchten läßt.

Der Verschlüsselungsmechanismus besteht aus einem Rotorensystem. Die einzelnen Rotoren haben seitlich Schleifkontakte angebracht und leiten den Strom der Tastatur von der einen Seite zu einem anderen Kontakt auf der anderen Seite.

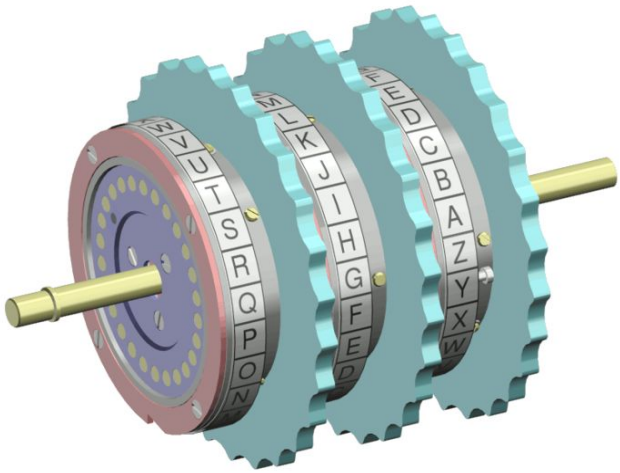


Dieses Bild[19] zeigt genau dieses Prinzip: wird links die Taste A gedrückt, dann fließt der Strom in den Rotor hinein und wird dort, gemäß dem individuellen Aufbau des Rotors, an die Lampe C weitergeleitet, wodurch diese zu leuchten beginnt. Durch die Betätigung der Taste jedoch wird der Rotor nun auch um eine Position weitergedreht, womit ein erneutes Betätigen der Taste A nicht mehr den Buchstaben C, sondern einen anderen leuchten läßt.

In der Grundversion der Enigma wurden nun drei solcher Rotoren nebeneinander gestellt, wodurch sich die Anzahl der Möglichkeiten zur Verschlüsselung eines Buchstaben von 26 auf 26^3 (17576) erhöhte. Ähnlich wie bei einem Kilometerzähler dreht sich die linke Walze bei jedem Anschlag und die jeweils rechte immer erst dann um eine Position weiter, wenn die linke eine komplette Umdrehung vollführt hatte. Sender und Empfänger mußten zum erfolgreichen Ver- bzw. Entschlüsseln natürlich dieselben Rotorstellungen verwenden.

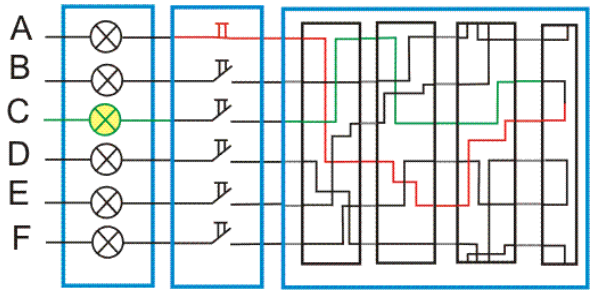
Es ließ sich außerdem mit Hilfe eines gekerbten Ringes an jeder Walze frei entscheiden, ob die nächstgrößere Walze erst beim Wechsel von Z nach A auf Walze 1 eine Position weitersprang, oder an einer beliebigen anderen Position. Die nachfolgende Graphik[20] zeigt die Rotoren und läßt auch eine Übertragungskerbe unten links erkennen:

[19] http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/steffensauer/enigma_aufbau_02.html
[20] http://de.wikipedia.org/wiki/Bild:Enigma_rotor_set.png



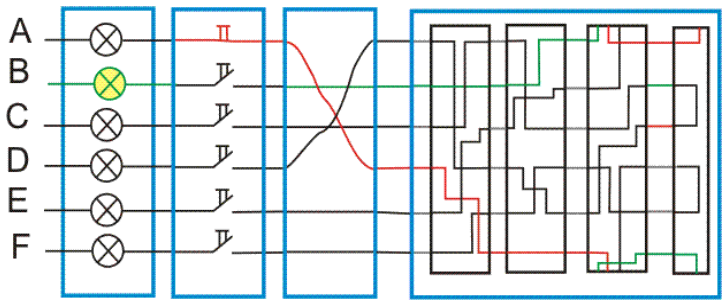
Der Vorteil liegt auf der Hand: ein neugieriger Blick auf die Rotorstellungsanzeige konnte keineswegs Aussage über die Rotorstellung geben.

Ein weiteres Bauelement ist der Reflektor (auch Umkehrwalze genannt), der im Prinzip eine weitere Walze darstellt, die sich aber nicht dreht. Außerdem liegen die elektrischen Kontakte nur an einer Seite. Somit fließt der Strom von der Tastatur durch die drei Walzen, durch den Reflektor, erneut durch die drei Walzen und dann erst auf das Lampenfeld (siehe Abbildung).



Dadurch ergibt sich der Vorteil, daß erstens kein Buchstabe auf sich selbst abgebildet werden kann und daß das Chiffrat mit derselben Methode entschlüsselt werden kann, wie es verschlüsselt wurde. Es handelt sich im Falle der Enigma also um ein symmetrisches Verschlüsselungsverfahren.

Ein letztes Element, das die kryptographische Sicherheit der Enigma extrem verstärkt, ist das Steckbrett, das an der Front angebracht ist. Hiermit ist es möglich, einen beliebigen Buchstaben mit einem anderen zu vertauschen:



Sender und Empfänger mußten zusätzlich zu den Rotorstellungen natürlich auch die benutzte Steckverbindung übermitteln.

In der Praxis nun wurden alle genannten Prinzipien (Rotorreihenfolge, Position des gekerbten Ringes pro Walze, Steckverbindungen sowie Rotorstellung) gemäß vorgegebener Gesetzmäßigkeiten regelmäßig verändert. Dies konnte exemplarisch folgendermaßen aussehen:

```
Tag UKW  Walzenlage  Ringstellung  ---- Steckerverbindungen ----

 31  B   I   IV III    16 26 08    AD CN ET FL GI JV KZ PU QY WX

 30  B   II  V  I      18 24 11    BN DZ EP FX GT HW IY OU QV RS

 29  B   III I  IV     01 17 22    AH BL CX DI ER FK GU NP OQ TY
```

Die erste Zeile bedeutet also, daß am 31. Tag (des Monats) Walze B als Umkehrwalze (UKW) benutzt werden soll. Die Rotoren sollen in der Reihenfolge 1, 4, 3 stehen, die Ringstellung auf Walze 1 soll auf 16 stehen, auf 26 bei 4 und auf 8 bei 3. Außerdem mußte mittels Steckverbindung Buchstabe A gegen D getauscht werden, C gegen N, usf.

Ein sehr schöner Softwarenachbau für den Computer kann unter [21] heruntergeladen werden.

Bomba

Der Pole Marian Rejewski entwickelte 1938 die Bomba, eine Dechiffriermaschine namens Bomba für die Enigma. Der Ansatzpunkt hierfür lag darin, daß die Anwender der Enigma die von ihnen gewählte Rotorstellung zu Anfang einer jeden Nachricht mit dem am jeweiligen Tag aktuellen Trigramm anfügen mußten. Wurde zum Beispiel das Trigramm „ABC“ gewählt, dann tippte der

[21] http://users.telenet.be/d.rijmenants/en/enigmasim.htm

Anwender „ABCABC“ in die Maschine, was zum Beispiel zu „BJEGSM“ werden konnte. Die Tatsache, daß sowohl „BJE“, als auch „GSM“ für „ABC“ standen, lieferte dem 27jährigen Kryptologen das nötige Grundwissen zur Entschlüsselung. Die in der Bomba befindlichen Schlüsselwalzen durchliefen alle möglichen Buchstabenkombinationen für die drei Walzen in einer Enigma, bis die richtige Einstellung gefunden wurde, mit der eine Meldung auf den polnischen Enigma-Nachbauten entziffert werden konnte[22]. Da die Enigma mit drei benutzten Walzen sechs Walzenlagen ermöglicht, benötigte man sechs Bomba. Mit ihnen gelang es, in weniger als zwei Stunden anhand von drei Paaren verschlüsselter Spruchschlüssel, in denen Ein-Buchstaben-Zyklen vorkommen, die Walzenlage und die Ringstellung des Tages herauszufinden.

Kurz bevor Polen von der deutschen Wehrmacht überfallen wurde, übergaben sie ihr Wissen an die Engländer, die, unter der Federführung von Alan Turing, das Verfahren weiter entwickelten und einer verbesserten Enigma Variante (mit zwei neuen Walzen) anpassten. Diese Leistung und vor allem die von Rejewski wird von vielen zurecht als die größte kryptoanalytische Leistung aller Zeiten gesehen.

PURPLE

PURPLE, eigentlich *97-shiki oobun Inji-ki* (zu deutsch: S*ystem 97 Druckmaschine für europäische Zeichen*), nannten die Amerikaner eine japanische Verschlüsselungsmaschine, die vom Prinzip der Enigma sehr ähnelte[23] und ebenfalls im zweiten Weltkrieg eingesetzt wurde. Anstelle von Rotoren benutzte PURPLE allerdings gestaffelte Schalter, wie sie auch in früheren Telefonvermittlungen zur Anwendung kamen. Während 20 Buchstaben des Alphabetes durch vier solcher aufeinanderfolgender Schalter verschlüsselt wurden, wurden die übrigen 6 Buchstaben des Alphabetes nur durch einen Schalter verschlüsselt. Dies stellte sich auch als größte Schwäche der Maschine heraus, zusammen mit der Tatsache, daß sich die Staffelschalter nicht austauschen ließen, wie die Rotoren der Enigma.

---

[22] http://www.wlb-stuttgart.de/seekrieg/ultra/wicher.htm

[23] http://www.hypermaths.org/quadibloc/crypto/ro020304.htm

NEMA

NEMA war der Name einer Rotorverschlüsselungsmaschine aus der Schweiz, die nach dem zweiten Weltkrieg für diplomatische Zwecke eingesetzt wurde. Sie verstand sich als Nachfolgemodell der Enigma und verbesserte deren Prinzip durch den Einsatz von 4 Rotoren und einem ebenfalls drehbaren Reflektor[24]. Eine entscheidende Verbesserung jedoch betraf das Prinzip der Weiterschaltung der Kontaktwalzen. Während sie bei der Enigma - wie bei einem Kilometerzähler - stets nacheinander drehten, verstellten sich bei der NEMA gleich mehrere Walzen gleichzeitig und unabhängig voneinander.

M-209

Die tragbare amerikanische Verschlüsselungsmaschine M-209[25] basierte auf einem Modell des schwedischen Kryptographen Boris Hagelin und erfüllte die Nachfrage nach einem kleinen Gerät, das nicht größer als eine Brotdose war. Zum ersten Mal kam es bei der Afrika Invasion im November 1942 zum Einsatz[26]. Sie funktionierte ohne elektrischen Strom und war demnach ein Meisterwerk der Feinmechanik. Zur Verschlüsselung stellte der Anwender die sechs Rotoren auf den vereinbarten Schlüssel, stellte einen Schalter auf „Verschlüsseln“ und wählte am linken Einstellrad den zu verschlüsselnden Buchstaben aus. Durch Betätigung einer Kurbel wurde nun der entsprechende Buchstabe des Chiffrats auf ein Papierband gedruckt.

[24] http://frode.home.cern.ch/frode/crypto/simula/nema/p1.jpg

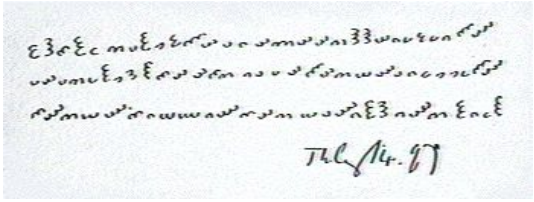
[25] http://www.ilord.com/m209manual.html

[26] http://www.jproc.ca/crypto/m209.html

Die Rotoren hatten allesamt eine unterschiedliche Anzahl von Buchstaben, so daß diese stets teilerfremd war. Die Maschine selbst galt nie als sonderlich sicher und man konnte sie nur dann benutzen, wenn es reichte, die gegnerische Verschlüsselung des Klartextes nur zu verzögern.

Unknackbare Verschlüsselungen?

Alle vorgestellten Verschlüsselungsmethoden hatten gemeinsam, daß sie irgendwann von irgendjemandem, womöglich unter großen Anstrengungen und noch größerem Druck, geknackt wurden. So stellt sich zurecht die Frage, ob es auch derart geniale Verschlüsselungsmethoden gibt, die selbst nach heutigen, durch die Computertechnik beflügelten Gesichtspunkten unknackbar sind. Eine solche Vorstellung, die man wohl eher als Kuriosität bezeichnen sollte, bietet das sogenannte Dorabelle Chiffre. Benutzt wurde es in einem einzigen Text den der britische Komponist Edward Elgar 1897 an seine Geliebte Dora Penny[27] richtete.



Bis heute konnte niemand diesen Brief entschlüsseln. Allerdings steht zu bedenken, daß, wie weiter oben erwähnt, bereits eine homophone Verschlüsselung bei einem entsprechend kurzen Klartext als hinreichend gutes (unknackbares?) Chiffrat gilt. Wenn noch hinzukommt, daß nur ein einziges Exemplar eines Chiffrats vorliegt, dann darf eine Dechiffrierung ohne das Wissen um die angewandte Methodik getrost als unmöglich angesehen werden. In diesem Falle kann man sie aber nicht als praxistaugliche oder „gute“ Verschlüsselungsmethodik ansehen.

Fremde Sprachen als Verschlüsselung

Ob man fremde Sprachen als schlichte, aber brauchbare Verschlüsselungsmethodik betrachten sollte, darf jeder selbst entscheiden. Die USA jedenfalls setzten im Pazifikkrieg gegen Japan ab

[27] http://www.geocities.com/Vienna/4056/cipher.html

1942 tatsächlich Navajo Indianer ein, um die militärischen Anweisungen zu verschlüsseln[28]. Diese Sprache eignete sich deshalb gut, weil sie weder mit europäischen noch mit asiatischen Sprachen verwandt ist. Außerdem werden in Navajo Verben nicht nur nach dem Subjekt, sondern auch nach dem Objekt konjugiert und enthalten Adverbien, die bereits Aufschluß darüber geben, ob der Sprecher etwas selbst erlebt hat oder nur wiedererzählt. Somit können einzelne Verben schon komplette Sätze darstellen. Die Tatsache, daß ausgerechnet die Navajo Indianer zum Einsatz kamen, hing im Übrigen auch damit zusammen, daß sie der einzige Stamm waren, der nicht zuvor durch deutsche Wissenschaftler besucht worden war. Ansonsten, so die Befürchtung, hätte Deutschland dem verbündeten Japan womöglich entscheidene Informationen zukommen lassen können.

Ein anderes und sehr populäres Beispiel für den kryptographischen Charakter einer fremden Sprache stellt wohl die Entschlüsselung der ägyptischen Hieroglyphen dar. Diese wurden ansatzweise erst um das Jahr 1814 durch konkurrierende französische und englische Wissenschaftler verstanden und erst viel später zuverlässig gelesen.

SCHLUSSWORT

Im Informationszeitalter, das auf gewaltige Rechenleistungen zurückgreifen kann, besteht die Gefahr, die kognitiven Leistungen der Leute, die seit tausenden von Jahren Chiffren entwerfen und vor allem brechen, zu unterschätzen.

Der erste Schritt zur erfolgreichen Entschlüsselung jedoch bestand immer darin, Teile des Klartextes zu kennen oder zu erraten. Ob es nun an mangelnder Sorgfalt der Anwender lag oder an Schwachstellen, die vom Erfinder vorher nicht durchdacht wurden, ein Geheimnis kann noch so gut verschlüsselt sein. Es kann noch schwerer sein, es für sich zu behalten.

[28] http://library.nau.edu/speccoll/exhibits/indigenous_voices/navajo/codetalkers.html