Geschichte der Kryptografie und Steganografie

Miriam Amélie Peer

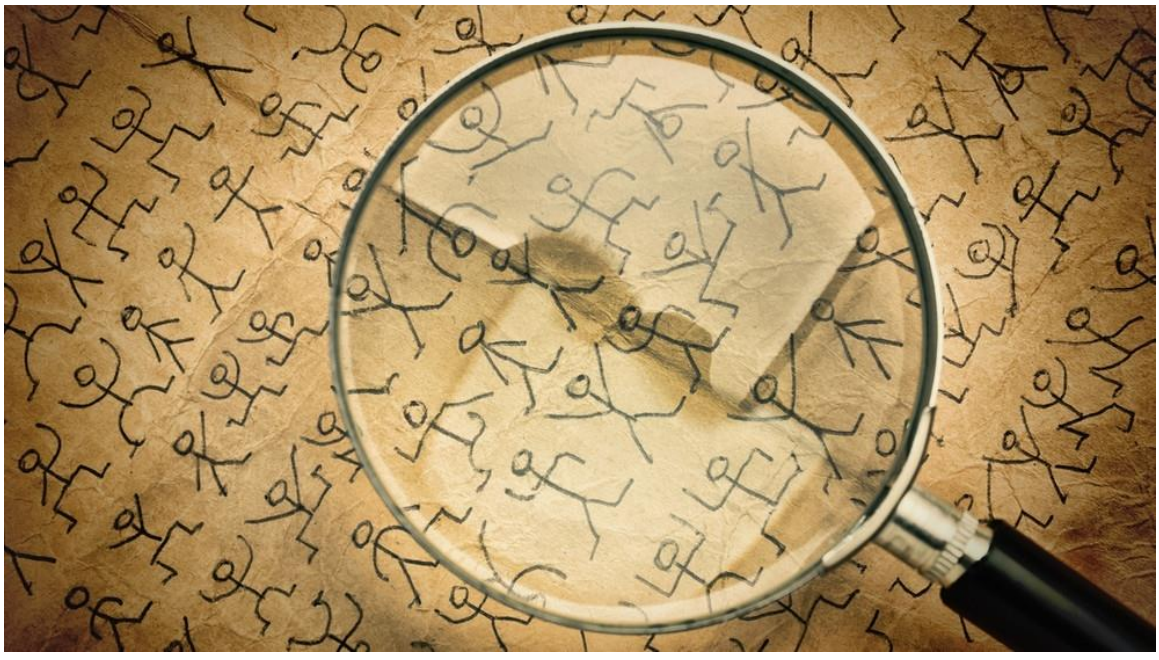
Klasse 3C

Mittelschule Lana

Schuljahr 2020/21

Tutorin: Prof. Königsrainer Ulrike

Geschichte der Kryptografie und Steganografie



Introduzione

Ho scelto il tema crittografia e steganografia, perché ho partecipato a un calendario d'avvento online, dove risolvevo ogni giorno un enigma. Alla fine ho addirittura vinto un gioco interessante come premio. Gli enigmi mi piacciono molto, ho deciso di scrivere la mia tesi su questo tema. Mi concentrerò soprattutto sulla storia della crittografia e i metodi di crittografare del passato, perché per la crittografia moderna si usa solo il computer. Durante le mie ricerche ho scoperto che la crittografia viene usata dappertutto. All'inizio soprattutto nelle guerre, dopo, grazie all'industrializzazione e lo sviluppo tecnico, anche nella vita privata e nell'economia. I greci e romani antichi hanno crittografato le loro lettere. Più tardi viene codificato il telegramma o il messaggio radio. Nella Seconda Guerra mondiale invece si usavano già macchine per crittografare. Oggi tutti i computer usano la crittografia, per garantire la privacy. Anche la carta di credito, le app sul cellulare, le chiavi della macchina, il telecomando per aprire il garage, il codice QR del corona pass o bambini piccoli che vogliono scrivere un messaggio segreto usano la crittografia.

Generale

La crittografia e la steganografia sono metodi per crittografare e nascondere messaggi. Quando gli uomini hanno imparato a scrivere, era subito importante crittografare i messaggi, per essere sicuro, che nessuno riesca a leggerli. Soprattutto durante la guerra la crittografia era molto importante, per evitare che il nemico leggesse tutti i messaggi. Erodoto, che visse circa nel 500 avanti Cristo, era uno dei primi che ha scritto a proposito di queste tecniche.

Oggi, in alcuni paesi, è vietato usare la crittografia, soprattutto nei paesi non democratici, perché il governo ha paura di una rivoluzione. Esempi sono la Bielorussia, la Cina, l'Iran, la Mongolia, il Kazakistan, il Pakistan, la Tunisia o il Vietnam. Da noi è legale usare la crittografia, anche se qualche volta si discute, perché può anche essere usata in ambito criminale.

Nel mondo del cinema si trova il tema crittografia in forma di filmati avvincenti. Per esempio "Breaking the Code", "Enigma" e "The Imitation Game".

Un tema attuale è la criptomoneta come per esempio Bitcoin. È un sistema di denaro completamente virtuale e digitale, creato nel 2009 da un gruppo anonimo. In differenza alla moneta normale nessuno può controllare il valore e la quantità. Nel momento la criptomoneta è un tema per esperti. Ma si diffonde sempre di più. Una cosa da non dimenticare è che serve tanta energia per calcolare tutto. La criptomoneta usa più del doppio dell'energia annuale dell'Austria.

https://www.altroconsumo.it/-/media/altroconsumo/images/home/soldi/conti%20correnti/news/bitcoin_shu_549334807_1600x900.jpg?rev=d27dc01d-79b2-4b7c-8296-3ce4bb05948a&hash=326A87204BE033D73209B3A49954BDC3

Erklärungen

Was ist Kryptografie

Bei der Kryptografie werden die Nachrichten verschlüsselt. Das heißt, dass mit einem bestimmten Verfahren der Text so verändert wird, dass man ihn nicht lesen kann, ohne dass man das Verfahren und den Schlüssel kennt. Das Wort Kryptografie kommt aus dem griechischen Wort kryptos, welches so viel wie verborgen heißt.

Sollte man jedoch von der Kryptoanalyse reden, ist damit das Entschlüsseln eines Textes gemeint. Außerdem gibt es auch noch das Wort Kryptologie, welches sehr oft als Überbegriff für Kryptografie und Kryptoanalyse verwendet wird. In diesem Wort steckt auch das griechische Wort logos, welches für Wort, Sinn oder Gedanke steht.

Sollte man die Merkmale einer Sprache untersuchen wollen, ist man in der Kryptolingustik tätig.

Manche Menschen verwenden den Begriff Code als Überbegriff für alle kryptografischen Verfahren. Die Codierung ist aber nur eine Verschlüsselung auf der Ebene der Wörter. Die Chiffrierung hingegen ist die Verschlüsselung auf Ebene der Buchstaben. Decodierung und Dechiffrierung sind die Entschlüsselungsvorgänge.

Wie wird verschlüsselt

Um einen Text zu verschlüsseln, braucht man einen Schlüssel, ein Verschlüsselungsverfahren und den Text, den man verschlüsseln will. Der Empfänger muss außerdem wissen, welches Verfahren gewählt und welcher Schlüssel verwendet wurde. Mit dem Verfahren wird der Klartext, welcher in der Kryptografie immer in Kleinbuchstaben geschrieben wird, in den Geheimtext, welcher immer in Großbuchstaben geschrieben wird, umgewandelt. Wenn ein Gegner die Nachricht abfangen sollte, ist es möglich, dass er weiß, welches Verfahren gewählt wurde. Trotzdem kann er die Nachricht nicht entschlüsseln, solange er den Schlüssel nicht kennt. “Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen: Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.” * Diesen Satz sagte einmal Kerckhoffs, ein niederländischer Linguist. Wenn bei einem Verschlüsselungsverfahren viele Schlüssel möglich sind, ist es ein sehr sicheres Verfahren. Sollten aber nur wenige Schlüssel zur Verfügung stehen, ist das Verfahren nicht so sicher, da ein Gegner die Nachricht schneller entschlüsseln kann.

*(Quelle: Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

Der Unterschied zwischen Transposition und Substitution

Bei der Transposition werden die Buchstaben einer Nachricht einfach in eine andere Reihenfolge gebracht. Diese Methode wird, je länger der Text, immer sicherer.

BIETASOIINEDNIBCSAEENRAHIHENAHNIENEEEHNOGGBAHDEEEHDWRJLNEDRETMESCEE
EDRRNPSTOWREDEUHTBNIENCRCTIFCIENADRRIEFLEERCTISMTOEIDEÄGRETXIMRIHRR

(Das ist ein Beispiel für die Transposition. Dieser Teil wurde mit der Gartenzaunverschlüsselung verschlüsselt.)

Bei der Substitution hingegen werden die Buchstaben durch andere Buchstaben oder Zeichen ersetzt. Sogar Julius Caesar verwendete solche Verschlüsselungen.

DGK FGT UWDUVKVWVKQP JKPIGIGP YGTFGP FKG DWEJUVCDGP FWTEJ CPFGTGDWEJUVCDGP QFGT BGKEJGP GTUGVBV. UQICT LWN KWU ECGUCT XGTYGPFGVG UQNEJG XGTUEJNWGUUGNWPIGP.

Schlüssel: 2

(Das ist ein Beispiel für die Substitution. Dieser Teil wurde mit der Caesar-Verschlüsselung verschlüsselt)

Die Substitution kann man nochmals unterteilen in die monoalphabetische und die polyalaphabetische Substitution. Bei der monoalphabetischen Substitution wird mit einem Geheimtextalphabet gearbeitet, bei der polyalphabetischen Substitution hingegen mit mehreren.

Was ist Steganografie?

Bei der Steganografie werden Nachrichten versteckt. Das Wort kommt aus dem griechischen Wort “steganos”, was übersetzt so viel wie bedeckt heißt und aus dem Wort “graphein”, welches für Schreiben steht. Die Steganografie ist sehr sicher, nur sollte der Bote kontrolliert werden, können die Gegner die Nachricht ohne weitere Hindernisse lesen und verstehen. Deshalb entwickelte sich zur gleichen Zeit die Kryptografie. War ein höchstes Maß an Sicherheit gewünscht, kombinierte man die Steganografie mit der Kryptografie. Das heißt, dass man einen verschlüsselten Text auch noch versteckte. So konnten die Gegner die Nachricht nicht verstehen, wenn der Bote durchsucht und die Botschaft entdeckt wurde.

Geschichte

Schlacht bei Salamis. Im alten Griechenland, 480 v. Chr., gab es eine Schlacht. Diese Schlacht wurde vor allem durch Kryptografie entschieden. Die Perser wollten einen Überraschungsangriff auf Griechenland starten. Das bekam ein

Grieche, der aus seiner Heimat verbannt worden war und im Reich der Perser leben musste, mit und entschied sich, die Griechen vorzuwarnen. Er wusste, dass er die Nachricht verstecken muss, um sicher zu gehen, dass sie ankommt. Der Grieche wusste aber nicht, wie er das anstellen solle. Er kam auf eine Idee. Er schabte das Wachs von einer Schreibtafel und schrieb die Nachricht darunter auf das Holz. Danach erhitzte er das Wachs, um es wieder darüber zu gießen. So konnte er seine Warnung an die Griechen senden ohne dass die persischen Wachen die Nachricht entdecken konnten. Jetzt gab es noch ein Problem. Die Nachricht kam in Griechenland an, nur wusste keiner, was man mit einer nicht beschriebenen Schreibtafel machen sollte. Etwas später kam man auf die Idee, das Wachs abzuschaben. So konnten sich die Griechen vorbereiten und gewannen die Schlacht bei Salamis.

https://media1.faz.net/ppmedia/aktuell/feuilleton/forschung-und-lehre/216195482/1.3554739/default-retina/seeschlacht-von-salamis.jpg

Mittelalter. In sehr vielen Verwaltungshandbüchern der Araber konnte man schon im Mittelalter einen extra Abschnitt mit Kryptografie finden. Außerdem waren die Araber die Ersten, die es schafften, Verschlüsselungen zu knacken. Mit der Kryptoanalyse konnte man sehr einfach und leicht monoalphabetische Substitutionen entschlüsseln. Den Anfang machten Theologen, die die Offenbarungen des Korans in die richtige Reihenfolge bringen wollten. Dafür zählten sie, wie oft welches Wort in den Texten vorkommt. An der Häufigkeit der Wörter konnte man das ungefähre Alter der Schriften ermitteln. Wörter kommen mal mehr in Mode und verschwinden dann langsam wieder aus unserem Sprachgebrauch. Später haben die Araber die Buchstaben gezählt und sie entdeckten, dass verschiedene Buchstaben verschieden oft in Texten vorkommen. Dies führte zum Durchbruch der Kryptoanalyse. Die erste Erklärung dieses Verfahrens fand man in einem Buch von Abū Yūsūf Ya’qūb ibn Is-hāq ibn as-Sabbāh ibn ‘omrān ibn Ismaīl al-Kindī:

> *Eine Möglichkeit, eine verschlüsselte Botschaft zu entziffern, vorausgesetzt, wir kennen ihre Sprache, besteht darin, einen anderen Klartext in derselben Sprache zu finden, der lang genug ist, um ein oder zwei Blätter zu*

füllen, und dann zu zählen, wie oft jeder Buchstabe vorkommt. Wir nennen den häufigsten Buchstaben den ersten den zweithäufigsten den zweiten und den folgenden den dritten und so weiter, bis wir alle Buchstaben in der Klartextprobe durchgezählt haben.

Dann betrachten wir den Geheimtext, den wir entschlüsseln wollen, und ordnen auch seine Symbole. Wir finden das häufigste Symbol und geben ihm die Gestalt des ersten Buchstaben der Klartextprobe, das zweithäufigste Symbol wird zum zweiten Buchstaben, das dritthäufigste Symbol zum dritten Buchstaben und so weiter, bis wir alle Symbole des Kryptogramms, das wir entschlüsseln wollen, auf diese Weise zugeordnet haben.

(Quelle: Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

Am Anfang zählt man jedes Zeichen und schreibt auf, wie oft es vorkommt. Nun muss man wissen, in welcher Sprache der Geheimtext geschrieben wurde. Jetzt sucht man das häufigste Symbol und schreibt stattdessen ein E, weil der Buchstabe E in der deutschen Sprache der häufigste ist. Auf der Tabelle kann man sehen, wie oft jeder Buchstabe vorkommt. Außerdem kreist man alle Wörter ein, die drei Buchstaben haben. Jetzt kann man das zweithäufigste Symbol suchen und es durch ein N ersetzen. Sollte man inzwischen einige Buchstaben aus den eingekreisten Wörtern aus dem Zusammenhang erkennen, kann man diese auch schon ersetzen. Man kann die Buchstaben nämlich nicht alle so einsetzen, wie sie in der Tabelle stehen, da ihre Häufigkeit von Text zu Text leicht schwanken kann. Deshalb rentiert es sich erst die Häufigkeitsanalyse anzuwenden, wenn man einen Text mit mehr als 100 Buchstaben hat. Wenn man weniger Buchstaben hat, wird die Häufigkeitsanalyse zu leicht getäuscht. (Informationen: Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

1	E	17,4 %
2	N	9,78%
3	I	7,55%
4	S	7.27%
5	R	7%
6	A	6,51%
7	T	6,15%
8	D	5,08%
9	H	4,76%
10	U	4,35%
11	L	3,44%
12	C	3,06%
13	G	3,01%
14	M	2.53%
15	O	2,51%
16	B, W	1,89%
18	F	1,66%
19	K	1,21%
20	Z	1,13%
21	P	0,79%
22	V	0,67%
23	J	0,27%
24	Y	0,04%
25	X	0,03%
26	Q	0,02%

Gleichzeitig steckte Europa noch im Mittelalter. Es gab nur wenige Orte, an denen die Kryptografie gefordert wurde. Mönche in den Klöstern versuchten versteckte Nachrichten in der Bibel zu finden. Es wurden tatsächlich Teile im Alten Testament mit einer sehr leichten Methode verschlüsselt. Dies wurde nur gemacht, um die Bibel geheimnisvoller wirken zu lassen. Trotzdem entstand das Interesse an ernsthafter Kryptografie. Deshalb knackten die Mönche alte Geheimschriften und entwickelten neue. So kam die Kryptografie wieder in die westliche Kultur.

Im 13. Jahrhundert wurde das erste Werk über die Kryptografie von einem Mönch geschrieben. Etwa 100 Jahre später hat es die Kryptografie wieder geschafft an Bedeutung zu gewinnen.

Sehr wichtig wurde die Kryptografie in Italien. Damals bestand Italien noch aus vielen kleinen Stadtstaaten, welche versuchten, sich gegenseitig auszuschalten. Diese Stadtstaaten schickten Botschaften an ihre Gesandten im Ausland, mit Anweisungen, wie die Außenpolitik zu führen ist. Diese schickten Nachrichten mit allen Informationen, die sie erhalten haben, zurück. Solche Nachrichten mussten verschlüsselt werden, damit kein anderes Herrscherhaus die Nachrichten mitlesen kann. Es dauerte nicht lange, dann hatten die Botschafter der Stadtstaaten schon einen eigenen Geheimsekretär.

Inzwischen erforschte man auch im Westen die Kryptoanalyse, da man wissen wollte, was der Gegner weiß und macht. Die Wissenschaft ist sich nicht sicher, ob die Häufigkeitsanalyse aus Arabien eingeführt oder sie unabhängig davon in Europa entwickelt wurde. Der erste Kryptoanalytiker in Europa war Giovanni Soro, welcher 1506 zum Geheimsekretär von Venedig ernannt wurde. Etwa zur gleichen Zeit kam die spanische Regierung drauf, dass ganz Europa ihren Nachrichtenverkehr lesen konnte. Sie hatten zu schwache Verfahren gewählt. Dieses Problem bekamen zu dieser Zeit fast alle Länder in Europa. Die Verschlüsselungsverfahren sind zu schwach und die Kryptoanalyse zu stark.

Monoalphabetische Substitutionen konnte man ohne Probleme mit der Häufigkeitsanalyse entschlüsseln. Trotzdem wurde an dieser Art der Verschlüsselung festgehalten. Kryptographen wollten stärkere Methoden entwickeln. Sie sollten aber trotzdem einfach und schnell angewendet werden können. Die Kryptografen fingen an, Füller in die Geheimtexte einzufügen. Das waren Zeichen, die zur Verwirrung eingesetzt wurden. Der Empfänger wusste, welche Symbole nur als Füller standen und konnte so den Text ohne Probleme lesen, die Füller konnten die Häufigkeitsanalyse aber durcheinanderbringen. Andere Kryptografen schrieben die Wörter extra falsch, auch so konnte man die Häufigkeitsanalyse täuschen, den Text aber trotzdem noch lesen.

Eine andere Art der Verschlüsselung war das Codebuch. Dabei ersetzte man alle Wörter durch Symbole. Anfangs dachte man, dass man so eine größere Sicherheit hat. Dabei hat ein Codebuch auch viele Nachteile. Man braucht ein Verzeichnis aller Wörter. Ein solches Buch hat etwa die Dicke eines Wörterbuchs. Außerdem kann ein Codebuch dem Gegner in die Hände fallen. In diesem Fall müsste man ein völlig neues erstellen. Das Erstellen eines Codebuchs ist schwierig und dauert lange. Danach muss dieses Buch über einen sicheren Weg an alle im Nachrichtennetz beteiligten Personen geschickt werden. Auch das konnte lange dauern, wenn es in der ganzen Welt verteilt werden musste.

Wenn man jedoch mit Chiffren arbeitet, ist es kein so großes Problem, wenn der Gegner das Geheimtextalphabet in die Hände bekommt, da man sehr leicht ein neues entwickeln kann. Außerdem kann man es sich leicht einprägen und verteilen. Aufgrund der zu leicht zu entschlüsselnden monoalphabetischen Substitution und der zu aufwändigen Codes wurde der Nomenklator entwickelt. Dieses Verschlüsselungssystem wurde auch von Maria Stuart verwendet. Dabei ersetzte man häufige Wörter durch Symbole. Der Rest wird mit der monoalphabetischen Substitution verschlüsselt. Man kam aber schon bald drauf, dass diese Art der Verschlüsselung nicht viel sicherer ist, da man den größten Teil mit der Häufigkeitsanalyse entschlüsseln kann. Der Rest erschließt sich aus dem Zusammenhang. Die besten Kryptoanalytiker schafften es, alle Hürden bei der monoalphabetischen Substitution zu bewältigen und so die Geschichte in Europa zu beeinflussen und viele Geheimnisse aufzudecken.

The story of Maria Stuart. Maria Stuart was a Scottish Queen, born on 8th December 1542. Maria and her aunt second grade, Elisabeth I., were fighting for the Throne of England. Maria was held captive by Elisabeth I., the Queen of England. After 18 years detention, in March 1586, Maria got a pack of letters. To be able to bring her these letters, they were hidden in a beer barrel. This technique is part of the steganography. The letters were sent by her follower, Anthony Babington and other people and were delivered by Gifford. They planned the assassination of Elisabeth I. and the liberation of Maria Stuart and asked for approval of their plans. Babington used the nomenclator technique for encryption. Every letter had its sign. Often used words, phrases and double letters also had their signs to deceive the frequency analysis. The nomenclator is a substitution. Maria and the conspirators were sure, that no one could decrypt the letters. Also Gifford was very persuasive. But in reality, Gifford, was a double agent. He brought all letters to Walsingham, Elisabeth's Head of Agents. The letters were copied, so that Thomas Phelippes had enough time to decrypt them. He was a linguist and one of the best cryptanalysts of this time. Phelippes could decrypt the letters very quickly, because he was an expert of frequency analysis. He discovered the correct signs for the letters. The signs for words and phrases he deducted from the meaning of the text. The letters described the whole plan for the assassination of Elisabeth I. Phelippes informed his chief Walsingham, who waited and falsified later even the Maria's handwriting to find all other conspirators. Maria and her followers were not aware of this. All of them were arrested and Maria was executed on the 18th of February 1587 at 10 o'clock in the great hall of castle Fotheringhay. This example shows that bad encryptions can be deadly.

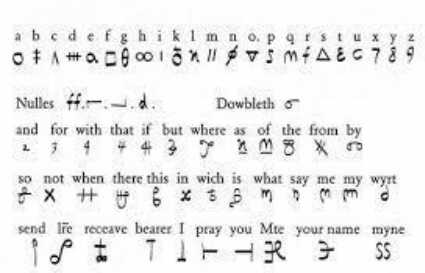


Bild: Maria Stuart's nomenclator. https://www.swisseduc.ch/geschichte/kryptographie/docs/script_kryptographie_swisseduc.pdf

Polyalaphabetische Verschlüsselung. Aufgrund der Entwicklung der Kryptoanalyse mussten die Kryptografen eine neue Verschlüsselungsmethode entwickeln. Die ersten Ideen stammen von Battista Alberti, der 1404 geboren wurde. Viele Jahre später entwickelten drei andere Kryptografen sein Werk weiter. Als erster Johannes Trithemius, der 1492 geboren wurde, dann Giovanni Porta, geboren 1535 und als letzter Blaise de Vigenère, welcher 1523 geboren wurde. Vigenère versuchte, aus den Notizen von Alberti, Trithemius und Porta ein mächtiges Verschlüsselungssystem zu schaffen. Nach langer Arbeit war er erfolgreich. Um ihn zu ehren, wurde das System nach ihm benannt, die Vigenère-Verschlüsselung. Bei diesem Verfahren verwendet man 26 Geheimtextalphabete, zwischen denen man hin und her wechselt. Aufgrund dieser Tatsache kann man die Vigenère-Verschlüsselung nicht mit der Häufigkeitsanalyse knacken. Außerdem hat man eine enorm große Anzahl von möglichen Schlüsseln. Um mit der Vigenère-Verschlüsselung zu arbeiten, braucht man ein Vigenère-Quadrat (siehe unten) und ein Schlüsselwort oder Schlüsselsatz. Nun schreibt man über jeden Buchstaben des Klartextes einen Buchstaben des Schlüsselworts. Wenn das Schlüsselwort fertig ist, fängt man wieder von vorne an. Um jetzt zu verschlüsseln, sucht man den ersten Buchstaben des Schlüsselworts in der ersten Spalte und den ersten Buchstaben des Klartextes in der ersten Zeile. Der Buchstabe, der am Schnittpunkt dieser beiden steht, ist der Geheimtextbuchstabe. So fährt man mit der ganzen Nachricht fort.

Bild: Blaise de Vigenère: https://www.howold.co/uploads/photo/300x300/63/blaise-de-vigenere.jpg

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Geheimtext: N L W _ P X W K R B _ T W M _ L G Y B O Y _ !

Klartext: d a s _ w e t t e r _ i s t _ s c h o e n _ !

Schlüssel: klettern

(Das ist ein Beispiel für die Vigenère-Verschlüsselung)

Die Homophone Verschlüsselung. Wenn es um einen wichtigen Nachrichtenaustausch ging, musste besser verschlüsselt werden. Zusätzlich brauchte man auch eine schnelle Verschlüsselung. Kryptoanalytiker entwickelten deshalb die homophone Verschlüsselung. Der Name homophon kommt aus dem Griechischen. Homos steht für gleich und phone steht für Klang. Bei dieser Verschlüsselung werden jedem Buchstaben mehrere Symbole zugeordnet. Die Anzahl hängt von der Häufigkeit des Buchstabens ab. Das Ziel dieser Verschlüsselung war, dass jeder Buchstabe eine ungefähre Häufigkeit von einem Prozent hat. Man konnte aber, wenn man die Eigenschaften der Buchstaben kennt, die Verschlüsselung trotzdem knacken.

Die homophone Verschlüsselung ist nur eine weiter entwickelte Form der monoalphabetischen Substitution, da, einmal das Geheimtextalphabet festgelegt, sich nichts mehr ändert.

11,2,22 _ 38,9,34,6,21 _ 13,42,10,51,1,31 _ 7,59,35,20,56,54 _ 24,55,66,39

i,c,h _ h,e,i,s,s,e _ m,i,r,i,a,m _ a,m,e,l,i,e _ p,e,e,r

(Hier wurde die Homophone Verschlüsselung verwendet)

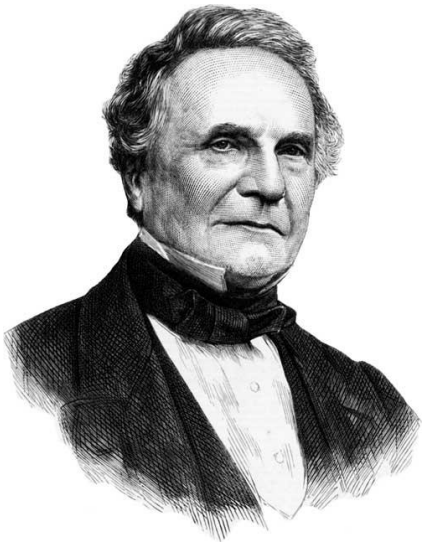
Die Schwarzen Kammern. Im 17. Jahrhundert war die Kryptoanalyse ein ausgewachsenes Gewerbe und jede große Macht in Europa hatte ihre eigenen schwarzen Kammern. In diesen Kammern wurden Botschaften entschlüsselt und Informationen zusammengetragen. Die dort gesammelten Informationen wurden in die ganze Welt verkauft. Ein Beispiel zum Tagesablauf in einer schwarzen Kammer ist die Kabinettskanzlei in Wien. Über diese Kanzlei wurden alle Nachrichten an die Wiener Botschaft umgeleitet. Um sieben Uhr morgens trafen die Briefe ein. Sekretäre schmolzen die Siegel und öffneten die Briefe. Eine Gruppe von Stenografen schrieb die Briefe ab. Dann wurden sie wieder versiegelt und drei Stunden später waren sie schon bei ihren eigentlichen Adressen angekommen. Danach begann die Arbeit der Kryptoanalytiker. Sie nahmen die Kopien der Briefe und entschlüsselten sie. Die meisten monoalphabetischen Substitutionen waren kein Problem und konnten sehr schnell entschlüsselt werden. Deshalb wurden die Kryptografen indirekt dazu gezwungen, die polyalphabetische Substitution zu benutzen. Langsam fingen die Geheimsekretäre an, die polyalphabetische Verschlüsselung einzusetzen.

Telegrafie. Im Jahr 1753 wurden die ersten Ideen der Telegrafie umgesetzt und 1851 wurde das europäische Morsealphabet erfunden. Schon bald wurden die Menschen auf ein Problem aufmerksam, welches auch 1853 in einem Artikel in der englischen Zeitung Quarterly Review beschrieben wurde.

> *Auch sollten Maßnahmen ergriffen werden, um einen schwerwiegenden Einwand zu entkräften, der gegenwärtig im Blick auf die telegrafische Versendung privater Botschaften erhoben wird: der Bruch jeglicher Geheimhaltung. Denn in jedem Fall müssen ein halbes Dutzend Personen jedes Wort erfahren, das eine Person an die andere richtet. Die Beamten der Englischen Telegrafengesellschaft werden auf Geheimhaltung eingeschworen, doch schreiben wir oft Dinge, bei denen es unerträglich wäre, wenn wir sehen würden, dass Fremde es vor unseren Augen lesen. Dies ist ein bedauerlicher Mangel der Telegrafie, und er muss durch das eine oder andere Mittel behoben werden.*
>
> (Quelle: Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

Deshalb wurden die Botschaften verschlüsselt, bevor man sie zu Telegrafen brachte. Die Vigenère-Verschlüsselung war die beste Methode, den Nachrichtenverkehr geheim zu halten. Man meinte, dass man die Vigenère-Verschlüsselung nicht brechen kann.

Die Entschlüsselung der Vigenère-Verschlüsselung. Charles Babbage wurde 1791 in London geboren. Bekannt ist das Genie für den ersten Entwurf des modernen Computers. Als Charles Babbage es schaffte, die Vigenère-Verschlüsselung zu brechen, zählte man dies zum größten Durchbruch der Kryptoanalyse nach der Entdeckung der Häufigkeitsanalyse.



Die meisten Kryptoanalytiker hatten bereits aufgegeben, die Vigenère-Verschlüsselung je zu knacken. Babbage packte aber der Ehrgeiz, es selbst mal zu versuchen. Deshalb suchte er nach einem Schwachpunkt der Vigenère-Verschlüsselung, welchen er auch fand. Als erstes suchte Babbage nach Buchstabenfolgen, die öfters geschrieben wurden, denn dann ist es wahrscheinlich, dass es sich um die gleichen Wörter handelt, die mit den gleichen Buchstaben verschlüsselt wurden. Jetzt zählte Babbage den Abstand zwischen den Buchstabenfolgen. So konnte er, wenn er noch andere gleiche Wörter fand, herausfinden, wie lange das Schlüsselwort war. Jetzt wusste Babbage, welche Buchstaben mit dem gleichen Geheimtextalphabet verschlüsselt wurden. So konnte er eine Häufigkeitsanalyse mit allen Buchstaben durchführen, die mit dem ersten Buchstaben des Schlüsselworts verschlüsselt wurde. Jetzt musste Babbage wissen, welcher Buchstabe der erste des Schlüsselworts war. Dafür zeichnete er ein Säulendiagramm und untersuchte das Häufigkeitsgebirge. Er wusste, dass im Englischen die Buchstaben R, S, und T ziemlich häufig sind und nebeneinander liegen. Im Alphabet folgen danach viele seltene Buchstaben. Das heißt, dass es einen Berg aus drei Säulen geben muss und danach ein breites Tal kommt. Mit solchen Hinweisen konnte Babbage herausfinden, welches der erste Buchstabe des Schlüsselworts war. So konnte Babbage die Vigenère-Verschlüsselung dechiffrieren. Man weiß nicht genau, wann ihm dieser Durchbruch gelungen war, da er seinen Erfolg geheim hielt. Man geht aber davon aus, dass er es im Jahr 1854 geschafft hat.

Bild: Charles Babbage https://science4fun.info/wp-content/uploads/2020/03/Charles-Babbage.jpg

Die Kryptografie der Öffentlichkeit. Die breite Masse an Menschen fing an, sich immer mehr für Kryptografie zu interessieren. Mit der Erfindung des Telegrafen wurde das Interesse auch in der Wirtschaft entfacht. Man ließ Telegramme verschlüsseln, auch wenn sie somit teurer wurden, da ein Telegrafist länger braucht, eine wilde Kombination von Buchstaben zu verschicken. Dabei wurden nur einfache Verschlüsselungsverfahren genutzt, weil diese ausreichten, um eine Nachricht vor neugierigen Menschen zu schützen.

Auch junge Liebespaare verwendeten die Kryptografie, um Nachrichten auszutauschen. Oft durften sie sich nämlich nicht treffen und die Eltern durften nichts von dieser Beziehung mitbekommen. So kamen einige auf die Idee, Nachrichten verschlüsselt an Zeitungen zu schicken und sich so auszutauschen. Viele Kryptoanalytiker machten sich einen Spaß daraus, diese Nachrichten in den Zeitungen zu entschlüsseln und selbst Nachrichten mit der gleichen Verschlüsselungsmethode und dem gleichen Schlüssel an die Zeitung zu schicken.

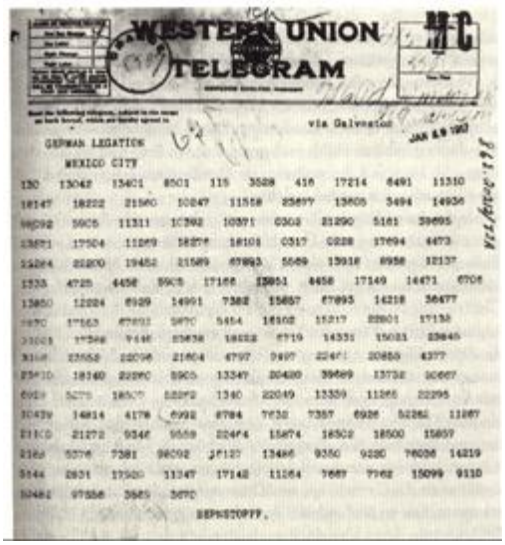
Der erste Weltkrieg. Die Kryptografie war Ende des 19. Jahrhunderts auf der Suche nach einem neuen, sichereren Verfahren. Außerdem begann Guglielmo Marconi, geboren am 25. April 1874, mit elektrischen Stromkreisen zu forschen. Später erfand er den Funk. Der Vorteil dieser Technik war, dass man Nachrichten über die ganze Welt schicken konnte, ohne ein Kabel legen zu müssen. Mit dieser Erfindung wurde die Verschlüsselung jedoch noch viel wichtiger, weil jeder diese Nachrichten empfangen konnte und demnach auch probieren konnte, sie zu entschlüsseln. Sollte das Militär den Funk im Krieg verwenden, musste man sich seiner Verschlüsselung absolut sicher sein. Die Suche nach einem neuen Verschlüsselungsverfahren wurde mit dem Ausbruch des ersten Weltkriegs immer wichtiger, trotzdem schafften die Kryptografen den entscheidenden Durchbruch nicht. Es gab nur massenhaft Fehlversuche.

Ein Beispiel ist die ADFGVX-Verschlüsselung. Diese Verschlüsselung wurde vom deutschen Heer als sicherstes Verschlüsselungssystem ausgewählt, da es eine Mischung aus Substitution und Transposition ist. Als Mitte 1918 das deutsche Militär nur noch 100 Kilometer von Paris entfernt war, war die letzte Chance der Alliierten, die ADFGVX-Verschlüsselung zu knacken. Dies gelang dem Kryptoanalytiker Georges Painvin auch und die Deutschen verloren den Überraschungseffekt. Durch die Entschlüsselung der Nachrichten erfuhr man, wo sich die deutschen Truppen aufhalten und konnte eigene zur Verstärkung schicken. Eine Woche später konnte man die Deutschen in einer fünf Tage langen Schlacht zurückdrängen.

Im ersten Weltkrieg wurden viele solche Verschlüsselungen erfunden, doch dauerte es nie lange, bis es die Kryptoanalytiker schafften, die Verschlüsselungen zu knacken. Die Franzosen analysierten sogar bei Funksprüchen die Handschrift der Funker. Da die Nachrichten mit dem Morse-Code verschickt wurden, beobachtete man die Schnelligkeit, die Pausen und die Länge der Striche und Punkte. Außerdem verwendeten die Franzosen Peilstationen. Mit diesen konnte man den ungefähren Standort des Funkers ausfindig machen. Diese Methode war sehr wichtig, wenn die Geheimschlüssel gerade verändert wurden und die Kryptoanalytiker den Schlüssel erst wieder neu ermitteln mussten. Die Deutschen waren in Sachen Kryptografie sehr unerfahren. Sie starteten den Krieg ohne Kryptoanalytiker und richteten erst 1916 einen Abhorchdienst ein. Als die Deutschen am Anfang des Krieges in französische Gebiete eingedrungen sind, zerstörten die Franzosen ihre Telegrafenleitungen und zwangen somit die Deutschen zum Funkverkehr. Die Franzosen konnten somit alle Nachrichten der Deutschen abhören, verwendeten selbst aber noch ihre eigenen Telegrafenleitungen.

Die Briten fingen im Januar 1917 eine Nachricht ab, in der stand, dass die Deutschen einen uneingeschränkten U-Boot-Krieg gegen die Amerikaner beginnen wollten.

Wir beabsichtigen, am ersten Februar uneingeschränkten U-Boot-Krieg zu beginnen. Es wird versucht werden, Vereinigte Staaten trotzdem neutral zu halten. Für den Fall, dass dies nicht gelingen sollte, schlagen wir Mexiko auf folgender Grundlage Bündnis vor. Gemeinsam Krieg zu führen. Gemeinsam Friedensschluss. Reichlich finanzielle Unterstützung und Einverständnis unsererseits, dass Mexiko in Texas, New Mexiko, Arizona früher verlorenes Gebiet zurückerobert. Regelung im einzelnen Euer Hoheit überlassen.


WESTERN UNION
TELEGRAM
via Galveston
GERMAN LEGATION
MEXICO CITY

Sie wollen Vorbestehendes dem Präsidenten streng geheim eröffnen, sobald Kriegsausbruch mit Vereinigten Staaten feststeht, und Anregung hinzufügen, Japan von sich aus zu vermitteln. Bitte den Präsidenten darauf hinweisen, dass rücksichtslose Anwendung unserer U-Boote jetzt Aussicht bietet, England in wenigen Monaten zum Frieden zu zwingen. Empfang bestätigen.

Zimmermann.

(Quelle: Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

Dies war das Telegramm, welches die Deutschen zu ihrer Botschaft in Mexiko geschickt haben. Dieses Telegramm musste verschlüsselt sein, da bekannt war, dass die Alliierten alle Nachrichten abhörten, da sie die direkte Telegrafenleitung von Deutschland nach Amerika am Anfang des Krieges zerstört hatten. So musste diese Nachricht über Schweden laufen und die Kabel lagen genau vor der Küste Englands. So konnten die Briten die Nachricht an ihren Dechiffrierdienst weiterleiten. Schon nach einigen Stunden waren kleine Teile des Textes entschlüsselt. Die zwei Kryptoanalytiker, Montgomery und Grey, gaben ihren teils entschlüsselten Text an den Chef der Marineaufklärung, Admiral Sir William Hall, weiter. Dieser legte den Text in seinen Tresor und gab den Kryptoanalytikern den Auftrag, ihn fertig zu entschlüsseln.

Bild: Zimmermann Telegramm https://upload.wikimedia.org/wikipedia/de/7/76/Zimmermann_Telegramm.png

Hall wollte den Text zwar den Amerikanern geben, hatte aber Angst, dass die Deutschen ihre Verschlüsselungssysteme dann verstärken würden. Deshalb musste eine andere Lösung her. Hall wollte sich die mexikanische Version dieses Telegramms beschaffen und in den Zeitungen veröffentlichen. Dann würden die Deutschen nämlich denken, dass die Amerikaner das Telegramm aus Mexiko gestohlen hatten. Hall schaffte dies und die amerikanische Bevölkerung erfuhr von den Absichten Deutschlands. Daraufhin trat Amerika am 2. April 1917 in den Krieg ein. So konnten sich die Alliierten einen Vorteil verschaffen und später den Krieg gewinnen.

Die unentschlüsselbare Chiffre. Im ersten Weltkrieg hatten die Kryptoanalytiker sehr viele Siege zu verzeichnen. Seit der Entschlüsselung der Vigenère-Verschlüsselung waren die Kryptoanalytiker wieder im Vorteil. Doch schafften die Amerikaner einen erneuten Durchbruch der Kryptografie. Sie entwickelten eine Verschlüsselung, welche auf der Vigenère-Verschlüsselung basiert, doch ist sie viel stärker als diese. Man musste nur ein Schlüsselwort nehmen, welches gleich lang wie der Text selbst ist. Dann funktioniert das Verfahren zu Entschlüsselung der Vigenère-Verschlüsselung nämlich nicht mehr. Man könnte denken, dass man jetzt einfach einen schon bestehenden Text nehmen könnte, doch dann ist das Verfahren zu unsicher und man kann es relativ schnell knacken, da der Schlüssel aus logisch zusammenhängenden Buchstaben besteht. Wenn man häufige Wörter nämlich an beliebige Stellen setzt und dann die Schlüsselbuchstaben ermittelt, kann man sehen, ob einer der Buchstaben richtig ist, wenn der Schlüssel einen Sinn ergibt. Deshalb kam man auf die Idee, eine willkürliche Buchstabenfolge zu verwenden. Das heißt, dass der Schlüssel keine sinnvolle Reihenfolge aufweisen darf. 1918 führte Joseph Mauborgne, welcher am 26. Februar 1881 geboren wurde, die Verschlüsselung mit dem Zufallsschlüssel ein. Diese Verschlüsselung ist nicht zu brechen, hat aber trotzdem einen Nachteil. Man braucht für jeden Verschlüsselungsvorgang einen neuen Schlüssel. Zufallsschlüssel sind sehr aufwändig zu generieren und man muss sie an alle Stellen im Kommunikationsnetz verteilen. Dieses Verschlüsselungssystem trägt den Namen one-time-pad. Das Verfahren wurde aufgrund seiner Nachteile aber kaum eingesetzt. Sollte man einen Schlüssel öfters verwenden, kann die verschlüsselte Nachricht entschlüsselt werden. Nur bei extrem wichtigen Nachrichten, wo es egal ist, wie viel sie kosten, wird das one-time-pad verwendet.

Enigma. Im 15. Jahrhundert erfand Leon Alberti die Chiffrierscheibe. Daraus entwickelte Artur Scherbius eine ausgeklügelte Maschine. Artur Scherbius wurde am 30. Oktober 1878 geboren und studierte Elektronik in Hannover und München. Anfangs wollte er nur eine elektrische Version der Chiffrierscheibe erschaffen. Später wurde sie jedoch zu einer der besten Verschlüsselungsmethoden der Welt.

Im Grunde besteht die Enigma aus drei Hauptteilen: Tastatur, Verschlüsselungseinheit und ein Lampenfeld. Über die Tastatur gab man, ähnlich wie auf einer Schreibmaschine, die Buchstaben in die Enigma ein. So schickte man einen Stromstoß los, welcher durch die Verschlüsselungseinheit fließt. Die Verschlüsselungseinheit besteht aus mehreren Gummiwalzen, welche Drähte in ihrer Mitte haben. Die Drähte gehen auf der einen Seite in die Walze hinein, wechseln dort ihre Position und gehen auf der anderen Seite an einer anderen Stelle wieder hinaus. Dort konnte der Stromstoß dann direkt seinen Weg durch die nächste Walze nehmen. Am Ende der letzten Walze geht ein Kabel zum entsprechenden Lämpchen mit dem Geheimtextbuchstaben, welches aufleuchtet.

Mit diesem Verfahren konnte man eine monoalphabetische Substitution machen. Man wollte jedoch ein stärkeres Verschlüsselungsverfahren haben. So entwickelte Scherbius seine Maschine weiter. Er kam auf die Idee, die Walze nach jedem Buchstaben automatisch eine Stelle weiterdrehen zu lassen.

Bild: Arthur Scherbius https://pantheon.world/images/profile/people/261520.jpg

So würde sich das Geheimtextalphabet nach jedem Buchstaben ändern und man könnte eine polyalphabetische Substitution erzeugen. Die Walze ist zwar gut für eine bessere Verschlüsselung, aber auch gleichzeitig der Schwachpunkt. Wenn die Walze nach einer Umdrehung wieder bei ihrem Startpunkt angelangt ist, kann man dieses System gleich wie die Vigenère-Verschlüsselung entschlüsseln.

So kam Scherbius auf die Idee, eine zweite Schlüsselwalze einzubauen. Wenn die erste Walze jetzt ihre erste Runde gemacht hat, dreht sich die zweite Walze mit. So hatte man aber nur eine begrenzte Zahl an Schlüsseln. Deshalb baute Scherbius noch eine dritte Walze ein, die die gleich Aufgabe wie die zweite hat, nur kommt sie erst zum Einsatz, wenn die zweite Walze eine komplette Umdrehung gemacht hat. Um nun auch noch mit der Enigma zu entschlüsseln, hat Scherbius einen Reflektor eingebaut. Der Reflektor ähnelt einer Walze, jedoch gehen seine Drähte auf der gleichen Seite rein und raus und der Reflektor rotiert nicht. Er dreht die Stromsignale um und schickt sie durch die Walzen wieder zurück, am Ende leuchtet dann das Lämpchen mit dem Buchstaben auf.

Wenn man mit dem Verschlüsseln beginnen möchte, muss man sich zuerst den Schlüssel ausdenken. Bei der Enigma ist der Schlüssel die Position der Walzen. Da man mit einem großen Funknetz arbeitet, werden in einem Schlüsselbuch alle Schlüssel aufgelistet. Diese werden im Funknetz verteilt. An einem Tag wird immer die gleiche Grundeinstellung verwendet. Erst jetzt kann man mit dem Verschlüsseln beginnen. Man tippt den ersten Klarbuchstaben in die Tastatur ein und schaut, welcher Geheimtextbuchstabe aufleuchtet. Diesen schreibt man dann auf einen Zettel, damit man ihn später übermitteln kann. Wenn der Empfänger die Nachricht erhalten hat, muss er seine Enigma auf die gleiche Grundeinstellung wie der Sender stellen. Nun kann er die Geheimtextbuchstaben in die Tastatur eingeben und die Klartextbuchstaben leuchten auf dem Leuchtfeld auf.

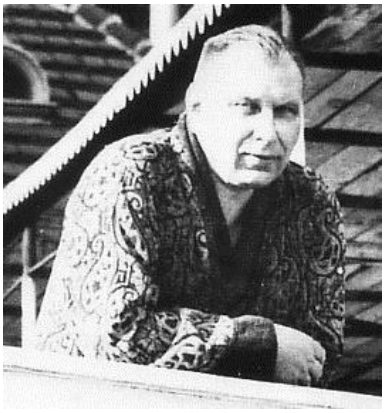
Sollte ein Gegner eine Nachricht in die Finger bekommen, müsste er alle möglichen 17.576 Schlüssel ausprobieren. Für einen einzigen Menschen wäre das unmöglich, sollten jedoch mehrere Menschen an dieser Aufgabe arbeiten, könnte man die ganzen Einstellungen an nur einem einzigen Tag prüfen. Um das Verfahren zu verstärken, musste man die Zahl der möglichen Schlüssel erhöhen. Zusätzliche Walzen würden die Enigma zu unhandlich machen. Dafür konnte man die Walzen herausnehmen und ihre Position ändern. Zusätzlich wurde das Steckbrett erfunden. Es befindet sich zwischen der Tastatur und der ersten Walze. Durch diesen Zusatz konnte man die Kabel der Buchstaben vertauschen, bevor das Signal in die erste Walze gelangt. Die Einstellung des Steckbrettes musste auch im Schlüsselbuch aufgezeichnet werden.

Eine Enigma, wie ich sie hier erklärt habe, hat ungefähr 10.000.000.000.000.000 (10 Billiarden) mögliche Schlüssel. 1918 meldete Scherbius sein erstes Patent der Enigma an. Durch den hohen Preis fand die Enigma aber weniger Anklang in der Gesellschaft als ursprünglich erhofft. Fast gleichzeitig erhielten drei andere Erfinder Patente für ähnliche Maschinen. So zum Beispiel Robert Koch, welcher 1919 ein Patent anmeldete, Arvid Damm oder Edward Hebern. Alle ihre Erfindungen brachten keinen Erfolg.

Scherbius war der Einzige, der Glück hatte. Das deutsche Militär fand zwei britische Dokumente, auf welchen stand, wie die Briten im Krieg die Nachrichten der Deutschen abhörten und entschlüsselten. Daraufhin bekam das deutsche Militär einen Schock und sie kauften die Enigma von Scherbius. 1925 begann die Serienanfertigung der Enigma und so kam Deutschland zu der besten Verschlüsselungsmethode der Welt. Man dachte, dass diese Chiffriermaschine Deutschland in einem zweiten Weltkrieg zum Sieg verhelfen würde, stattdessen sollte diese Maschine aber zum Ende von Hitler führen. Scherbius erlebte diesen Misserfolg nicht mehr. Er starb am 13. Mai 1929.

Bild: Enigma https://www.ansa.it/webimages/ch_620x438/2021/5/8/c4ec6a44ee119c6ed92af3c0f4e044f9.jpg

Die Enigma wurde entschlüsselt. Nachdem das deutsche Militär anfing, die Enigma zu verwenden, hatten die Briten, Franzosen und Amerikaner keine Chance mehr, die Nachrichten zu entschlüsseln. Den Alliierten war dies aber relativ egal. Sie hatten keine Angst mehr vor Deutschland, nachdem sie den ersten Weltkrieg gewonnen hatten. So waren aber nicht die Polen. Sie wollten, nachdem sie nun unabhängig waren, versuchen, ihr Land zu verteidigen, da die Nachbarstaaten versuchten, Gebiete von Polen zu besetzen. Die Polen überwachten den deutschen Funkverkehr so lange, bis sie 1926 auf Funkmeldungen stießen, die mit der Enigma verschlüsselt wurden. Man hatte zu dieser Zeit keine Chance, die Enigma zu entschlüsseln, da man dazu die innere Verdrahtung kennen musste.



Im deutschen Militär gab es einen Schwachpunkt, der es möglich machte, die Enigma zu entschlüsseln. Dieser Schwachpunkt war Hans-Thilo Schmidt, er wurde 1888 geboren. Er versuchte sich anfangs als Geschäftsmann, doch ging sein Plan nicht auf. Deshalb stand er hilflos mit seiner Familie da, im Gegensatz zu seinem älteren Bruder Rudolph, welcher beim deutschen Militär arbeitete. Irgendwann war Hans-Thilo gezwungen, seinen Bruder um Hilfe zu bitten. So bekam er Arbeit in der Berliner Chiffrierstelle. Dort verdiente er aber zu wenig Geld, um seine Familie zu unterhalten. Deshalb entschied er sich, geheime Informationen an andere Länder zu verkaufen. So konnte Hans-Thilo mehr Geld verdienen und gleichzeitig der Arbeitsstelle seines Bruders schaden, der den Einsatz der Enigma befürwortete. Im November 1931 traf sich Schmidt mit einem französischen Agenten und überreichte ihm Dokumente. Auf diesen Papieren standen alle nötigen Informationen, um eine Kopie der Enigma zu bauen. Mit einer Kopie konnte man noch lange nicht die Nachrichten entschlüsseln, da man den Tagesschlüssel herausfinden musste. Die Franzosen machten sich aber gar nicht die Mühe, eine Kopie anzufertigen, da sie davon ausgingen, dass man den Schlüssel nicht herausfinden kann. Doch wollten sich die Polen bei dieser Aufgabe probieren. So händigten die Franzosen den Polen die Unterlagen aus. Die Polen bekamen auch Informationen über die Schlüsselbücher. Jeden Monat gab es neue Schlüsselbücher und jeder Schlüssel wurde immer einen Tag lang verwendet.

Bild: Hans-Thilo Schmidt https://upload.wikimedia.org/wikipedia/en/c/c3/Hans_thilo_schmidt.jpg

Nun hatten die Polen einen Anhaltspunkt. Sie wussten, dass ein Schlüssel immer einen ganzen Tag lang verwendet wurde. Das heißt, dass mit dem gleichen Schlüssel mehrere hundert Nachrichten verschlüsselt wurden. Wenn ein Schlüssel öfters verwendet wurde, um Nachrichten zu verschlüsseln, können Kryptoanalytiker die Nachrichten schneller entschlüsseln, da man mehrere Seiten Text hat und nicht nur ein paar Sätze. Aufgrund dieses Schwachpunktes setzten die Deutschen Spruchschlüssel ein. Und genau bei diesen Spruchschlüsseln machten die Deutschen einen Fehler. Sie gaben vor, den Spruchschlüssel zwei Mal vor die Nachricht zu schreiben. Der Spruchschlüssel wurde mit dem Tagesschlüssel verschlüsselt und änderte sich bei jeder Nachricht. Wenn man den Tagesschlüssel also kannte, konnte man den Spruchschlüssel entschlüsseln, welcher dann die Informationen zur Walzenstellung für den Rest der Nachricht liefert.

Am Anfang denkt man, dass eine solche Nachricht unmöglich zu entschlüsseln ist. Doch die Polen hatten Angst und waren bereit, alles auszuprobieren. Sie kamen auf die Idee, Mathematiker als Kryptoanalytiker auszubilden. Eingesetzt wurden Mathematiker von der Universität Poznàn, da dort alle Studenten fließend Deutsch sprechen konnten. Darunter war auch Marian Rejewski, welcher ein besonderes Talent in diesem Bereich zeigte. Später kam er ins Biuro Szyfrów. Das heißt auf Deutsch übersetzt so viel wie Chiffrierbüro und es war das Büro des polnischen Geheimdienstes. Rejewski schaffte es, sehr viele Nachrichten zu entschlüsseln und so wurde ihm die unmögliche Aufgabe zugeteilt, die Enigma zu knacken.

Bild: Marian Rejewski https://bi.im-g.pl/im/8/2380/z2380508V,Marian-Rejewski.jpg

Anfangs analysierte er die Enigma genau, um herauszufinden wie sie funktionierte. Dabei entdeckte er, dass die Wiederholungen am Anfang jeder Nachricht der Schlüssel zum Erfolg sein könnten.

Rejewski bekam jeden Tag einen neuen Stapel abgehörter Nachrichten. Dabei schrieb er sich zum Entschlüsseln immer die Spruchschlüssel heraus und fertigte eine Tabelle an. Er wusste, dass beim Spruchschlüssel der erste und der vierte immer der gleiche Klartextbuchstabe war. Wenn Rejewski an einem Tag genug Nachrichten bekam, konnte er diese Tabelle vervollständigen. Um den Tagesschlüssel herauszufinden, fing Rejewski an, Muster zu suchen. Er fand sogenannte Ketten, die verschieden lang waren.

Erster Buchstabe	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
Vierter Buchstabe	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K
Kette	1	1	1	6	6	2	3	2	9	1	4	7	2	6	4	7	2	8	4	5	7	5	3	3	5	3

Ketten:

A-F-W-A	3 Verknüpfungen
B-Q-Z-K-V-E-L-R-I-B	9 Verknüpfungen
C-H-G-O-Y-D-P-C	7 Verknüpfungen
J-M-X-S-T-N-U-J	7 Verknüpfungen

(Informationen: Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

Auf dem Bild sieht man eine Tabelle, wie sie auch von Rejewski stammen könnte. Oben sind die Zeilen, in die die Buchstaben der Spruchschlüssel eingetragen worden sind. Unten sieht man die Ketten und die Anzahl der Verknüpfungen. Eine solche Tabelle wurde auch für den zweiten und fünften und den dritten und sechsten Buchstaben angelegt. Rejewski kam drauf, dass sich die Anzahl der Verknüpfungen jeden Tag änderte. Er wusste aber immer noch nicht, wie er aus diesen Ketten den Tagesschlüssel herauslesen sollte. Als Rejewski an diesem Punkt war, machte er eine sehr wichtige Bemerkung: Auf die Länge der Ketten hat das Steckbrett keinen Einfluss. Es ändern sich zwar ein paar Buchstaben, doch die Länge der Kette bleibt gleich. Jetzt hatte Rejewski nicht mehr 10 Billiarden mögliche Schlüssel, sondern nur noch 105.456. Nun konnte er sich mit einem viel einfacheren Rätsel befassen. Rejewski stellte Leute an, die alle Möglichkeiten durchprobierten und sie in einem Katalog notierten. Es brauchte ein ganzes Jahr, diesen Katalog zu erstellen. Erst dann konnte Rejewski mit der Entschlüsselung der Enigma beginnen.

Jeden Tag fertigte Rejewski eine Bezugstabelle an und suchte nach den Ketten. Dann schrieb er die Merkmale der Ketten der ersten und vierten, der zweiten und fünften und der dritten und sechsten Buchstaben auf. Diese Merkmale konnte er dann in seinem Katalog suchen. Zu allen Merkmalen passte nur eine Walzenstellung. Jetzt wusste Rejewski aber die Steckbrettverbindungen immer noch nicht. So kam er auf die Idee alle Kabel am Steckbrett zu entfernen und dann die Nachricht einzugeben. Größtenteils ergab das Ergebnis Unsinn, doch manchmal kamen Wortteile zum Vorschein, bei denen man erraten konnte, was sie eigentlich heißen sollten. So konnte Rejewski draufkommen welche Buchstaben mithilfe des Steckbrettes vertauscht wurden. Wenn er alle Steckbrettverbindungen herausgefunden hat, hatte er den ganzen Tagesschlüssel in der Hand und konnte alle Nachrichten von diesem Tag entschlüsseln und lesen. Manchmal veränderten die Deutschen ihre Systeme, doch Rejewski schaffte es immer wieder, sein Verfahren dementsprechend anzupassen. Rejewski entwickelte eine Maschine, die in zwei Stunden den Tagesschlüssel finden konnte.

Im Dezember 1938 wurde die Enigma verstärkt. Es wurden neue Walzen eingeführt und das Steckbrett erweitert. Es gab nun 159.000.000.000.000.000.000 (159 Trillionen) mögliche Schlüssel. Das Biuro Szyfrów müsste neue Maschinen bauen, welche aber viel zu teuer waren. Deshalb entschloss man sich, die Aufgabe den Franzosen und Briten zu übergeben. Am 24. Juli 1939 betraten Kryptoanalytiker aus Großbritannien und Frankreich das Biuro. Ihnen wurden die Entschlüsselungsmaschinen gezeigt und ein Nachbau der Enigma und die Baupläne für die Maschinen geschenkt. Am 1. September begann mit dem Überfall auf Polen der zweite Weltkrieg.

Auch die Engländer stellten nun Mathematiker und Naturwissenschaftler ein, darunter auch Frauen. Bis zu 7.000 arbeiteten im Entschlüsselungs-Hauptsitz Bletchley Park. Dort war auch die Government Code and Cypher School, welche es seit 1919 gibt. Sie schafften es, die polnischen Techniken zu erlernen, anzuwenden und zu perfektionieren. Jeden Tag machten sich die KryptoanalytikerInnen auf die Suche nach dem neuen Tagesschlüssel.

Am 10. Mai 1940 änderten die Deutschen ihr Protokoll. Der Schlüsselspruch wurde nicht mehr zwei Mal am Anfang jeder Meldung geschrieben, sondern nur noch ein Mal. Zum Glück erfand Alan Turing eine Maschine, die es erlaubte, auch ohne Wiederholung des Schlüsselspruchs den Tagesschlüssel herauszufinden. Diese Maschine wurde am 8. August fertiggestellt und die Briten konnten die Nachrichten wieder lesen. Die Entschlüsselung war nie Routine, da die KryptoanalytikerInnen immer wieder auf Hürden stießen.

Jeder einzelne Zweig des deutschen Militärs hatte seine eigene Enigma. Manche waren stärker verschlüsselt, andere schwächer. Nach einiger Zeit wussten die Briten, welche Enigmen zu knacken waren und welche nicht. Sie kamen auf die Idee, Schlüsselbücher zu stehlen, um so an die Tagesschlüssel zu kommen. Die deutsche Marine hatte die stärkste Enigma, deshalb versuchte man, ihre Schlüsselbücher zu erbeuten. Aber ähnlich wie im ersten Weltkrieg mussten die Briten sehr vorsichtig handeln, da die Deutschen nicht herausfinden sollten, dass ihre Verschlüsselung geknackt wurde. Obwohl die Briten manchmal Fehler begingen, waren die Deutschen überzeugt, dass die Enigma nicht zu knacken war.

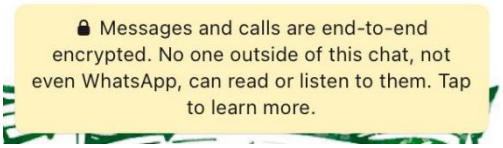
Durch die Erfolge von Bletchley wurden sehr viele Menschenleben gerettet, da der Krieg sonst länger gedauert hätte.

Nach Ende des Krieges wurde Bletchley geschlossen und alle Dokumente verbrannt oder weggeschlossen. Sogar die Entschlüsselungsmaschinen wurden verschrottet. Der Entschlüsselungsdienst wurde nach London in das Government Communications Headquarters verlegt. Manche Kryptoanalytiker kamen zwar mit, die meisten gingen aber zurück in ihr normales Leben. Sie durften nicht erzählen, was sie im zweiten Weltkrieg geleistet hatten, da sie am Anfang ihrer Karriere auf Geheimhaltung eingeschworen wurden. Viele mussten sich deshalb Beleidigungen anhören. Nach dreißig Jahren wurde das Geheimnis aufgedeckt. Man erlaubte Captain F. W. Winterbotham ein Buch über Bletchley zu schreiben. Seit da an erzählten die Kryptoanalytiker von ihrer Arbeit.

Bild: Alan Turing https://i.pinimg.com/originals/1e/30/f1/1e30f10974cb7afb75ea22ad09042f04.jpg

Cryptography today/ Kryptografie heute

During my research I found out, that our modern life without cryptography would not be possible. Whenever technology makes our life easier, it is an important part of it. Just think at social media. Everyone knows “WhatsApp” and the yellow pop-up window at the beginning of a chat. It explains that all messages are end-to-end encrypted, so that only the participating people can read the messages. Nevertheless, WhatsApp knows with whom and from where you write or phone. This encryption is a good start, but it could be improved. Therefore, many users switch to other apps, like Telegram.



I was fascinated how cryptography influenced history and I will see it through different eyes. During wars it was essential. It often saved human lives because the enemy’s movements were predicted. I liked that the mathematicians and the linguists were more important than soldiers and generals. Most of the times all these people had to keep their work secret and only many years later their accomplishments were revealed.

Die meisten guten Computer entwickelte ursprünglich das Militär, da dort immer bessere Ver- und Entschlüsselungsverfahren gebraucht wurden. Nach einiger Zeit kamen diese Geräte dann auch in unseren Alltag, wie zum Beispiel GPS und Internet.

Neu ist, dass unentschlüsselbare Verschlüsselungsverfahren von Privatpersonen erfunden wurden. Ein Vorteil ist, dass Menschen in Diktaturen sich so vor Verfolgung schützen können, andererseits kann die gleiche Technik von Verbrechern verwendet werden. Politik und Entwickler müssen entscheiden, ob es Möglichkeiten zum Entschlüsseln geben soll. Es wird spannend zu beobachten, wie sich die Kryptografie in Zukunft entwickelt.

Quellen

Singh, Simon: Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München, 2000 (16. Auflage 2020)

https://de.wikipedia.org/wiki/Maria_Stuart, 12. April 2021

https://de.wikipedia.org/wiki/Kryptographie, 15. Februar 2021

https://de.wikipedia.org/wiki/Transposition_(Kryptographie), 3. März 2021

https://de.wikipedia.org/wiki/Substitution_(Kryptographie), 14 Januar 2021

https://kiwithek.kidsweb.at/index.php/Geheimschrift, 19. Januar 2021

https://de.wikipedia.org/wiki/Rotor-Chiffriermaschine, 26. März 2021

https://de.wikipedia.org/wiki/Antoine_Rossignol, 10. Februar 2017

https://de.wikipedia.org/wiki/Homophone_Verschl%C3%BCsselung, 20. Juni 2020

https://de.wikipedia.org/wiki/Samuel_F._B._Morse, 27. April 2021

https://de.wikipedia.org/wiki/Beale-Chiffre, 17. März 2021

https://de.wikipedia.org/wiki/Guglielmo_Marconi, 30. Januar 2021

https://de.wikipedia.org/wiki/Herodot, 19. April 2021

https://it.wikipedia.org/wiki/Crittografia, 25. April 2021

https://www.youtube.com/watch?v=blMoryQcfUM, 1. November 2017

https://de.wikipedia.org/wiki/Joseph_Mauborgne, 4. Januar 2019

https://it.wikipedia.org/wiki/Bitcoin, 4. Mai 2021

https://de.wikipedia.org/wiki/Arthur_Scherbius, 21. Februar 2021

https://de.wikipedia.org/wiki/Biuro_Szyfr%C3%B3w, 8. November 2020

https://de.wikipedia.org/wiki/Government_Communications_Headquarters, 16. April 2021

https://images.computerwoche.de/bdb/3303232/738x415_f5f5f5.jpg, Bild Titelblatt