swisseduc.ch

Kryptographie und Geschichte

Einblicke in die Geschichte der Geheimsprachen

Abbildung 1: Enigma im Verkehrshaus der Schweiz, Luzern
(https://de.wikipedia.org/wiki/Datei:Enigma_Verkehrshaus_Luzern_cropped.jpg)

Inhaltsverzeichnis

1 Geheimsprachen in der Geschichte

1.1 Steganographie[1]

> ➢ **Die Buchstaben bleiben was sie sind, aber man erkennt nicht, wo die Nachricht ist.**

Schon in vorchristlicher Zeit versuchte man wichtige Botschaften vor den Augen des Feindes zu verstecken. Bekannte Beispiele stammen aus den Perserkriegen. (Als Perserkriege bezeichnet man allgemein die im frühen 5. Jahrhundert v. Chr. von den persischen Großkönigen Dareios I. und Xerxes I. unternommenen Versuche, durch militärische Gewalt Griechenland ihrem Reich anzugliedern). Nachdem Persien in der Schlacht bei Marathon eine Niederlage einstecken musste, begann der persische Großkönig Darius mit einer gewaltigen Aufrüstung seines Heeres. Diese gewaltigen Rüstungsmassnahmen blieben natürlich nicht verborgen. Ein im Exil lebender Grieche namens Demaratos lebte zu dieser Zeit in der persischen Stadt Susa. Er beschloss, eine Nachricht an die Spartaner zu übermitteln, um diese zu warnen. Da er sich jedoch in Feindesland befand, durfte die Botschaft nicht in die Hände der Perser gelangen.

Die damaligen Schreibtafeln bestanden aus Holz mit einer dickeren Wachsschicht. Auf dieser Wachsschicht wurden die Texte und Botschaften eingeritzt. Hätte Demaratos seine Botschaft an die Spartaner dort niedergeschrieben und diese mittels Boten übermittelt, so wäre die Gefahr der Entdeckung zu groß gewesen. Er kam daher auf die Idee, das Wachs der Schreibtafel zu entfernen und die Botschaft direkt auf das Holz zu schreiben. Anschliessend erneuerte er die Wachsschicht wieder und übergab die Tafel einem Boten. Die Schrifttafel erreichte schließlich ihren Bestimmungsort, jedoch waren die Empfänger verwundert über eine leere Tafel. Die Gattin des Leonidas kam nun auf die Idee, das Wachs zu entfernen. Die Spartaner waren gewarnt. Die Griechen begannen jetzt aufzurüsten. Xerxes hatte seinen Überraschungsvorteil verloren und musste um 480 v. Chr. eine verheerende Niederlage einstecken.

Steganographie

Bei der Steganographie werden Nachrichten versteckt, bspw.:

- Beschriebener Seidenstoff wurde in Wachskügelchen eingetaucht und geschluckt.
- Schweineblasen wurden beschrieben und danach in eine Flasche gesteckt und mit Wein gefüllt.
- Unsichtbare Geheimtinte wurde verwendet.

In Herodots Übermittlungen findet sich eine weitere Episode der versteckten Nachrichtenübermittlung. So liess Histaeus einem Boten die Kopfhaut rasieren, brannte die Botschaft ein und wartete, bis die Haare nachgewachsen waren. Nun musste sich der Bote am Zielort nur noch den Kopf rasieren und selbigen zum Lesen hinhalten. Die Liste ließe sich beliebig fortsetzen.

Die verschiedenen Spielarten der Steganographie spielten noch bis in das 20.Jahrhundert eine Rolle. So dürften sich viele wohl noch an einen Briefwechsel mit Geheimtinte in ihrer Jugendzeit erinnern. Der entscheidende Vorteil der versteckten Botschaften besteht zweifelsohne in der Einfachheit der Übermittlung. Der Empfänger der Botschaft muss lediglich wissen, wo die geheime Nachricht versteckt wurde. Jedoch besteht der große Nachteil in der Offenheit der Botschaft.

Während des Zweiten Weltkrieges versteckten Geheimagenten ihre Botschaften in sogenannten Mikropunkten. Dokumente wurden mittels Photographie auf einen Millimeter verkleinert, so dass diese - auf einem herkömmlichen Dokument untergebracht - nicht auffielen. Durch einen anonymen Tipp wurden diese 1941 entdeckt und somit der Inhalt der Botschaft sichtbar. Das Problem der offenen Botschaften war jedoch nicht erst seit dieser Zeit bekannt. Daher entstand zeitgleich mit der Steganographie die Kryptographie (Krypto = verbergen), verstanden als die Wissenschaft von der Verschlüsselung von Informationen.

[1] Gruhn, Ralf, Geschichte der Kryptographie mit Beispielen, Wismar 2004, http:/www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 7ff.

1.2 Aufgaben: Finden Sie die versteckten Botschaften?[2]

Lieber Chef
Mein Mitarbeiter, Herr X, ist immer dabei,
seine Arbeit zu tun, und das sehr eifrig, ohne jemals
seine Zeit mit Schwätzchen zu verplempern. Nie
lehnt er es ab, anderen zu helfen, und trotzdem
schafft er sein Arbeitspensum; oft bleibt er länger
im Büro, um seine Arbeit zu beenden. Er arbeitet sogar
in der Mittagspause. Mein Mitarbeiter ist jemand ohne
Überheblichkeit in Bezug auf seine überragenden
Fachkenntnisse. Er ist einer der Kollegen auf die man
stolz sein kann und auf deren Arbeitskraft man nicht
gern verzichtet. Ich denke, dass es Zeit wird für ihn,
befördert zu werden, damit er nicht auf den Gedanken kommt,
zu gehen. Die Firma kann davon nur profitieren.

[2] Die Beispiele stammen Klaus Schmehs Blog: http://scienceblogs.de/klausis-krypto-kolumne/klaus-schmehs-collection-of-flipflop-ciphers/.

1.2.1 An Amazing Love Story

Once there was a boy who loved a girl very much. The girl's father however didn't like the boy. The boy wanted to write a love letter to the girl but he was sure that the girl's father would read it first. Nevertheless, he wrote this letter:

"This great love I said I have for you
Is gone and I find my dislikes for you
Increases everyday, when I see you
I don't even like the way you look,
The one thing I want to do is to
Look another way. I never wanted to
Marry. Our last conversation
Was very dull and in no way
Has made me anxious to see you again.
You think only of yourself.
If we were married I know that I'd find
Life very difficult nor would I find
Pleasure in living with you. I've heart
To give, but it is not a heart
I want to give you, No one is more
Demanding or selfish than you and less
Able to care for me and helpful to me
I sincerely want you to understand that
I speak the truth. You will do me a favor
If you consider to put this to an end. Do not cry
To answer this. Your letters are full of
Things that do not interest me.
True concern for me. Goodbye! Believe me
I don't care for you. Please don't think
I am still yours"

The girl's father read the letter, was very happy and gave it to his daughter. His daughter read the letter and was very happy too.

"CAN YOU ANSWER WHY WAS SHE HAPPY"

Liebste Eltern! 3.3.333

Macht euch keine Sorgen um uns, die währen wirklich unbegründet. Es währe ganz falsch, wenn ihr denken würdet, gute Eltern, Hänsel und Gretel sind in der Gewalt einer Hexe! Wir leben hier bei einer sehr netten alten Dame, die uns jeden Wunsch von den Augen abliest! Zuerst dachte Gretel ja, wir werden gefangen gehalten und sollten geschlachtet werden! Geht denn so was zu fassen! Wir haben uns dusselig gelacht! Es gibt hier viele Tiere, vor allem Vögel, die fliegen gewöhnlich bis zur großen Eiche und dann in Richtung Norden, dort liegt nämlich ihr Futterplatz. Wir haben auch sehr schöne Puppen, mit denen wir spielen, und dazu viele Einrichtungen, so etwa auch ein Kuchenhaus mit einem Dach aus Schokolade und Marzipan.

Einmal spielten wir Kasperletheater, da haben Löwen die Kaspers auf einen Baum gejagt und da schrien sie: He da ihr Förster! Hier sind wir! Kommt rasch und rettet uns! Eure unglücklichen Dienstzeiten, ihr Waldwächter, sind unmöglich! Ihr müsstet mittags jagen, anstatt Amts pausen zu halten und zu pennen!- Eure Kinder Hänsel und Gretel bitten euch darum, nicht länger zu sorgen, teuerste Eltern! Uns geht`s vorzüglich. Gestern durfte Gretel ein Kleid der lieben alten Dame mit einem rosa Band umsäumen. Vielleicht- sie sprach schon davon- schlachtet morgen die liebe alte Dame ein Gänslein für uns oder sie spielt mit uns wieder Theater. Gestern schenkte sie gar von ihren Marionetten die Hexe Hänsel. Es klingt unglaublich und ist doch die Wahrheit. Dürfen wir dies denn auch annehmen? fragten wir, doch die Gute nickte. Nun will sie mit uns spazieren gehen und ruft uns zu: Eilt! Eilt! Es ist höchste Zeit! Wo bleibt ihr nur! Helft eurer alten Dame den Mantel anzuziehen! So wollen wir jetzt schließen und bitten sehr: Seit sorglos und freut euch mit euren Kindern.

Hänsel und Gretel

2 Codierung[3]

> ➢ **Die Buchstaben bleiben wo sie sind, aber nicht was sie sind. Jeder kann nachschlagen, was sie bedeuten, man nennt so etwas einen Code. Mit einem Code soll nichts geheim gehalten werden.**

Beispiele für Codes sind:

- Morse-Alphabet: Damit kann man sich mit Lichtzeichen verständigen.
- Braille-Schrift: Damit können Blinde lesen.
- Winker-Alphabet: Damit kann man sich in Sicht, aber außer Hörweite verständigen.

2.1 Morse

1832 erfand der Amerikaner Samuel Morse den Morsetelegraphen. Damit konnte man Nachrichten über grosse Entfernungen übermitteln. Dazu wurden Telegraphenmasten aufgestellt und Leitungen durch das ganze Land gespannt. Es war nicht möglich, gesprochene Worte zu übertragen, sondern lediglich kurze oder lange elektrische Impulse. Deshalb dachte sich Morse ein Alphabet aus, das nur aus kurzen und langen Signalen bestand. Die Wahl der Codes für die verschiedenen Zeichen orientiert sich an der geschätzten Buchstabenhäufigkeit in der englischen Sprache. Öfter auftretende Buchstaben sollten einen kürzeren Code besitzen als seltenere, um die zu übertragenden Zeichen zu minimieren

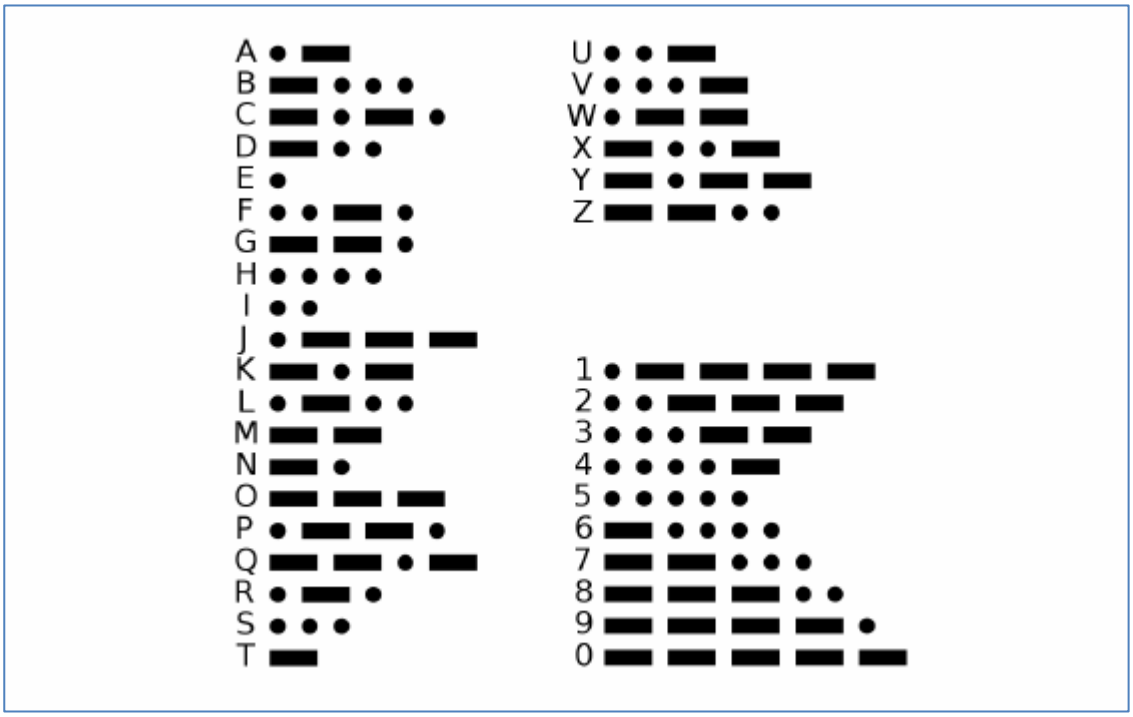


Abbildung 2: Der Morsecode

2.1.1 Aufgaben: Können Sie folgende Code entschlüsseln:

[3] Ausgezeichnetes Material zu Kryptographie findet man auf der Seite der Bergischen Universität Wuppertal: http://ddi.uni-wuppertal.de/material/spioncamp.html. Das vorliegende Material stammt von dieser Seite, vgl. dazu auch das dortige Manual: http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

2.1.2 Eine „harmlose“ Kinderzeichnung

Abbildung 3: Finden Sie die äusserst fragwürdige Botschaft :-)?[4]

[4] http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

3 Kryptographie

Unter dem Begriff der Kryptographie versteht man ganz allgemein, die Wissenschaft von der Verschlüsselung von Informationen. Es gibt dabei zwei häufig verwendete Verfahren: Die Transposition und die Substitution.

3.1 Transposition

> ➢ **Bei der Transposition bleiben die Buchstaben, was sie sind, aber nicht wo sie sind.**

(Das Wort Transposition ist abgeleitet vom lateinischen Wort transponere = verschieben. Ein Beispiel für eine Transposition ist die Skytale).

3.1.1 Skytale[5]

Vom griechischen Historiker Plutarch wissen wir, dass die Spartanische Regierung Nachrichten an ihre Generäle wie folgt verschlüsselte: Man wickelte einen Pergament- oder Lederstreifen um einen Zylinder und schrieb in horizontaler Richtung die Botschaft zeilenweise auf (vgl. Abbildung 3). Danach löste man den Streifen vom Zylinder und überbrachte den verschlüsselten Text. Die Entschlüsselung war einfach, man benötigte dazu einen Zylinder gleichen Umfangs, bzw. mit gleichem Radius. Sehr sicher war dieses Verfahren nicht, da man durch Probieren den Umfang des Zylinders erraten und so den Text entziffern konnte.

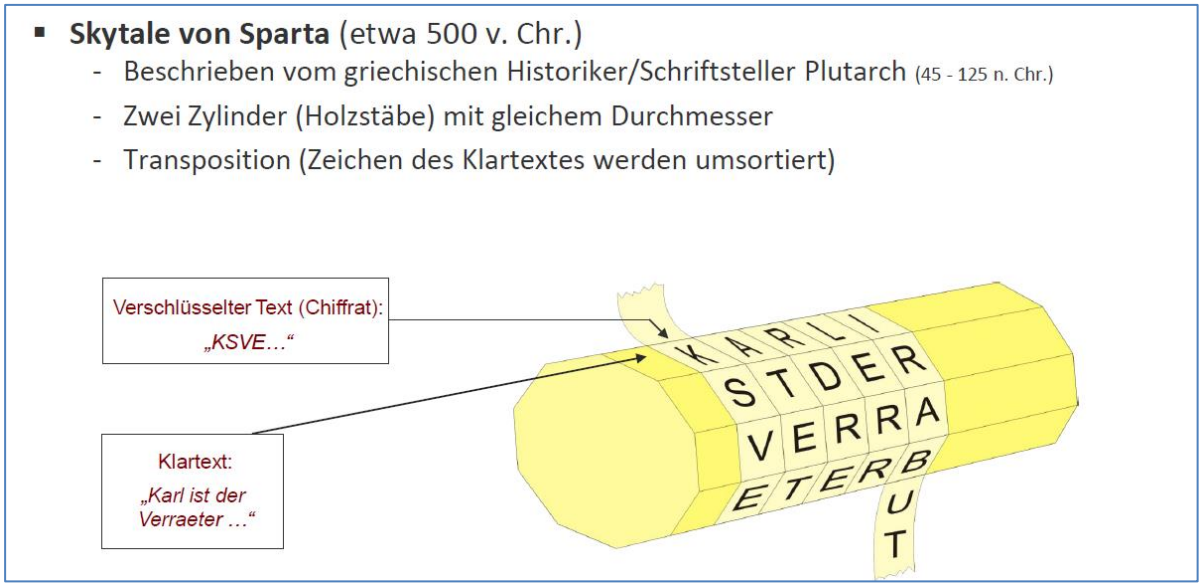


Abbildung 4: Beispiel einer Verschiebung von Buchstaben[6]

3.1.2 Aufgabe: Können Sie folgende Nachricht ohne Skytale knacken?[7]

K R C I O G H N M E B X M N E D M N R K O A L P

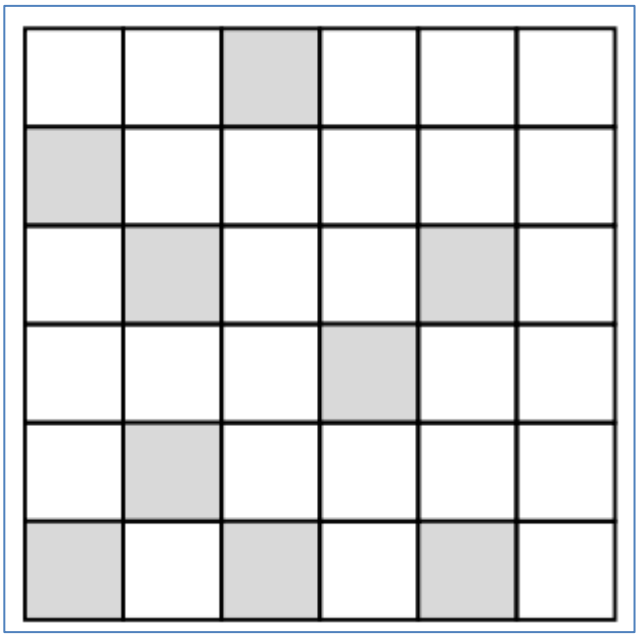
[5] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 9.
[6] https://www.cryptoportal.org/data/CrypTool%201.4.30%20German%20v11.pdf, S. 9.
[7] http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

3.1.3 Schablone

Ein Geheimtext kann auch mit einer Schablone erstellt werden (Fleißnersche Schablone). Die Schablone besteht aus einem Quadrat, aus dem mehrere kleinere Quadrate ausgeschnitten werden. Die Schablone wird auf ein Blatt Papier gelegt und jeweils ein Buchstabe des Klartextes wird in ein ausgeschnittenes Quadrat eingetragen. Dann wird die Schablone um neunzig Grad gedreht und die nächsten Buchstaben werden in die Lücken eingetragen. Das Ganze erfolgt viermal, so dass ein Quadrat mit Buchstaben entsteht. Ist die Nachricht länger, wird ein neues Quadrat begonnen. Ist sie kürzer, werden die übrig gebliebenen Lücken mit willkürlich gewählten Buchstaben aufgefüllt.[8]

3.1.4 Aufgabe: Können Sie folgenden Text mit der Schablone entschlüsseln?[9]

C	E	D	R	H	T
I	T	5	Z	S	S
E	E	I	E	N	R
K	C	S	A	H	U
T	C	N	O	D	I
H	E	R	N	I	N



[8] https://de.wikipedia.org/wiki/Flei%C3%9Fnersche_Schablone.
[9] http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

3.2 Substitution

> ➢ **Die Buchstaben bleiben wo sie sind, aber nicht was sie sind.**

(Solche Verschlüsselungen heißen Substitution. Das Wort Substitution ist abgeleitet vom lateinischen Wort substituere = ersetzen).

3.2.1 Cäsar

Der römische Feldherr Julius Caesar verschlüsselte seine Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Diese Anzahl der Stellen nennt man Caesar-Schlüssel. Es können somit 25 verschiedene Geheimschriften erzeugt werden.

Beispiel Beim Schlüssel 3 nahm Caesar immer den Buchstaben, der im Alphabet drei Stellen weiter rechts steht.
Dazu schrieb er das Alphabet zweimal untereinander. Das untere Alphabet schrieb er allerdings um drei Stellen verschoben.

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

Caesar ersetzte also in seinem Text jedes **A** durch ein **D**, jedes **B** durch ein **E** usw. Beachte, dass **X** durch **A** ersetzt wird, also das Alphabet nach dem Z einfach mit A weitergeschrieben wird.

Abbildung 5: Die Cäsar-Verschlüsselung[10]

Auf der folgenden Seite findet man eine Chiffrierscheibe, um die Cäsar-Verschlüsselung schneller zu ver- oder entschlüsseln.

[10] Text und Bild von: http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf

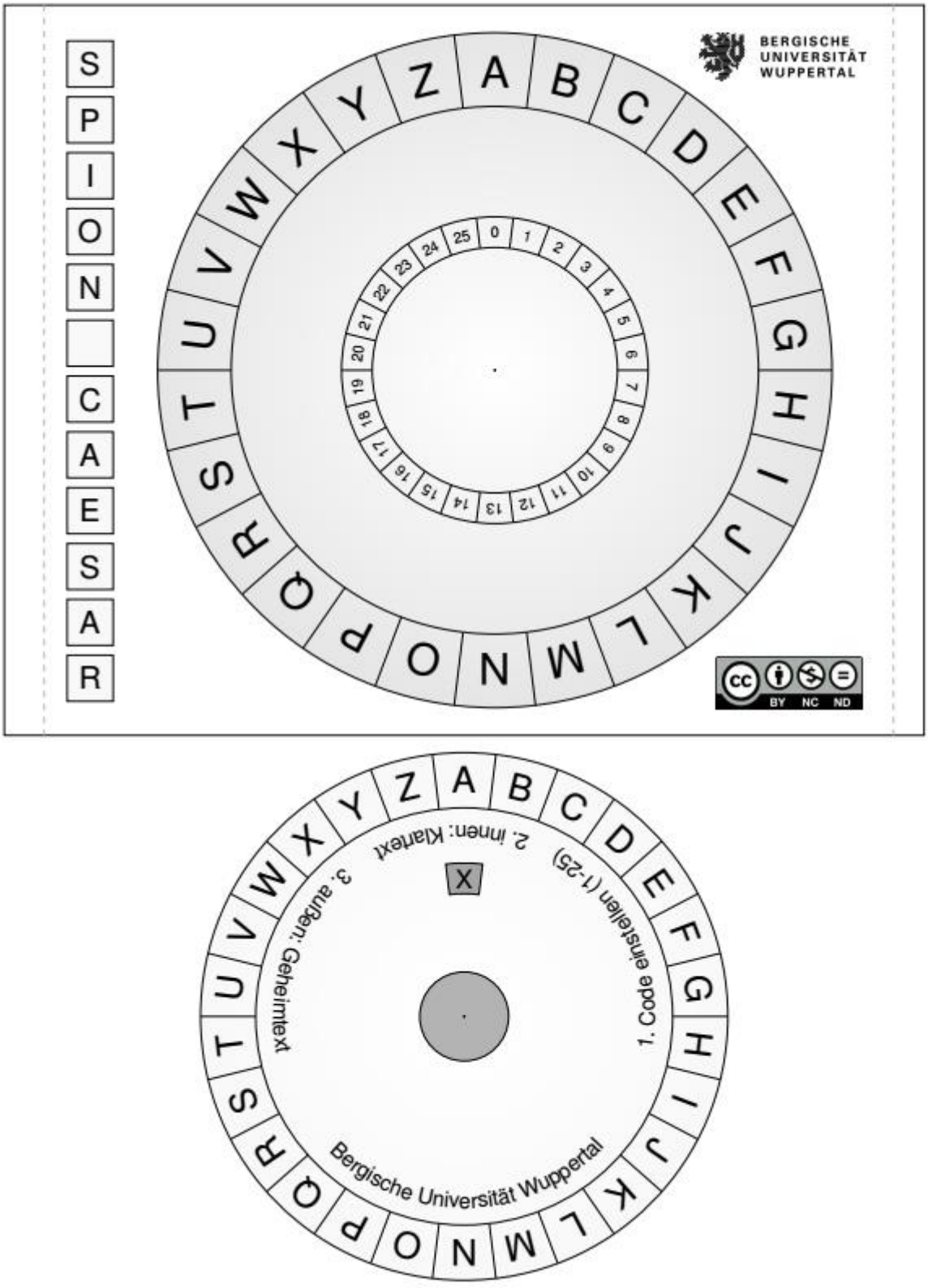


Abbildung 6: Chiffrierscheibe für die Cäsar Verschlüsselung[11]

[11] http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

Die Caesar-Verschlüsselung kann leicht geknackt werden. Man muss maximal 25 Schlüssel durchprobieren, um den Klartext zu erhalten. Schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird. Das funktioniert wie folgt:

- Sender und Empfänger einigen sich auf ein Schlüsselwort.
- Dieses Wort schreibt man unter ein normales Alphabet. Buchstaben, die doppelt vorkommen, lässt man dabei weg.
- Anschließend wird das Alphabet mit den noch nicht benutzten Buchstaben, in alphabetischer Reihenfolge beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt.
- Kein Buchstabe darf doppelt vorkommen.

Beispiel Schlüsselwort: GEHEIMSCHRIFT. Dieses Schlüsselwort wird unter das Alphabet geschrieben, doppelte Buchstaben werden dabei weggelassen.

	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
wird ersetzt durch	G	E	H	I	M	S	C	R	F	T																

Nun wird mit den restlichen Buchstaben aufgefüllt.

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

Mit dieser Tabelle wird dann ver- und entschlüsselt.

Abbildung 7: Cäsar Verschlüsselung mit einem Schlüsselwort[12]

3.2.2 Aufgabe: Cäsar entschlüsseln

1. Können Sie die Nachricht ohne bekannten Schlüssel entschlüsseln? ***YHQL YLGL YLFL?***
2. Entschlüsseln Sie (evtl. mit einer Chiffrierscheibe) die folgenden Nachrichten. Mögliche Schlüssel sind: 2, 7, 10, 13. Einer ist jeweils der richtige Schlüssel.

   a) SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU?
   b) YVRORE PNRFNE, VPU JREQR QN FRVA.

Wenn man mit einem Geheimtextalphabet Umstellungen des Klartextalphabets zulässt, kann man eine sehr viel grössere Zahl von Geheimschriften erzeugen. Es gibt dann über 400 000 000 000 000 000 000 000 000 solcher Neuanordnungen. Wenn ein Agent jede Sekunde einen der 400 000 000 000 000 000 000 000 000 möglichen Schlüssel testen würde, benötigt er die milliardenfache Lebensdauer des Universums, um sie alle zu testen und die Nachricht zu entschlüsseln.[13]

Wie soll man eine so verschlüsselte Botschaft knacken? Damit beschäftig sich die Kryptoanalyse, darunter versteht man Methoden und Techniken, um Informationen aus verschlüsselten Texte zu gewinnen.

[12] Bild, Text und Aufgabe aus: http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

[13] Singh, Simon, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 2000, S. 26ff.

4 Die Kryptoanalyse[14]

Um 610 n. Chr. erschien Mohammed der Erzengel Gabriel und Mohammed war fortan Prophet. Die darauffolgenden Offenbarungen wurden nach Mohammeds Tod von dem Kalifen Abu Bakr in 114 Kapiteln zum Koran zusammengefasst. In den theologischen Schulen wurden die Kapitel des Koran erforscht. Die Gelehrten interessierte auch die zeitliche Einordnung der Offenbarungen des Mohammed. Der Gedanke war folgender: Bestimmte Wörter stammen aus anderen zeitlichen Epochen. Die Forscher untersuchten daher auftretende Häufigkeiten von Wörtern der damaligen Zeit von Offenbarungen. Wurde ein nicht mehr sehr gebräuchliches Wort häufig gezählt, so konnte diese Offenbarung chronologisch in die entsprechende Zeit eingeordnet werden, in der dieser Sprachgebrauch üblich war. Diese Technik fand schließlich auch Verwendung für einzelne Buchstaben. Dabei entdeckte man, dass gewisse Buchstaben häufiger auftauchten als andere. Im arabischen sind dies ”a” und ”l” für den Artikel ”al”. Andere Buchstaben tauchten prozentual gesehen weniger häufig auf. Diese Beobachtung war der Schlüssel zur Kryptoanalyse und somit deren Geburtsstunde.

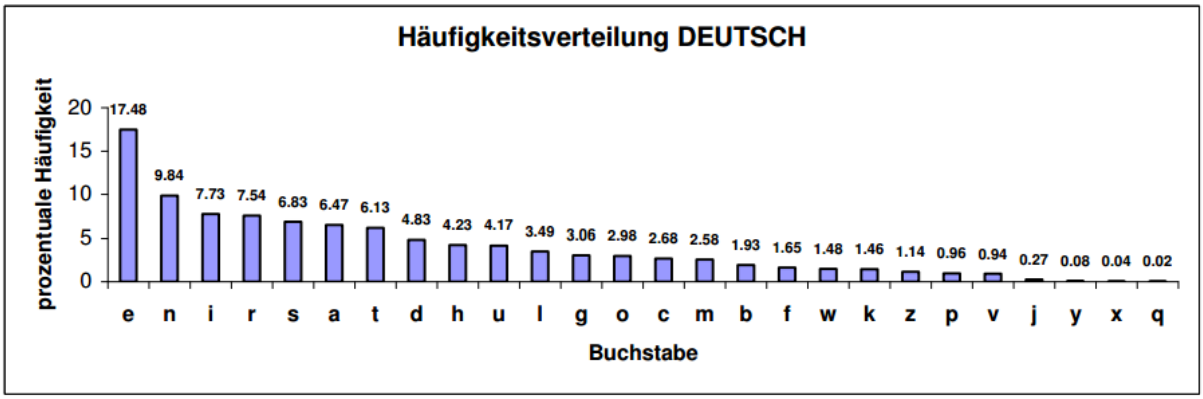
Es lässt sich nicht genau einordnen, wann mit der ersten Kryptoanalyse begonnen wurde. Die erste schriftliche Erwähnung dieses Verfahrens stammt von einem Gelehrten des 9. Jahrhunderts namens Al-Kindi. Erst 1987 wurde in einem Istanbuler Archiv sein Werk mit dem Namen ”Abhandlung über die Entzifferung kryptografischer Botschaften” gefunden. Der entscheidende Abschnitt seines Artikels beschreibt die Kryptoanalyse sinngemäß wie folgt: Man muss einen Klartext derselben Sprache finden, welcher lang genug ist um ein bis zwei Blätter zu füllen. Jetzt müssen die Buchstaben gezählt und nach ihrer Häufigkeit sortiert werden. Des häufigsten Buchstaben nennt man ”erster”, dann ”zweiter” und so weiter. Der Geheimtext wird nach dem gleichen Verfahren sortiert und auch hier die häufigsten Symbole mit ”erster”, ”zweiter”, ... bezeichnet. So müssen die jeweiligen Buchstaben nur noch eingesetzt werden, um den Test zu entschlüsseln. Al-Kindis Verfahren nennt man Häufigkeitsanalyse.

Die Häufigkeitsanalyse sorgt dafür, dass nicht alle Möglichkeiten bei einer angewendeten Substitution probiert werden müssen. Wir erinnern uns, bei einer reinen alphabetischen Substitution waren dies 25 Möglichkeiten. Je nach Länge des ausgewerteten Textes kann sich für das deutsche Alphabet folgende Häufigkeit ergeben:

4.1.1 Eine knifflige Aufgabe: Finden Sie den Klartext?[15]

Der nachfolgende Geheimtext wurde mit einem monoalphabetischen Verfahren verschlüsselt. Der Klartext ist in Deutsch. Entschlüsseln Sie ihn.

XDY IKJKAHMCALYQDPECY SYOPECHRYPPYHRJB DPQ DI WYDQAHQYO XYP EKIMRQYOP JDECQ IYCO AGQRYHH. PDY DPQ SDYH WR YDJZAEC WR GJAEGYJ RJX PKIDQ ZRYO XYJ PDECYOYJ XAQYJARPQARPEC JDECQ BYYDBJYQ



[14] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 13ff.
[15] http://swisseduc.ch/informatik/daten/kryptologie_geschichte/docs/caesar_knacken_aufgabe.pdf.

4.1.2 Historisches Beispiel: Die Hinrichtung von Maria Stuart[16]

Maria Stuart, Königin von Schottland, war des Verrats angeklagt. Sie wurde beschuldigt, an einer Verschwörung zur Ermordung von Königin Elisabeth I. beteiligt gewesen zu sein, mit dem Ziel, selbst die englische Krone an sich zu reissen. Sir Francis Walsingham, der für die Sicherheit zuständige Minister Elisabeths, hatte die anderen Verschwörer bereits verhaften lassen, ihnen Geständnisse abgepresst und sie hingerichtet. Nun wollte er beweisen, dass Maria das Herz des Komplotts war.

Walsingham wusste genau, dass er Königin Elisabeth von der Schuld Marias überzeugen musste, wenn er sie hinrichten lassen wollte. Zwar verabscheute Elisabeth Maria, doch sie hatte gute Gründe, vor einem Todesurteil zurückzuschrecken. Zum einen war Maria eine schottische Königin, und viele bezweifelten, dass ein englisches Gericht befugt war, ein ausländisches Staatsoberhaupt zum Tode zu verurteilen. Zum andern würde die Hinrichtung Marias einen Präzendenzfall schaffen – wenn es dem Staat erlaubt war, diese Königin zu töten, dann würden die Aufständischen vielleicht weniger Skrupel haben, eine andere Monarchin zu töten, nämlich Elisabeth selbst. Zudem waren Elisabeth und Maria Kusinen, und diese Blutsverwandtschaft liess Elisabeth erst recht vor der letzten Konsequenz zurückscheuen. Kurz, Elisabeth würde Marias Hinrichtung nur gutheissen, wenn Walsingham zweifelsfrei beweisen konnte, dass sie in eine Mordverschwörung verstrickt war.

Die Verschwörer benutzten eine monoalphabetische Verschlüsselung und fügten zusätzlich noch Codewörter ein.

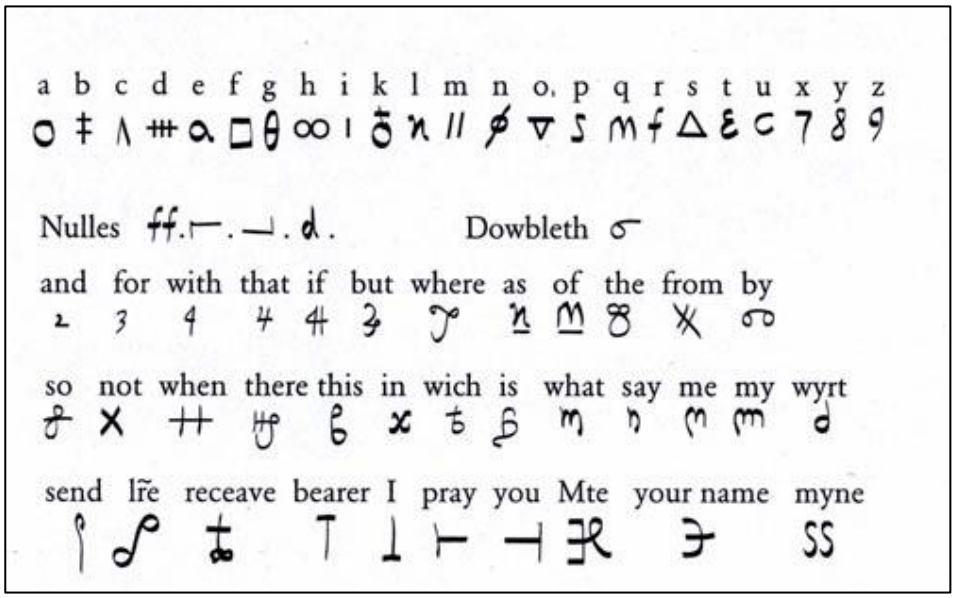


Abbildung 8: Maria Stuarts Geheimtextalphabet und Codewörter

Dieses Verfahren ist an sich zwar etwas sicherer als eine einfache monoalphabetische Verschlüsselung, aber nicht wirklich vor der Entzifferung geschützt, denn der Großteil der Nachricht kann durch Häufigkeitsanalyse entschlüsselt werden und Kryptoanalytiker können die restlichen Wörter aus dem Textzusammenhang herausfinden.

Der Code wurde von Thomas Phelippes, welcher damals für Francis Walsingham arbeitete, gebrochen und führte zur Hinrichtung Maria Stuarts. Die einfache monoalphabetische Verschlüsselung gewährte jahrhundertelang ausreichend Sicherheit, bis sie durch die Entwicklung der Häufigkeitsanalyse in Arabien und Europa untergraben wurde. Das tragische Ende Maria Stuarts machte die Schwäche dieser Verschlüsselung deutlich.

[16] Singh, Simon, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 2000, S. 15ff.

4.2 Die polyalphabetische Verschlüsselung[17]

Die monoalphabetische Verschlüsselung bot seit der Erfindung der Häufigkeitsanalyse keine Sicherheit mehr. Die Kryptoanalytiker hatten vorläufig gewonnen und waren in der Lage, diese Texte zu entschlüsseln. Um 1460 bahnte sich aber eine neue Erfindung an. Der italienische Mathematiker Leon Battista Alberti erfand ein modifiziertes Substitutionsverfahren. Seine Idee bestand darin, anstatt einen Schlüssel, mehrere Schlüssel zu verwenden und zwischen diesen hin und her zu springen.

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

Abbildung 9: Mehrschlüssel - Verfahren

Die erste Reihe entspricht in diesem Beispiel dem Klartext-Alphabet, die zwei anderen Reihen dem ersten und dem zweiten Schlüssel. Aus dem Wort „Hallo“ wird nun der verschlüsselte Text ”udboc”. Für jeden Buchstaben bestehen in diesem Beispiel zwei Möglichkeiten der Verschlüsselung, so wird aus den beiden „ll“ im Wort „Hallo“ ein „bo“.

Alberti legte damit den Grundstein für die bekannte Vigenère-Verschlüsselung. Blaise de Vigenère (1523 – 1596) stieß während eines Aufenthaltes in Rom auf die Texte von Alberti, Trithemius und Porta und verband die Schriften der drei zu einem in sich schlüssigen Kryptographieverfahren, der Vigenère-Verschlüsselung.

Die Verschlüsselung funktioniert wie folgt:[18]

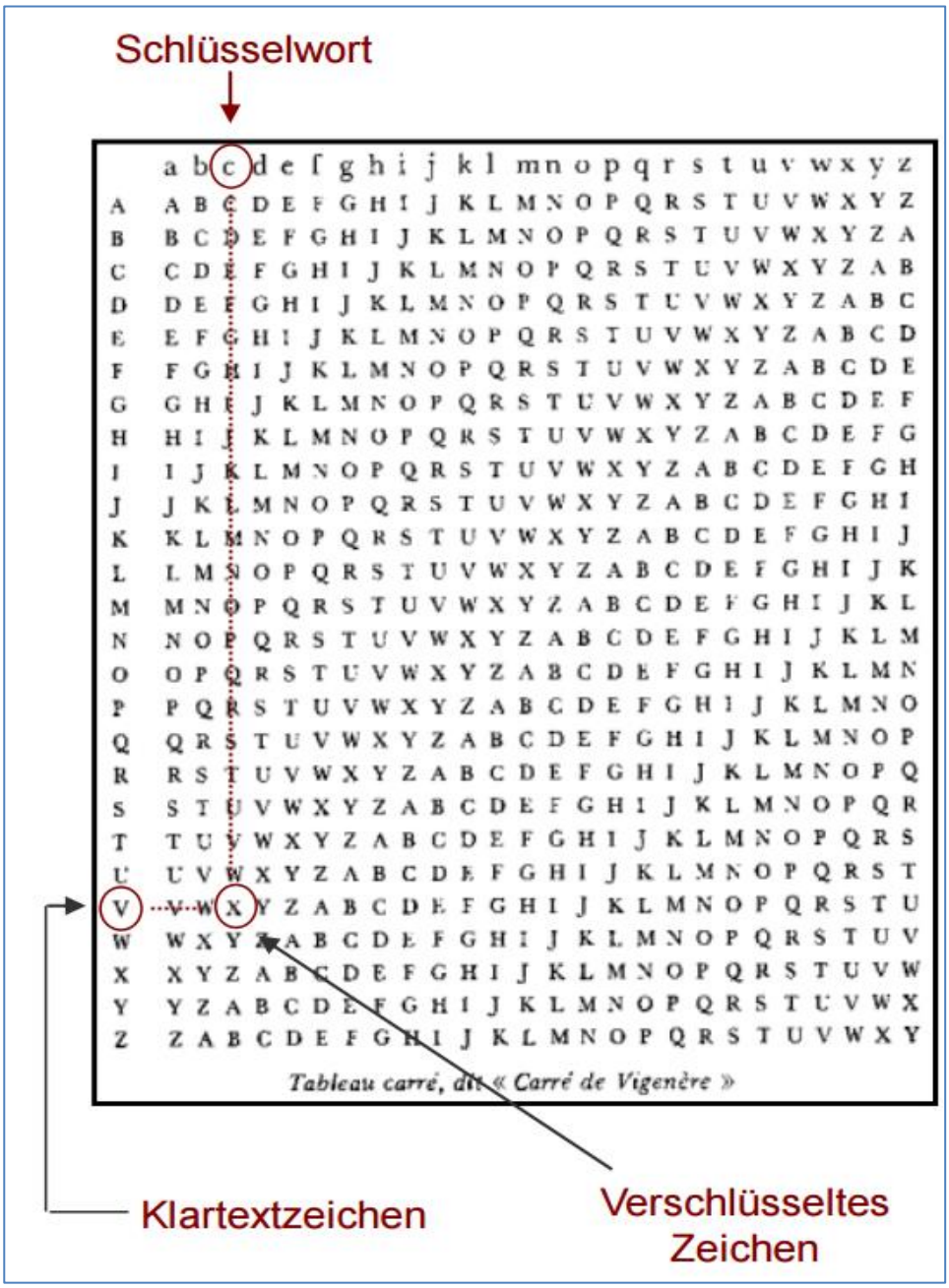
- Sender und Empfänger einigen sich auf ein Schlüsselwort. Dieses wird unter die Nachricht geschrieben. Unter jeden Buchstaben der Nachricht wird ein Buchstabe des Schlüsselwortes geschrieben. Das Schlüsselwort wird dabei ständig wiederholt.
- Nun nimmt man sich jeweils einen Buchstaben der Nachricht und sucht ihn in der ersten Zeile des Vigenère-Quadrates. Von da aus geht man nach unten bis zu dem Alphabet, das ganz links mit dem entsprechenden Buchstaben des Schlüsselwortes beginnt.
- Der Buchstabe, den man dort findet, ist der verschlüsselte Buchstabe.

[17] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 18f.
[18] http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.

4.2.1 Beispiel für eine Vigenère Verschlüsselung [19]

Schlüsselwort: CHIFFRE

Verschlüsselung: VIGENERE → XPOJSVVG



[19] https://www.cryptoportal.org/data/CrypTool%201.4.30%20German%20v11.pdf, S. 11.

4.2.2 Aufgabe: Entschlüsseln Sie folgenden Text[20]

XIM XSFRQAK (Das Schlüsselwort ist ROT)

Klartext

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

Bei dieser Verschlüsselung kann ein Buchstabe mehrmals im Geheimtext vorkommen, das macht die Sache sehr schwierig. Vigenère vollendete sein Werk 1586, im selben Jahr als die Geheimschrift von Maria Stuart entschlüsselt wurde.

Die Vigenère-Verschlüsselung kann durch die Häufigkeitsanalyse nicht mehr entschlüsselt werden, weil einzelne Klartextbuchstaben durch verschiedene Geheimbuchstaben substituiert werden können. Die Komplexität der Verschlüsselung lässt sich zusätzlich steigern, indem man einen längeren Schlüssel wählt.[21]

4.2.3 Die Homophone Verschlüsselung[22]

Die polyalphabetische Verschlüsselung konnte sich kaum verbreiten, da das Verfahren umständlich zu handhaben war. Man versuchte daher, einen Mittelweg zu finden. Das neue Verfahren sollte schwerer zu entschlüsseln sein als die monoalphabetische Verschlüsselung, jedoch einfacher in der Anwendung sein als die Polyalphabetische. Die Lösung fand man in der homophonen Verschlüsselung. Die Buchstaben wurden durch Platzhalter in Form von Zahlen ersetzt. Eine solche Geheimschrift konnte aber mittels Häufigkeitsanalyse einfach entschlüsselt werden. Da dies allgemein bekannt war, wollte man die auftretenden Häufigkeiten «neutralisieren». Gemäß der Häufigkeitstabelle tritt das «e» mit 17% und das «n» mit 10% Häufigkeit auf (weitere Häufigkeiten gem. Tabelle). Stellt man als Platzhalter für das «e» 17 verschiedene

[20] http://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf.
[21] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 21.
[22] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 22f.

Platzhalter in Form von 17 verschiedenen Zahlen zur Verfügung und analog dazu für die anderen Häufigkeiten auch die entsprechende Anzahl, dann sind die auftretenden Häufigkeiten gleichverteilt. Damit kann man eine Tabelle erstellen, in der für jeden Buchstaben in Abhängigkeit seiner Wahrscheinlichkeit zweistellige Zahlen zugeordnet sind. Beispiel für das «e»: 45 79 14 16 24 44 46 55 57 64 74 82 87 98 10 31 06. Das «e» kann nun mit diesen 17 Zahlen substituiert werden. Aufgrund der Gleichverteilung von 1% gibt es keine Möglichkeit, dieses Verfahren zu brechen, aber es gibt unscheinbare Spuren.

Unscheinbare Spuren entstehen durch gewisse Buchstabenkombinationen im deutschen Alphabet. So folgt auf das sehr seltene q immer der Buchstabe u. Diese Gesetzmäßigkeit lässt sich natürlich ausnutzen. Man sucht in einem geeigneten langen Text nach einer Zahl, welche nur einmal auftaucht. Wenn dann noch hinter dieser Zahl immer eine von vier gleichen Zahlen erscheint, so handelt es sich vermutlich um das u (siehe Häufigkeitstabelle). Ein weiterer Einstieg könnte sein, sich die Häufigkeiten von Bi-und Trigrammen (zwei- oder drei aufeinanderfolgende Buchstaben) zunutze zu machen.

Das Verfahren der homophonen Verschlüsselung lässt sich knacken, es ist jedoch wesentlich mehr Aufwand nötig ist als bei der reinen Monoalphabetischen. Es ist auch nicht so sicher wie die Polyalphabetische, aber gleichzeitig auch nicht so aufwendig zu verschlüsseln. Es war also genau das, wonach man zu dieser Zeit suchte.[23]

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
09	78	48	13	45	25	39	65	83	51	84	22	58	71	95	29	35	40	76	49	61	89	28	21	52	66
12	92	81	41	79	23	50	68	88			27	59	91	94			42	86	69	63					
33			62	14		56	32	93			18		00				77	96	75	34					
47			01	16			70	15					05				80	17	85	60					
53			03	24			73	04					07				11	20	97						
67				44				26					54				19	30	08						
				46				37					72				36	43							
				55				58					90												
				57									99												
				64									38												
				74																					
				82																					
				87																					
				98																					
				10																					
				31																					
				06																					

Abbildung 10: Häufigkeitstabelle für deutsche Buchstaben mit Zahlen als Platzhalter

4.3 Die Entschlüsselung von Vigenère[24]

Wie war es möglich, die komplexe Vigenère-Verschlüsselung zu brechen. Die Entschlüsselung verdanken wir einem exzentrischen Genie des 19. Jahrhunderts: Charles Babbage.

Ein Zeitgenosse von Babbage behauptete, eine neue Verschlüsselung erfunden zu haben. Babbage wies den Mann darauf hin, dass diese Vigenère-Verschlüsselung schon lange existierte und er deshalb nichts Neues entdeckt habe. Der vermeintliche Entdecker war empört und forderte Babbage auf, seine Verschlüsselung zu knacken. Babbage fühlte sich herausgefordert und begann eine Lösung zu suchen.

[23] Grafik aus: Singh, Simon, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 2000, S. 74f.

[24] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 23ff.

4.3.1 Vigenère Chiffre brechen[25]

Wenn in einer Vigenère Verschlüsselung das Schlüsselwort «Key» lautet, so kommen nur drei verschiedene, sich wiederholende, Cäsar-Alphabete zum Einsatz. Die Sicherheit hängt von der Länge des Schlüssels ab. Wenn der Schlüssel nur aus einem Zeichen besteht, so wird jeder Buchstabe mit demselben Caesar-Alphabet chiffriert; das heisst, wir hätten eine Cäsar-Verschlüsselung. Genau hier setzte Babbage an: Es galt zuerst die Schlüssellänge herauszufinden. Anschließend muss der Angreifer noch eine Häufigkeitsanalyse für die sich wiederholenden Cäsar-Alphabete durchführen. Das Vorgehen sieht wie folgt aus:

- (wahrscheinlichen) Passwort-Abstand bestimmen
    - Zeichenketten (ab drei Zeichen) suchen, die mehrfach vorkommen. Den Abstand zueinander tabellieren
    - alle Teiler der Abstände aufschreiben
    - wahrscheinlichsten auswählen
- bei Passwort der Länge n hat man jetzt n Texte
- den Geheimtext schreibt man dann in n = 4 Spalten an. In der ersten Spalte stehen alle Zeichen, die mit dem ersten Schlüsselwortbuchstaben verschlüsselt wurden, in der zweiten Spalte wurden alle Zeichen mit dem zweiten Schlüsselwortbuchstaben verschlüsselt, usw. Pro Spalte liegt daher eine Cäsar-Verschlüsselung vor. Diese n Cäsar - Codes können wie oben beschrieben geknackt werden. Fügt man die Spalten anschließend wieder zusammen, so erhält man den Klartext.[26]

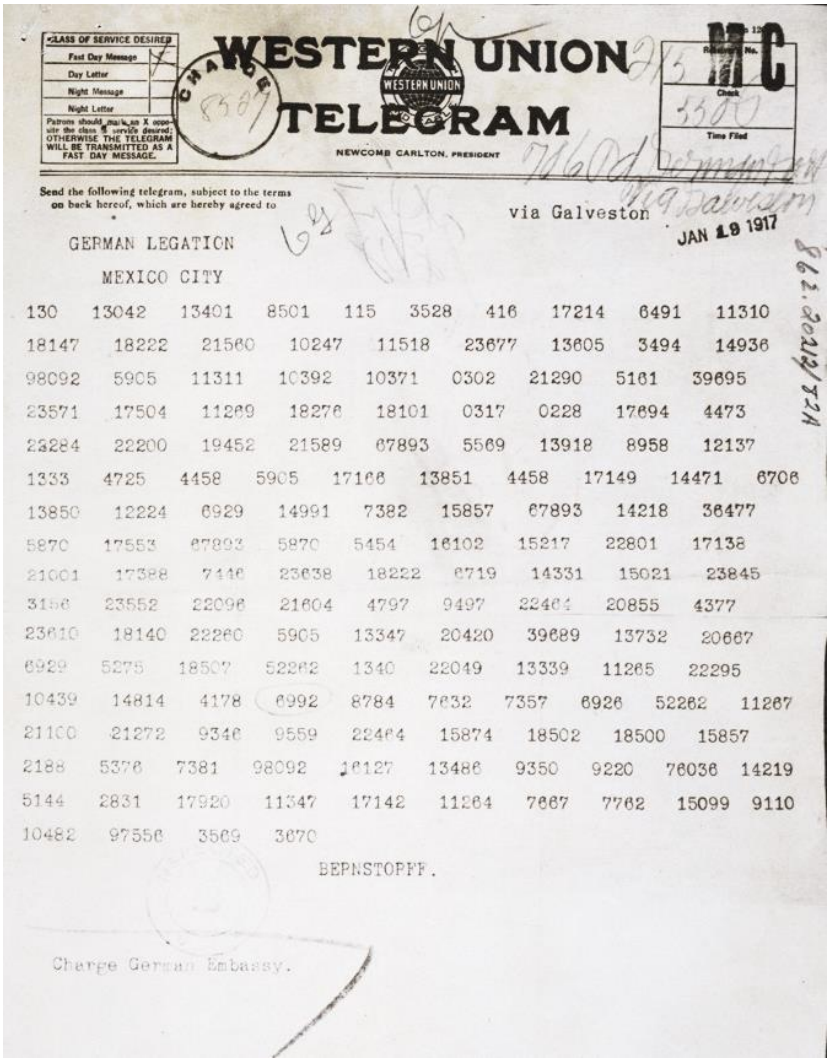
5 Historisches Beispiel: Die Zimmermann-Depesche[27]

Die Zimmermann-Depesche (auch Zimmermann-Telegramm) war ein verschlüsseltes Telegramm, das Arthur Zimmermann, der deutsche Staatssekretär des Auswärtigen Amts, am 19. Januar 1917 über die deutsche Botschaft in Washington, D.C. an den deutschen Gesandten in Mexiko sandte. Das Telegramm bot Mexico Unterstützung an, wenn sie Amerika angreifen würden.

[25] http://www.cryptool-online.org/index.php?option=com_content&view=article&id=51&Itemid=98&lang=de.

[26] Ein Beispiel dazu: http://swisseduc.ch/informatik/daten/kryptologie_geschichte/docs/vigenere_knacken_loesung.pdf.

[27] https://de.wikipedia.org/wiki/Zimmermann-Depesche sowie http://www.sueddeutsche.de/politik/mexiko-die-usa-und-das-deutsche-kaiserreich-wie-pancho-villa-den-ersten-weltkrieg-bestimmte-1.1884405.



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

CLASS OF SERVICE DESIRED: Fast Day Message / Day Letter / Night Message / Night Letter

Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310

18147 18222 21560 10247 11518 23677 13605 3494 14936

98092 5905 11311 10392 10371 0302 21290 5161 39695

23571 17504 11269 18276 18101 0317 0228 17694 4473

23284 22200 19452 21589 67893 5569 13918 8958 12137

1333 4725 4458 5905 17166 13851 4458 17149 14471 6706

13850 12224 6929 14991 7382 15857 67893 14218 36477

5870 17553 67893 5870 5454 16102 15217 22801 17138

21001 17388 7446 23638 18222 6719 14331 15021 23845

3156 23552 22096 21604 4797 9497 22464 20855 4377

23610 18140 22260 5905 13347 20420 39689 13732 20667

6929 5275 18507 52262 1340 22049 13339 11265 22295

10439 14814 4178 6992 8784 7632 7357 6926 52262 11267

21100 21272 9346 9559 22464 15874 18502 18500 15857

2188 5376 7381 98092 16127 13486 9350 9220 76036 14219

5144 2831 17920 11347 17142 11264 7667 7762 15099 9110

10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.

Abbildung 11: Das verschlüsselte Zimmermann Telegramm

1916 und 1917 standen Mexiko und die USA zeitweise am Rand eines offenen Krieges. Diese Spannungen wollte Deutschland schüren - ähnlich wie man später auch die revolutionären Umtriebe in Russland förderte, indem man Lenin aus seinem Schweizer Exil quer durch Deutschland heimlich ins Zarenreich schaffte. Zimmermann hoffte, mittels der mexikanischen Bürgerkriegsarmeen, die Vereinigten Staaten von einem Eintritt in den Ersten Weltkrieg abhalten zu können: Je unruhiger es an der mexikanisch-amerikanischen Grenze sei, desto geringer werde Washingtons Interesse am europäischen Krieg sein.

Ziel war ein Bündnis zwischen Deutschland und Mexiko für den Fall, dass die Vereinigten Staaten von Amerika ihre Neutralität aufgeben sollten. Der Regierung von Mexiko wurde in diesem Falle Unterstützung in Aussicht gestellt für die Rückgewinnung des 1848 an die Vereinigten Staaten verlorengegangenen Territoriums. Im Vertrag von Guadalupe Hidalgo hatte Mexiko über 40 Prozent seines Territoriums (Kalifornien, Nevada, Arizona, Neu-Mexiko, Utah sowie Teile von Colorado und Wyoming) an die USA abtreten müssen.

Das Telegramm wurde vom britischen Marinegeheimdienst abgefangen und entziffert.[28]

> *„Wir beabsichtigen, am ersten Februar uneingeschränkten U-Boot-Krieg zu beginnen. Es wird versucht werden, Amerika trotzdem neutral zu halten. Für den Fall, dass dies nicht gelingen sollte, schlagen wir Mexiko auf folgender Grundlage Bündnis vor. Gemeinsame Kriegführung. Gemeinsamer Friedensschluss. Reichlich finanzielle Unterstützung und Einverständnis unsererseits, dass Mexiko in Texas, Neu Mexico, Arizona früher verlorenes Gebiet zurückerobert. Regelung im einzelnen Euer Hochwohlgeborenen überlassen. Euer Hochwohlgeborenen wollen Vorstehendes Präsidenten streng geheim eröffnen, sobald Kriegsausbruch mit Vereinigten Staaten feststeht, und Anregung hinzufügen, Japan von sich aus zu sofortigem Beitritt einzuladen und gleichzeitig zwischen uns und Japan zu vermitteln. Bitte Präsidenten darauf hinweisen, dass rücksichtslose Anwendung unserer U-Boote jetzt Aussicht bietet, England in wenigen Monaten zum Frieden zu zwingen. Empfang bestätigen. Zimmermann“*

[28] https://de.wikipedia.org/wiki/Zimmermann-Depesche.

5.1 Hintergründe zur Entzifferung[29]

Um Botschaften zu verschlüsseln, verwendete Deutschland zu Beginn des Ersten Weltkriegs sogenannte Codebücher. Man kann sich darunter grosse Lexika vorstellen, in denen bestimmten Begriffen entsprechende Zahlen zugeordnet waren. So wurde etwa dem Begriff „Bodenstück“ die Zahl „53431“ zugewiesen, dem Begriff „Bodenventil“ die Zahl „53432“ oder dem Begriff „Bohrer“ die Zahl „53442“, vieles folgte dann entsprechend in alphabetischer Folge.

Am 25. August 1914, knapp einen Monat nach Ausbruch des Ersten Weltkrieges, kam es zu einem entscheidenden Zwischenfall: Deutschland hatte Russland den Krieg erklärt und war mit mehreren Kreuzern und Torpedobooten vor dem Eingang zum Finnischen Meerbusen in Stellung gegangen. Der deutsche Kreuzer Magdeburg lief bei der estnischen Insel Osmussaar auf Grund. Die Ursache wurde nie restlos geklärt. In einem solchen Fall sollten sämtliche Geheimsachen (Codebücher) vernichtet werden. In der Hektik des Geschehens wurden jedoch zwei Signalbücher übersehen und nicht vernichtet.

Russische Taucher fanden die beiden intakten Signalbücher und kurze Zeit später konnten die russischen Dechiffrierspezialisten bereits die ersten Funksprüche der deutschen Seite entziffern. Die kaiserliche Marine war ahnungslos und ging davon aus, dass alle Codebücher vernichtet worden waren.

Im Oktober 1914 erhielt der britische Marineminister Winston Churchill durch russische Offiziere eines der beiden Exemplare überreicht. Es gelang den englischen Kryptologen unter Zuhilfenahme weiterer erbeuteter Materialien, die geheimen Nachrichten ohne Wissen der deutschen Seite zu entziffern.

Als die Zimmermann - Depesche übermittelt wurde war den Fachleuten des Deutschen Kaiserreichs nicht bewusst, dass die Briten über wichtiges Wissen verfügten, das die Entzifferung ihres Codes ermöglichte. Es wurde sogar darauf verzichtet, eine „doppelte“ Verschlüsselung durchzuführen. Dies führte dazu, dass die britischen Codebreakers die Botschaft bereits am 17. Januar 1917 teilweise entziffern konnten. Am 5. Februar 1917 leiteten die Briten - das noch nicht vollständig – entzifferte Telegramm an die Amerikaner weiter, um so US-Präsident Wilson zum Kriegseintritt zu bewegen.

"All the News That's Fit to Print."

The New York Times.

THE WEATHER

NEW YORK, THURSDAY, MARCH 1, 1917.—TWENTY-TWO PAGES.

GERMANY SEEKS AN ALLIANCE AGAINST US; ASKS JAPAN AND MEXICO TO JOIN HER; FULL TEXT OF HER PROPOSAL MADE PUBLIC

CONGRESS TO BACK WILSON

Laconia Tragedy Adds Strength to President's Support.

MODIFIED BILL IN HOUSE

But Leaders Predict That Senate's Armed Neutrality Measure Will Prevail.

THINK PUBLIC IS AROUSED

WILSON GIVES OUT APPEAL FROM HOY

American Whose Mother and Sister Died on the Laconia Asks That They Be Avenged.

OFFERS SERVICES TO NATION

Zimmermann Says Again Neutral Ships Will Be Sunk; Escape of the Orleans Only an Instance of Luck

JAPAN CALLS IT MONSTROUS

Embassy Issues Statement Scouting Germany's Proposal.

RELATIONS WITH US CLOSER

Text of Germany's Proposal to Form an Alliance With Mexico and Japan Against the United States

FILIBUSTER FOR EXTRA SESSION

PACIFISTS PRESS VIEWS ON WILSON

WASHINGTON EXPOSES PLOT

Our Government Has Zimmermann's Note of Jan. 19.

BIG PROMISES TO MEXICO

BERNSTORFF CHIEF AGENT

BERLIN TO REPLACE GERMANY HOLDS

Abbildung 12: Die New York Times veröffentlicht das Zimmermann Telegramm

Am Morgen des 1. März 1917 erschien in der New York Times ein Artikel, der den Text des deutschen Vorschlags an Mexiko – inzwischen vollständig dechiffriert – in voller Länge ausbreitete. Es beeinflusste den Lauf der Geschichte massgeblich, indem es (unter anderem) die USA am 6. April 1917 veranlasste, Deutschland den Krieg zu erklären. Was wäre passiert, wenn das Telegramm besser verschlüsselt gewesen wäre? Hätten die Amerikaner nicht eingegriffen? Wie hätte das den Ausgang des Ersten Weltkrieges beeinflusst? Einmal mehr zeigt sich, wie wichtig die Verschlüsselung einer Botschaft ist, wenn sie sogar den Ausgang von Weltkriegen beeinflussen kann.

[29] https://de.wikipedia.org/wiki/Zimmermann-Depesche

6 Die Enigma[30]

6.1 Die Entstehungsgeschichte der Enigma

Arthur Scherbius war ein deutscher Erfinder und Unternehmer. Er studierte Elektrotechnik und machte sich 1905 selbstständig. Eines seiner Lieblingsvorhaben war es, die unzulänglichen Chiffriersysteme aus dem Ersten Weltkrieg durch neue zu ersetzen. Bleistift und Papier sollten der Vergangenheit angehören, das neue System sollte die technischen Möglichkeiten des 20. Jahrhunderts nutzen. Scherbius entwickelte eine Chiffriermaschine, die er Enigma (griechisch: Rätsel) nannte. Sie sollte die gefürchtetste Chiffriermaschine der Geschichte werden.

Abbildung 13: Die «gefürchtetste» Chiffriermaschine der Geschichte: Die Enigma[31]

30 Singh, Simon, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 2000 sowie http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 29ff.

31 https://de.wikipedia.org/wiki/Datei:Enigma(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg.

Die Enigma besteht aus sechs Hauptkomponenten:

- Einem Tastaturfeld (keyboard), ähnlich wie bei einer Schreibmaschine
- einem Lampenfeld (lampboard), welches den Ausgabebuchstaben signalisiert
- einem Walzensatz
- einem Reflektor
- einem Steckbrett (plugboard) sowie
- einer Batterie.

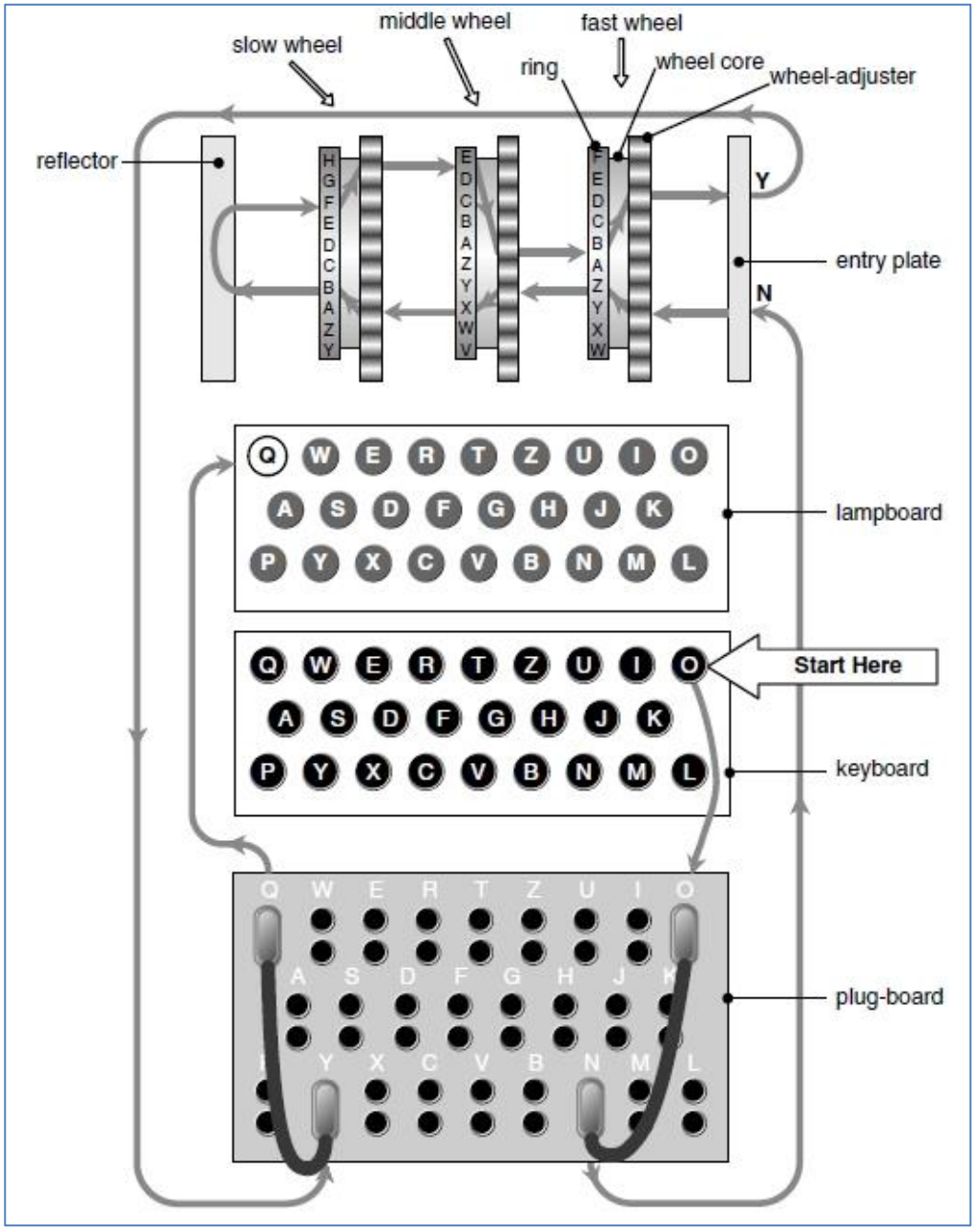


Abbildung 14: Aufbau der Enigma[32]

Das Steckbrett enthält 26 Buchsen, die mit einem Buchstaben beschriftet sind. Wird auf der Tastatur ein Buchstabe gedrückt, so wird durch die Batterie eine elektrische Spannung auf die Leiterbahn des gedrückten Buchstabens gelegt. Diese Leiterbahn führt im obigen Beispiel zum Buchstaben «O» der auf

[32] http://www.cryptool-online.org/index.php?option=com_content&view=article&id=87&Itemid=316&lang=de.

dem Steckerbrett mit einem anderen Buchstaben verbunden ist («N»). Danach läuft der Strom zu den Walzen.

Die Walzen sind willkürlich verdrahtet und je nach Stellung der Walzen resultieren daraus andere Buchstaben. Vom Reflektor aus läuft der Strom noch einmal über alle Walzen zurück. Wenn, wie in Abb. 14 zu sehen, die Spannung am Ende auf der Leiterbahn von «Y» liegt, leuchtet das Lämpchen für den Buchstaben «Y» auf. Dieser Buchstabe ist auf dem Steckbrett mit dem Buchstaben «Q» verbunden, so dass schlussendlich aus dem Input «O» der Output «Q» resultiert.

Die Walzen bilden den wichtigsten Teil der Maschine. Von der Tastatur ausgehend, führen die Drähte an sechs Punkten in die Walze hinein, in deren Innern sie kreuz und quer verlaufen, bis sie schliesslich an einem der sechs Punkten auf der anderen Seite austreten. Die Verdrahtung im Innern der Walze bestimmt, wie die Klarbuchstaben verschlüsselt werden.

Um mit der Enigma eine Nachricht zu dechiffrieren, muss also bekannt sein, welche Walze an welcher Stelle eingesetzt wurde und deren jeweilige Ringposition, welche die innere Verdrahtung einer Walze zu dem Übertrag auf die nächste Walze bildet. Außerdem muss man wissen, welche Steckverbindungen auf dem Steckbrett zu tätigen sind. Da sich bei jedem Tastendruck die Walzen, ähnlich wie bei einem mechanischen Kilometerzähler, weiterdrehen, ändert sich das geheime Schlüsselalphabet nach jedem Buchstaben, d.h. jeder Buchstabe wird auf eine andere Art und Weise verschlüsselt, so könnte aus «OTTO» der chiffrierte Text «PQWS» entstehen, es handelt sich also um eine polyalphabetische Substitution.[33]

6.2 Die Entschlüsselung der Enigma[34]

Der Bletchley Park (Name eines Landsitzes in der englischen Stadt Bletchley, ca. 70 km nordwestlich von London) war ab 1939 zuständig für die Entschlüsselung von Geheimnachrichten. Ursprünglich stand dort nur ein altes viktorianisches Herrenhaus aus dem 19. Jahrhundert. Der Park wurde aber bald durch zahlreiche Baracken erweitert, welche die verschiedenen Dechiffrierabteilungen beherbergten. Die Mitarbeiterzahl wuchs rasch von 200 auf 7000.

Abbildung 15: Alain Turing

Bevor die Kryptoanalytiker komplexe Entschlüsselungsverfahren einsetzten, versuchten sie ihr Glück mit sogenannten «cillies». Darunter versteht man einfache Tastenkombinationen, die man häufig einsetzte wie z.B. QWE oder BNM (auf der Tastatur nebeneinanderliebende Buchstaben. «Sillies» (dt. «Dummchen») sind vergleichbar mit einfachen Passwörtern wie «1234» oder «Passwort»).

Damit konnte man gewisse Meldungen dechiffrieren, aber diese zufälligen Treffer boten keinen wirklichen Schlüssel, um den deutschen Code systematisch zu knacken. Erst als Alan Turing auftauchte, kam der grosse Durchbruch.

Turing arbeitete in Bletchley Park in einem Team, das sich mit der Entschlüsselung der Enigma-Chiffriermaschine beschäftigte. Eine grosse Hilfe waren dabei die Ergebnisse des polnischen Mathematikers Marian Rejewski. Die Polen hatten eine Maschine gebaut, die ihnen beim Lösen der Enigma-Funksprüche half: die «Bomba» (angeblich soll Rejewski beim Verspeisen einer Eisbombe auf die Lösung des Problems gekommen sein, deshalb der Name: «Bomba». Da die entworfene Maschine tickte wie eine Bombe, haben die Polen die Maschine «Bomba» benannt – so eine andere Erklärung). Als die Deutschen die Anzahl der Rotoren von drei auf fünf erhöhten, waren sie nicht mehr in der Lage, die Nachrichten zu

[33] https://de.wikipedia.org/wiki/Enigma_(Maschine)

[34] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 34ff, sowie Singh, Simon, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 2000.

dechiffrieren. Turing erhielt nun die Aufgabe, eine neue Maschine zu konstruieren, welche die Entschlüsseln der Enigma-Funksprüche ermöglichen sollte. In Anlehnung an die polnische «Bomba», nannte Turing die Maschine: «Bombe».

Bei der Entschlüsselung half eine Schwachstelle der Enigma, die Turing aufgefallen war: Ein Buchstabe wurde bei der Verschlüsselung mit der Enigma nie in sich selber übergeführt. Der Buchstabe „a“ konnte nie als „A“ verschlüsselt werden, „b“ nie als „B“ usw. Dieses Wissen wurde mit einer zweiten Methode kombiniert: Dem Erraten von einzelnen Wörtern. Im Funkverkehr gab es oft wiederholende Meldungen, zum Beispiel der tägliche Wetterbericht um 6 Uhr morgens. Wurde ein Funkspruch um diese Zeit abgefangen, so konnte man annehmen, dass dieser das Wort „Wetter“ enthielt“ oder das Ende einer Nachricht wurde häufig mit „Heil Hitler“ signiert.

Dank solcher Anhaltspunkte (= Crib = Spickzettel - damit bezeichnet man eine Klartextphrase, von der der Codeknacker vermutet, dass sie in einem Geheimtext in verschlüsselter Form auftritt), konnte man die Anzahl der möglichen Kombinationen stark vermindern. Mit Hilfe einer Maschine, welche mögliche Kombinationen überprüfte, konnte man innerhalb weniger Stunden den aktuellen Tagescode knacken. Bereits im April 1940 wurde das erste Gerät in Betrieb genommen und danach laufend verbessert.[35]

Abbildung 16: General Guderian wartet auf die Entschlüsselung eines Funkspruchs (1940) (https://de.wikipedia.org/wiki/Enigma_(Maschine)

1941 waren fünfzehn Bomben im Einsatz, welche die Walzenstellungen prüften und Schlüssel enthüllten. Wenn alles optimal lief, dann fand die Bombe den korrekten Schlüssel innerhalb einer Stunde. Am Ende des Krieges waren rund 200 Bomben im Einsatz.

Aber damit war das Dechiffrierproblem keineswegs definitiv gelösten, denn die Enigma wurde während des Krieges laufend verändert, es gab verschiedene Varianten der Maschinen und die Protokolle für die Benutzung wurden ebenfalls verfeinert.

Dabei erwies sich der Marine Code als besonders schwierig zu knacken. Gerade dieser Code war aber von höchster Wichtigkeit, da die starke U-Boot Flotte der Deutschen noch mehr alliierte Schiffe zerstört und die Nachschublinien unterbrochen hätten.

Turing und seine Kollegen stellten fest, dass dieser Code ohne zusätzliche Informationen nicht zu knacken war: Sie brauchten deshalb die Informationen der Code-Bücher. Es gelang der britischen Navy mit Glück und Kühnheit, diese zu erbeuten.

Als die Deutschen Anfang 1942 einen zusätzlichen vierten Rotor einführten, konnten man die Funksprüche erneut nicht mehr lesen. Doch auch dieser Code wurde geknackt.[36]

Die Erfolge der Codebrecher von Bletchly Park blieben auch nach dem Krieg geheim. Grossbritannien wollte den erarbeiteten Wissensvorsprung weiterhin nutzen und beharrte deshalb auf grösster Geheimhaltung. So erfuhr Alan Turing nie eine öffentliche Würdigung seiner Leistung, im Gegenteil. 1952 wurde er wegen seiner Homosexualität verurteilt. Er musste einen Psychiater aufsuchen und eine Hormonbehandlung über sich ergehen lassen. Daraufhin bekam er schwere Depressionen und nahm sich am 7. Juni 1954 mit Zyanid das Leben.

[35] Mehr Information zur Entschlüsselung hier: https://de.wikipedia.org/wiki/Enigma_(Maschine)#Entzifferung.
[36] http://www.nzz.ch/wissen/wissenschaft/krieg-der-rechner-1.17256437.

7 One-Time Pad

Die Schwäche der Vignère-Verschlüsselung war ihre Wiederholung. Bei einem Schlüsselwort von der Länge 3 wiederholt sich das Geheimtextalphabet nach jedem 3. Schritt und ist somit dechiffrierbar. Wenn nun aber die Schlüssellänge gleich lang ist wie der Geheimtext, so entfallen die Wiederholungen und es kann keine Häufigkeitsanalyse mehr durchgeführt werden.

Das Problem besteht darin, einen passenden Schlüssel zu finden. Man könnte ein bekanntes Lied oder die erste Seite eines Buches benutzen, dabei gibt es aber folgendes Problem: Werden nämlich willkürlich an bestimmte Stellen des Geheimtextes Trigramme gesetzt (z.B. die), so kann man bei der Entschlüsselung dieser Trigramme auf bestimmte gebräuchliche Silben stossen (z.B. Ent). Probiert man diese Methode noch mit weiteren Bi- und Trigrammen aus, so können sich weitere Silben zeigen. Stösst man jetzt durch ein anderes Trigramm auf ”eck”, so kann das Schlüsselwort beispielsweise ”Entdecken” heissen.

Ein Schlüsselwort, welches die gleiche Länge des Textes besitzt, bietet also noch keine ausreichende Sicherheit. Die Schwäche besteht in der Sinnhaftigkeit des Schlüsselwortes. Aus diesem Grund wurde das Konzept eines Zufallsschlüssels eingeführt. Anstelle eines sinnvollen Textes wurde eine zufällige und sinnlose Folge von Buchstaben gewäht. Sender und Empfänger verfügten über je ein Blatt mit der gleichen Buchstabenfolge. Nach dem einmaligen Gebrauch dieses Schlüssels wurde das Blatt vernichtet und das nächste genommen, daher auch der Name «One-Time-Pad».

Das One-Time-Pad ist auch heute noch ein gutes Verfahren, das Problem besteht aber in der Schwierigkeit der Anwendung. So müsste man ständig eine riesige Anzahl von Schlüsseln bei sich haben, was sich bei einem grossen Funkverkehr als sehr mühsam erweist. Auch die ständige Generierung von Zufallsschlüsseln ist nicht einfach. Wie sollten sie gebildet werden ohne in bestimmte Muster zu verfallen?[37]

Grundlegende Voraussetzungen für die Sicherheit des Einmalschlüssel-Verfahrens sind: Der Einmalschlüssel muss

- mindestens so lang sein wie die Nachricht,
- gleichverteilt zufällig gewählt werden,
- geheim bleiben und
- darf nicht wiederverwendet werden, auch nicht teilweise.

7.1 Das One-Time Pad in der Geschichte

Wegen des hohen Aufwandes, wurde das One-Time Pad nur in seltenen, sehr wichtigen Fällen eingesetzt:

- Im 2. Weltkrieg übermittelten die britischen Enigma-Entschlüssler mit ihm dechiffrierte deutsche Geheimnachrichten an den Premierminister.
- Im und nach dem 2. Weltkrieg hat der sowjetische Geheimdienst KGB Nachrichten mit Spionen in den USA per One-Time-Pad ausgetauscht, diese Mitteilungen existieren heute noch und sind bis in alle Ewigkeit geschützt, solange die damals verwendeten One Time Pads nicht zur Verfügung stehen
- Nach der Kuba Krise von 1962 beschlossen die Sowjetunion und die USA einen «heissen Draht» einzurichten. Diese Verbindung (auch als das „Rote Telefon“ bekannt), wurde durch ein Einmalschlüssel-Verfahren geschützt.[38]

[37] http://www.wi.hs-wismar.de/~cleve/vorl/projects/krypto/ss04/Gruhn-Geschichte.pdf, S. 28f.
[38] https://de.wikipedia.org/wiki/Hei%C3%9Fer_Draht.

Abbildung 17: Testlauf des Fernschreibers am amerikanischen Ende, August 1963[39]

- Auch Che Guevara nutzte das One-Time-Pad Verfahren, um mit Fidel Castro zu kommunizieren und noch heute senden einige Regierungen OTP-verschlüsselte Botschaften in Form gesprochener Zahlen direkt an Spione im Ausland.

7.1.1 Wann wurde der heiße Draht genutzt?

Der Fernschreiber kann aber nur selten zwischen Washington und Moskau zum Einsatz. Im Sechs-Tage-Krieg 1967 und in den weiteren Nahostkrisen (1970 und 1973) wurde der heisse Draht genutzt.

Regelmäßig wird nur das Testsignal gesendet. Es lautet: «The quick brown fox jumps over the lazy dog», auf Deutsch: Der schnelle braune Fuchs springt über den faulen Hund. Welche Botschaft verbirgt sich hinter dem Satz? Keine – der Satz enthält aber alle Buchstaben, die der Fernschreiber darstellen kann. So kann man sichergehen, dass alles korrekt abläuft.

Es gibt solche direkten Verbindungen nicht nur zwischen Washington und Moskau sondern auch zwischen anderen Regierungen der Welt, so auch zwischen Washington und Peking.[40]

[39] http://www.nzz.ch/international/das-historische-bild/heisser-draht-zwischen-moskau-und-washington-1.18102448.
[40] http://www.wasistwas.de/archiv-geschichte-details/das-rote-telefon-der-direkte-draht-von-moskau-nach-washington.html.

8 Kryptographie heute – wie sicher sind die heutigen Verschlüsselungen?

Abbildung 18: Wie sicher sind unsere verschlüsselten Daten heute? Die NSA-Affäre hat diese Diskussion neu lanciert[41]

[41] http://www.dudelol.com/security-vs-liberty

9 Zeitleiste: Geschichte der Kryptologie[42]

Die Kryptologie spielt im Verlauf der Zeit keine unbedeutende Rolle. So verschleierte die Kryptographie verbotene Lieben, raffinierte Schlachtpläne und noch vieles mehr. Wann genau die Kryptographie erfunden, bzw. das erste Mal angewendet wurde weiss niemand. Durch bestimmte Funde kann man aber Rückschlüsse ziehen. Hier soll deshalb eine kleine Zeittafel mit Stationen der Kryptographie und Kryptoanalyse quer durch die Geschichte aufgezeichnet werden.

Ca. 1900 v. Chr.

Ca. 1900 vor Chr. verwendeten ägyptische Schriftgelehrte bei den Inschriften eines königlichen Grabes spezielle Hieroglyphen, dies ist die erste schriftlich dokumentierte Kryptographie. Ob vor den alten Ägyptern schon andere Völker Kryptographie angewandt haben, ist bisweilen noch nicht bekannt.

600-500 v. Chr.

In dieser Zeit benutzten hebräische Gelehrte einfache Zeichenaustauschalgorithmen. Einer dieser Zeichenaustauschalgorithmen ist beispielsweise die Atbash-Verschlüsselung, die um 600 v. Chr. in Palästina angewendet wurde.

400 v. Chr.

Die Griechen verschlüsselten 400 v. Chr. ihre Nachrichten mit der sogenannten Skytala (Holzstab). So wurde z.B. dem griechischen General Lysander von Sparta eine verschlüsselte Botschaft von einem Diener überbracht, die lesbar wurde, als er die Nachricht über die Skytala wickelte.

4 Jahrhundert v. Chr.

Im Kamasutra wird Frauen empfohlen 64 Künste zu studieren um eine „perfekte Ehefrau“ zu sein. Darunter ist neben Künsten wie Kochen, Bekleidung, Massage, Schach oder Teppichweberei auch die Kunst der Geheimschrift dabei. Gelernt werden soll die Kunst der Geheimschrift um Affären geheimzuhalten. Um aus einen Klartext einen Geheimtext zu machen, wird die Substitution, sprich das Ersetzen jedes Buchstaben durch einen anderen, vorgeschlagen.

170 v. Chr.

Der antike griechische Geschichtsschreiber Polybius entwickelt die *Polybius-Tafel*. Mit der Polybius-Tafel können Buchstaben in numerische Zeichen umgewandelt werden.

50 - 60 v. Chr.

Die heute immer noch gut bekannte Caesar-Chiffre findet das erste Mal vom großen römischen Feldherrn Gaius Julius Caesar Verwendung. Wie auch schon bei Atbasch handelte es sich bei der Cäsar Chiffre um eine monoalphabetische Substitution. Man verschob einen Buchstaben des Alphabets dabei um einen bestimmten Abstand. Caesar selbst verwendete dabei häufig den Schlüssel C, also eine Verschiebung des Alphabets um drei Buchstaben. Auch der römische Kaiser Augustus soll die Caesar Verschlüsselung genutzt haben, er nahm aber wahrscheinlich wegen des Namens, jeweils nur eine Verschiebung um einen Buchstaben, also dem Schlüssel A vor.

Ab 750 n. Chr.

Im “Goldenen Zeitalter” der islamischen Kultur findet eine rege Verwendung der Kryptographie statt. Neben der Verwendung der Kryptographie, erfanden die Araber zu dieser Zeit die Kryptoanalyse um sicher gehen zu können, dass ihre eingesetzte kryptographische Verfahren sicher sind.

Während die arabische Kultur zu dieser Zeit, unter kryptographischen Gesichtspunkten, Höchstleistung erbrachten, fand man in Europa während des Mittelalters genau das Gegenteil davon vor. Lediglich Mönche in den Klostern trieben das Studium der Geheimschriften voran, während sie nach verborgenen Bedeutungen in der Bibel forschten. So enthielt beispielsweise das Alte Testament absichtsvoll leicht durchschauende kryptographische Elemente. So wurde in Jeremia 25,26 und 51,41 das Wort Babel durch das Wort Scheschach ersetzt. Verschlüsselt wurde das Wort mit der Atbasch Verschlüsselung:

Zwar geht man davon aus, das Altbasch und andere „einfachen“ Geheimschriften, „der Bibel nur eine geheimnisvolle Aura verleihen“ und nicht Wörter verbergen sollte, dennoch reichte dies um das Interesse an der Kryptographie zu erwecken. Schon bald begann man damit sich intensiver mit der Kryptographie auseinander zu setzen.

13 Jahrhundert n. Chr.

Der englischer Franziskaner-Mönch, Philosoph und Mathematiker Roger Bacon schrieb das erste bekannte europäische Werk zur Kryptographie unter dem Namen: Die Abhandlung über die geheime Künste und die Nichtigkeit der Magie. Darin beschreibt er mehrere Verfahren zur Geheimhaltung von Botschaften.”

[42] http://www.kryptowissen.de/geschichte-der-kryptographie.html

15 Jahrhundert n. Chr.
Blütezeit der europäischen Kryptografie. Höfe legten sich eigene kryptographische Dienste zu.

1500 n. Chr.
Mußmatlich um das Jahr 1500 entstand das Voynich-Manuskript. Es ist in einer unbekannten Schrift verfasst, von der man ausgeht, dass es sich nicht um eine natürliche Sprache handelt. Obwohl man davon ausgeht, dass eine Verschlüsselung vorliegt, konnte diese bis heute nicht gelöst werden. Neuste Forschungen gehen von einer bedeutungslosen Buchstabenfolge aus.

1506 n. Chr.
Giovanni Soro wird zum Geheimsekretär Venedigs ernannt und gilt als erster großer Kryptoanalytiker. Dank seines Rufes bekommt er aus ganz Italien abgefangene Botschaften zum Entschlüsseln zugeschickt, auch von Papst Clements VII im Jahr 1526.

20. September 1586 n. Chr.
Hinrichtung der Babington-Verschwörer. Vorangegangen waren unter anderem verschlüsselte Nachrichten zwischen den Verschwörern und Maria Stuart.

Ende 16. Jahrhundert
Frankreich beginnt seine führende Rolle in der Kryptanalyse zu festigen

17. Jahrhundert
Ära der Schwarzen Kammern, also Orte an denen verschlüsselten Nachrichten abgefangen und kopiert wurden, um sie anschließend an die zuständigen Kryptoanalytiker weiterzuleiten.

1795 n. Chr.
Thomas Jefferson erfindet mit der Jefferson disk/wheel cypher den ersten Chiffrierzylinder. Das Gerät wurde nicht wirklich bekannt, sodass es ein Jahrhundert noch einmal von Kommandant Etienne Bazeries erfunden wurde. Eingesetzt wurde der Bazeries Cylinder in der US-Armee von 1923 bis 1942.

1854 n. Chr.
Charles Babbage gelingt es als Erstem die Entschlüsselung einer Vigenère-Chiffre.

1883 n. Chr.
Die Abhandlung "La Cryptographie militaire" von Auguste Kerckhoffs von Nieuwendhoff erscheint.

1917 n. Chr.
Entwicklung des "One-time-Pad" durch den Amerikaner Gilbert S. Vernam. Die Umsetzung folgte von Joseph O. Mauborgne, der auch der Namensgeber war.

1918 n. Chr.
Der deutsche Elektroingenieur Arthur Scherbius erfindet die erste Enigma.

1940 n. Chr.
Alan Turing knackt nach Vorarbeiten von Marian Rejewski mit seiner Idee der "Bomben" die Enigma.

1967 n. Chr.
David Kahn veröffentlicht mit "The Codebreakers - The Story of Secret Writing" ein Buch, das bald als das (englischsprachige) Standardwerk zur Geschichte der Kryptographie galt.

1976 n. Chr.
Diffie und Hellman veröffentlichen ihren Aufsatz New Directions in Cryptography. Darin beschrieben sie den mittlerweile nach ihnen benannten Diffie-Hellman-Schlüsselaustausch.

1977 n. Chr.
Veröffentlichung des asymmetrischen kryptographischen Verfahren RSA, dessen Bezeichnung sich aus den Anfangsbuchstaben der Familennamen der drei Entwickler Rivest, Shamir und Adleman ableitet.

1991n. Chr.
Phil Zimmermann veröffentlicht die erste Version seines Programms zur Verschlüsselung unter dem Namen Pretty Good Privacy, bzw. kurz PGP.