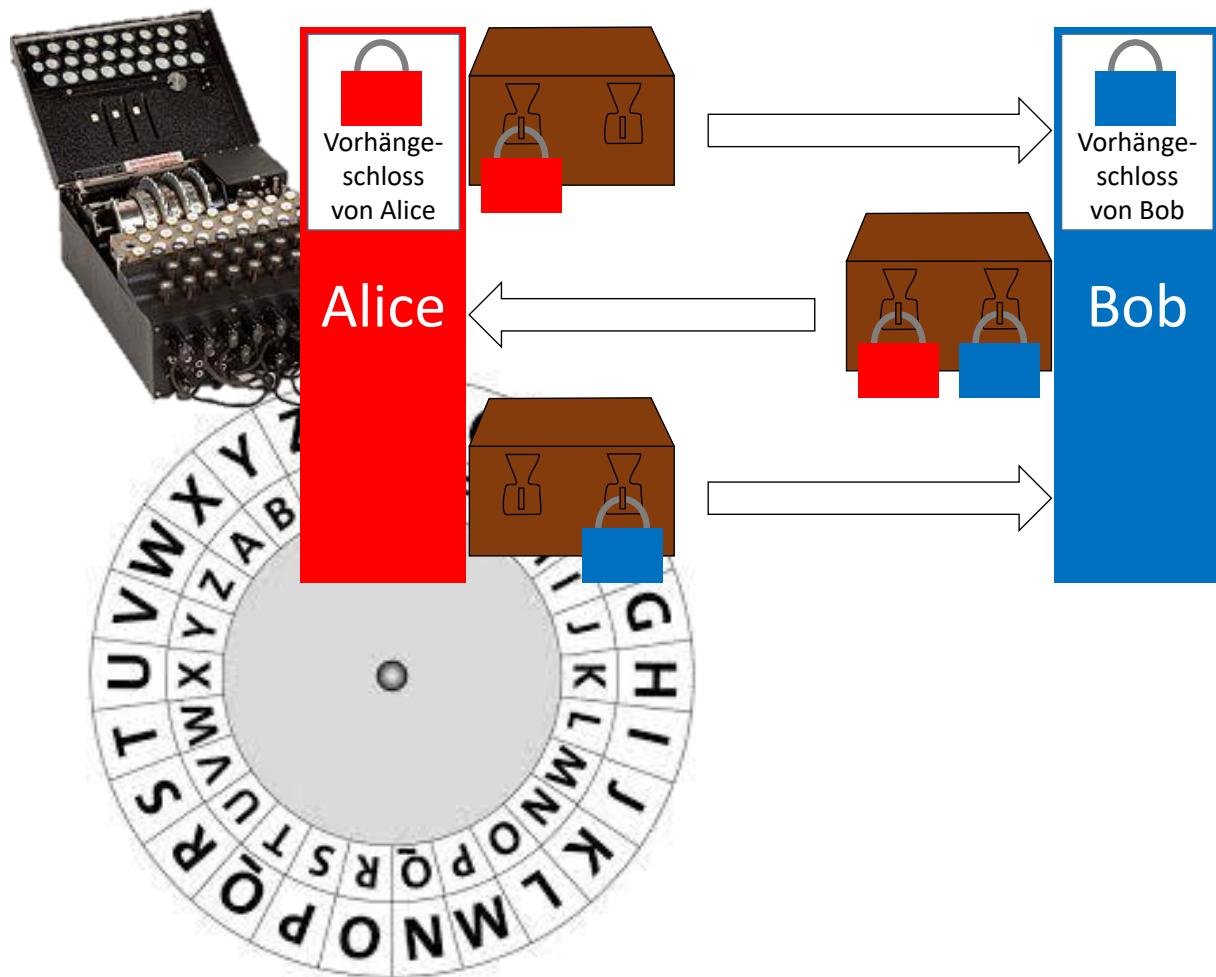


Der Schlüssel zur Kryptologie

Handbuch zum Selbststudium



Maturaarbeit von Florin Leandro Knüsel
Klasse 19b
Gymnasium Lerbermatt
15.10.2018
Betreut durch Herrn Jorma Wassmer

Inhaltsverzeichnis

1 Einleitung und Ziele dieser Arbeit	5
2 Anfänge der Kryptologie	6
2.1 Steganographie	6
2.2 Die Skytale	6
3 Monoalphabetische Verschlüsselung	8
3.1 Caesar-Chiffre	8
3.2 Chiffrierung mit Schlüsselwort	8
4 Kryptoanalyse	9
4.1 Kryptoanalyse und Buchstabenhäufigkeit	9
4.2 Kryptographen gegen Kryptoanalytiker	12
5 Polyalphabetische Verschlüsselung	13
5.1 Le chiffre indéchiffrable	13
5.2 Homophone Verschlüsselung	14
5.3 Entschlüsselung von Vigenère	15
5.4 Das One-Time-Pad	16
6 Mechanische Verschlüsselung	18
6.1 Die Chiffrierscheibe	18
6.2 Die Enigma	18
7 Kryptologie und Computer	21
7.1 Binäre Zahlen und der ASCII-Code	21
8 Das Problem der Schlüsselverteilung	23
8.1 Alice, Bob und Eve	23
8.2 Modulare Arithmetik	24
8.3 Gruppen	26
8.4 Einwegfunktionen	26
8.5 Das Diffie-Hellman-Merkle-Verfahren	27
9 Asymmetrische Verschlüsselung	30
9.1 Funktionsweise	30
9.2 RSA	30
9.2.1 Die eulersche Phi-Funktion für Primzahlen	31
9.2.2 Euklidischer Algorithmus	31
9.2.3 Erweiterter euklidischer Algorithmus	32
9.2.4 Anleitung RSA	33
9.2.5 Korrektheit RSA	34
9.2.6 Das RSA-Rätsel	35
9.3 Die asymmetrische Verschlüsselung und der Geheimdienst	36
10 Hybride Verschlüsselung	37
10.1 Pretty Good Privacy	37
10.1.1 Elektronische Unterschrift	37
10.2 Zertifikate	38

Inhaltsverzeichnis

11 Rückblick	41
12 Anhang	46
12.1 Zeichenerklärung	46
12.2 Euklidischer Algorithmus - Beweis	47
12.3 Kleiner Satz von Fermat - Beweis	48
12.4 Lösungen zu den Aufgaben	49

1 Einleitung und Ziele dieser Arbeit

Als ich mich in der neunten Klasse für ein Schwerpunktfach entscheiden musste, schwankte ich zwischen den Fächern „Wirtschaft und Recht“ (WR) und „Physik und Anwendungen der Mathematik“ (PAM). Ich entschied mich aufgrund meiner seit dem Kindergarten anhaltenden Begeisterung für Zahlen für letztere Variante. Spätestens als wir im zweiten Quartal in der angewandten Mathematik mit der Kryptologie begannen, war mir klar, dass ich die richtige Entscheidung getroffen hatte. Ich fand das Thema des Ver- und Entschlüsselns sehr spannend. Bereits als kleiner Junge hatte ich mit meinem Bruder Geheimschriften ausgedacht. Mit der Wiederentdeckung der Chiffrierscheibe, die ich noch aus Kriminalbüchern kannte, war die Faszination für das Unleserlichmachen eines Textes wieder da. Zuhause erzählte ich meiner interessierten Familie immer wieder von den neuen Methoden, die ich gelernt hatte. Die Behandlung der asymmetrischen Verschlüsselung mit RSA war das erste Thema, das ich nicht ohne weiteres verständlich erklären konnte. Meine Familie konnte die einzelnen Schritte nicht mehr ganz nachvollziehen, so sprachen wir am Tisch wieder über andere Dinge.

Im Herbst 2017 standen wir Sekundaner¹ vor der Aufgabe, ein Thema für unsere Maturaarbeit (MA) zu suchen. Nach einigen anderen Ideen kam mir der Gedanke, die Möglichkeit zu nutzen und meiner Familie doch noch die Schönheit der asymmetrischen Verschlüsselung näherzubringen. So entschied ich mich dazu, dieses Sujet als Grundbaustein für meine Arbeit zu nehmen und sie davon ausgehend zu gestalten.

In dieser Arbeit gehe ich einerseits einen Schritt zurück und erzähle, wie sich die Kryptologie bis zur Erfindung der asymmetrischen Verschlüsselung entwickelt hat, andererseits mache ich einen Schritt nach vorne und zeige, wie RSA in der hybriden Verschlüsselung angewendet wird. Mit der fortschreitenden Digitalisierung wird die Sicherheit der Datenübertragung nicht nur für die Privatsphäre immer wichtiger. Die neuen Möglichkeiten des Online-Shoppings und des E-Bankings können nur gefahrlos genutzt werden, wenn die Daten sicher verschlüsselt werden.

Das Ziel dieser Maturaarbeit ist es zu erklären, wie sich die Verschlüsselung entwickelt hat, welche Probleme es zu überwinden galt und wie sie gelöst wurden. Sie soll aufzeigen, wie es möglich ist zu verschlüsseln, ohne einen Schlüssel sicher übergeben zu müssen. Zudem soll sie die Frage klären, wie ich sicher sein kann, dass der Onlinehändler, dem ich meine Kartenzahlung angebe und auf dessen Seite ich mich mit einer PIN melde, wirklich der ist, den er vorgibt zu sein. Der interessierte Leser soll Schritt für Schritt in die Kryptologie eingeführt werden und dabei ausgewählte Verschlüsselungsverfahren aus verschiedenen Epochen verstehen und nachvollziehen können. Zum einfacheren Verständnis der mathematischen Ausdrücke sind im Anhang auf Seite 46 im Unterkapitel 12.1 die weniger bekannten mathematischen Zeichen erklärt. Um das Gelernte direkt anwenden zu können, gibt es zu jedem Kapitel Aufgaben. Die Lösungen dazu sind im Anhang ab Seite 49 zu finden. Zur Bewältigung der Aufgaben sind ein Taschenrechner und Zugang zum Internet von Vorteil.

Jetzt wünsche ich allen Lesern viel Vergnügen beim Lesen und Knobeln und beim Entdecken der faszinierenden Welt des Ver- und Entschlüsselns.

¹In dieser Arbeit wird aus Gründen der besseren Lesbarkeit stets die männliche Form verwendet. Die Angaben beziehen sich aber immer auf die Angehörigen beider Geschlechter.

2 Anfänge der Kryptologie

2.1 Steganographie

Geheimnachrichten wurden bereits vor tausenden von Jahren ausgetauscht. Der Legende nach soll der persische König Xerxes um das Jahr 480 v.Chr. den Spartanerkönig Leonidas angegriffen haben. Dieser wusste jedoch schon vor dem Auftauchen der Perser Bescheid, da ein Griech im persischen Exil ihm eine Nachricht geschickt hatte. Um sie für die Feinde unleserlich zu machen, nahm er eine Wachstafel, wie sie damals zum Schreiben verwendet wurde. Der Mann entfernte die Wachsschicht, schrieb die Mitteilung auf das Holz darunter und bestrich die Tafel wieder mit Wachs. Zum Schluss hinterliess er auf der Tafel einen belanglosen Text, um keine Aufmerksamkeit zu erregen. So gelangte die Nachricht der Ankunft von Xerxes unbemerkt nach Sparta, wo sie durch Zufall entdeckt wurde. Die Schlacht ging zwar trotzdem verloren, aber der Beginn der geheimen Nachrichtenübermittlung war Tatsache.²

Die hier beschriebene Art der Geheimhaltung, das simple Verstecken der Nachricht, heisst **Steganographie**. Dazu gehören auch das Schreiben mit Geheimtinte, die erst beim Erhitzen sichtbar wird, und das Verbergen der geheimen Mitteilung in einem unverfänglichen Text (Abbildung 1). Sie bietet zwar ein gewisses Mass an Sicherheit, hat aber einen entscheidenden Nachteil: Wird der Bote durchsucht und die Nachricht entdeckt, ist der Inhalt sofort für jeden verständlich. Ein Wachposten wird also routinemässig jeden Boten auf versteckte Botschaften kontrollieren. Deshalb hat sich die **Kryptographie** (griechisch: kryptos; verborgen) durchgesetzt, deren Ziel nicht die Verschleierung der Existenz einer Nachricht, sondern das Verbergen des Inhalts ist.³

Du bist der beste Mensch, den ich kenne. Eines Tages
wirst du meine Frau. Wir werden zusammen
durch alle Phasen des Lebens gehen.
Meine Liebe ist riesig, deshalb halte ich um deine
Hand an. Wir werden zusammen bleiben, bis wir
sterben.

Abbildung 1: Versteckte Morddrohung in einem Liebesbrief: Die ersten Wörter auf jeder Zeile ergeben den Satz: „Du wirst durch meine Hand sterben“.

2.2 Die Skytale

Eine erste Form der Verschlüsselung war die von der Regierung in Sparta benutzte **Skytale** (Abbildung 2). Das ist ein Holzzylinder mit einem bestimmten Durchmesser, um welchen ein schmales Stück Leder oder Pergament gewickelt wurde. Die Mitteilung wurde auf das Band geschrieben, abgewickelt und überbracht. Der Empfänger konnte sie einfach wieder auf seine eigene Skytale mit identischen Massen wickeln, um sie zu lesen. Wurde der Bote abgefangen, hatte er nur ein Stück Leder mit einer scheinbar zufälligen Buchstabenkette dabei.⁴

²Kippenhahn 2012.

³Singh 2017.

⁴Wassmer 2016.



Abbildung 2: Die Skytale⁵

Der Ausgangstext, der auf die Skytale geschrieben wird, heisst **Klartext** oder Plaintext. Die verschlüsselte Nachricht wird **Geheimtext**, Chiffre oder Cipher genannt. Der Verschlüsselungsvorgang heisst **Chiffrieren** und das Gegenteil ist **Dechiffrieren**.⁶

Beim genaueren Betrachten der Verschlüsselung mit der Skytale fällt auf, dass dabei nur die Buchstaben innerhalb des Textes verschoben wurden. Der Geheimtext ist also ein Anagramm des Ausgangstextes. Diese Verschlüsselungsart wird **Transposition** genannt. So funktioniert zum Beispiel auch die bei Kindern beliebte „Gartenzauntransposition“. Dabei wird zuerst der Klartext so aufgeschrieben, dass jeder zweite Buchstabe nach unten in die zweite Zeile versetzt ist (Abbildung 3).

D E I T I E E S H U S E T N C R C T
I S S E N V R C L E S L E A H I H

Abbildung 3: Die „Gartenzauntransposition“ mit dem Klartext „Dies ist eine verschlüsselte Nachricht“

Beim Übermitteln wird zuerst die obere Zeile geschrieben und dann die untere Zeile angehängt. So erhalten wir die Cipher „DEITIEESHUSETNCRCTISSENVRCLLESLEAHIH“. Um diese wieder in die ursprüngliche Botschaft zurückzuverwandeln, muss der Geheimtext einfach halbiert und untereinander auf zwei Zeilen geschrieben werden. Ist die Anzahl Buchstaben ungerade, befinden sich auf der oberen Zeile mehr Zeichen. Es wird immer abwechselnd von links nach rechts ein Buchstabe auf der oberen und dann einer auf der unteren Zeile gelesen.⁷

Bemerkung. Der Klartext wird in dieser Arbeit in Kleinbuchstaben, der Geheimtext in Grossbuchstaben geschrieben. Später kommt noch ein Schlüssel dazu, der gross und kursiv abgedruckt wird.

Aufgabe 1. Entschlüssle die durch „Gartenzauntransposition“ verschlüsselte Chiffre „DSSDER-TAFAEATIESEUGB“.

⁵Hebisch 2010.

⁶Beutelspacher 2009.

⁷Singh 2017.

3 Monoalphabetische Verschlüsselung

Die Alternative zur Transposition ist die Substitution. Dabei tauschen die Buchstaben nicht ihren Platz, sondern ihr Aussehen. Bei der **monoalphabetischen Verschlüsselung** erfolgt eine Permutation (lateinisch: permutare; vertauschen) des Klartextalphabets, so dass jedes Zeichen durch ein anderes ersetzt wird.⁸

3.1 Caesar-Chiffre

Julius Caesar benutzte eine einfache Substitutions-Chiffre. Er verschob das Alphabet um drei Positionen nach links, so dass aus einem A ein D wurde. In Abbildung 4 ist diese Verwandlung dargestellt. Oben ist das Klartextalphabet und darunter das Geheimtextalphabet. Jeder Buchstabe auf der oberen Zeile wird durch den Buchstaben darunter ersetzt. „veni vidi vici“ wird so zu „YHQL YLGL YLFL“.⁹

Aufgabe 2. Entschlüssle den mit Caesar verschlüsselten Text „JDLXV MXOLXV FDHV DU“.

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
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 4: Klar- und Geheimtextalphabet der Caesar-Chiffre

3.2 Chiffrierung mit Schlüsselwort

Zur Chiffrierung kann auch ein Schlüsselwort und ein Schlüsselbuchstabe verwendet werden.¹⁰

Beispiel. Schlüsselwort: *ZENTRIPETALBESCHLEUNIGUNG*

Schlüsselbuchstabe: *C*

Die doppelt vorkommenden Buchstaben des Schlüsselwortes werden gelöscht.

ZENTRIPALBSCHUG

Das nun entstandene Wort wird unter das Klartextalphabet geschrieben, beginnend beim Schlüsselbuchstaben. Die restliche Buchstabenfolge ist ein verschobenes Alphabet, wobei die bereits benutzten Buchstaben weggelassen werden. So entsteht das Geheimtextalphabet von Abbildung 5.

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

Abbildung 5: Klar- und Geheimtextalphabet bei Verwendung des Schlüsselwortes „ZENTRIPETALBESCHLEUNIGUNG“ und des Schlüsselbuchstabens „C“

Aufgabe 3. Verschlüssle mit dem Schlüsselwort „KATZE“ und dem Schlüsselbuchstaben „E“ den Satz „So einfach, so schön“.

⁸Kippenhahn 2012.

⁹Wassmer 2016.

¹⁰Singh 2017.

4 Kryptoanalyse

Alle bisher beschriebenen Verfahren bestehen aus einem Algorithmus und einem Schlüssel. Im Fall von Caesar (vgl. Kapitel 3.1) ist der Algorithmus das Verschieben des Geheimtextalphabets und der Schlüssel die Anzahl Verschiebungen (bei Caesar 3). Wenn ein Spion den Geheimtext in die Hände bekommt, hat er vielleicht eine Vermutung, mit welchem Verfahren chiffriert wurde, es besteht aber durchaus die Hoffnung, dass er den Schlüssel nicht kennt. Auguste Kerkhoffs von Nieuwenhof beschrieb die Bedeutung des Schlüssels gegenüber dem Algorithmus so:

Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.¹¹

Ideal ist zudem eine Vielzahl möglicher Schlüssel. Das Alphabet hat 26 Buchstaben (ä, ö, ü mit ae, oe, ue). Somit gibt es 25 verschiedene Möglichkeiten, das Alphabet zu verschieben. Man ahnt bereits, dass die Caesar-Cipher einem Brute-Force-Angriff (alle Möglichkeiten durchprobieren) keinen grossen Widerstand bietet. Nun kann man aber auch willkürlich einen Buchstaben dem anderen zuordnen. So gibt es bereits 26! Möglichkeiten (mehr als 400 000 000 000 000 000 000 000 000). Könnte ein Mensch eine Möglichkeit pro Sekunde prüfen und würde jeder Mensch auf der Erde jede Sekunde dafür aufwenden, hätte die Weltbevölkerung fast so lange, wie das Universum alt ist, um die richtige Zuordnung zu finden. Deshalb galt diese Verschlüsselungsart für mehrere hundert Jahre als unknackbar, bis die Araber die **Kryptoanalyse** erfanden, die Wissenschaft der Entschlüsselung ohne Kenntnis des Schlüssels. Zusammen mit der Kryptographie gehört sie zur **Kryptologie**, der Wissenschaft des Ver- und Entschlüsselns. Die islamische Kultur besagt, dass jeder Muslim Wissen auf allen Gebieten erlangen sollte. So ist es nicht erstaunlich, dass es Personen aus diesem Kulturreis waren, die die Idee hatten, Geheimschriften mit Hilfe der Häufigkeiten der Buchstaben zu entschlüsseln. Die früheste bekannte Beschreibung dieser Technik stammt aus dem 9. Jahrhundert von einem Gelehrten namens Abū Yūsūf Ya'kūb ibn ds-hāq ibn as-Sabbāh ibn 'omrān ibn Ismaīl al-kindī.¹²

4.1 Kryptoanalyse und Buchstabenhäufigkeit

Um einen durch willkürliche Substitution verschlüsselten Text ohne Kenntnis des Schlüssels zu dechiffrieren, sollte man einen möglichst langen Teil davon haben. Nun zählt man, wie oft jeder Buchstabe im Geheimtext vorkommt und vergleicht die Häufigkeit mit der Buchstabenhäufigkeit der jeweiligen Sprache. Die Verteilung der Häufigkeiten in der deutschen Sprache ist in Abbildung 6 dargestellt. Schnell findet man e und n. Da die Häufigkeiten in der Tabelle nur Durchschnittswerte sind, kann man jetzt nicht einfach so weiterfahren. Hilfe bietet die Häufigkeitsverteilung der Bigramme (Abbildung 7). Diese zeigt, wie oft welche zwei Buchstaben durchschnittlich aufeinander folgen. Durch auszählen der Bigramme kann man i, s, r, a und t herausfiltern. Über das Bigramm „ch“ kann man zusätzlich diese beiden Buchstaben finden, da sie fast nie in umgekehrter Reihenfolge vorkommen. Durch Ausprobieren findet man schnell den Rest, da die bereits bekannten Buchstaben schon über 60% des Textes ausmachen.¹³

¹¹Singh 2017.

¹²Singh 2017.

¹³Wassmer 2016.

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
A	6.51	N	9.78
B	1.89	O	2.51
C	3.06	P	0.79
D	5.08	Q	0.02
E	17.40	R	7.00
F	1.66	S	7.27
G	3.01	T	6.15
H	4.76	U	4.35
I	7.55	V	0.67
J	0.27	W	1.89
K	1.21	X	0.03
L	3.44	Y	0.04
M	2.53	Z	1.13

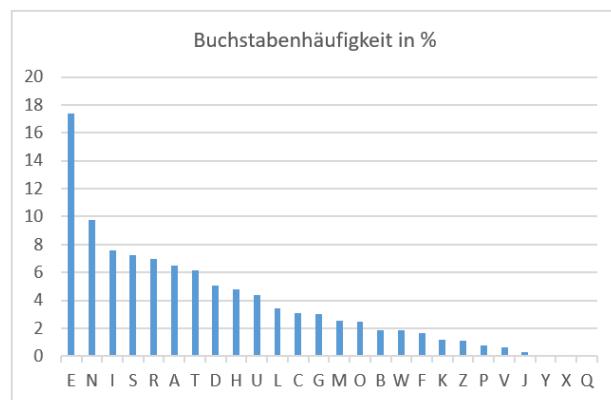


Abbildung 6: Buchstabenhäufigkeit in der deutschen Sprache¹⁴

Bigramm	Häufigkeit in %	Bigramm	Häufigkeit in %
en	3.88	nd	1.99
er	3.75	ei	1.88
ch	2.75	ie	1.79
te	2.66	in	1.67
de	2.00	es	1.52

Abbildung 7: Die häufigsten Bigramme in der deutschen Sprache¹⁵

Beispiel. Verschlüsselter Text:

BQMCKUDSH MWN SMQS ZXQQWUCXANWWPKENXEN XBW ISE AXZMVMS ISE WN-KUDRXVVWPMVS. SW WNXZZN BSRSE RXQIH OKZ CKUDSH XR, XBW ISZ SRSQWK IXW EKVVCKUDSH BQI IXW SMWCKUDSH CSEOKELSLXQLSQ WMQI. BQMCKUDSH TBEIS MQ WUCTSISQ, AMQQVXQI BQI ISE WUCTSMJ LSZSMQWXZ SQNTMUDSVN, BQNSE XQISESZ OKZ WUCTSMJSE NSXZVSMNSE ISE DVKNSQ AVHSEW, EKVA CBENM TMSIZSE. SW CXQISVN WMUC IXRSM BZ SMQ ISZ CXVVSQCKUDSH XSCQVMUCSW WPMSV, RSM ISZ XBUC CMQNSE ISQ NKESQ LSWPMSVN TSEISQ DXQQ.

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
S	62	B	12
Q	32	D	9
M	27	H	8
W	25	R	7
E	23	T	6
X	23	A	5
I	22	L	5
C	20	P	4
N	18	O	3
V	18	J	2
K	16	Y	1
U	15	G	0
Z	15	F	0

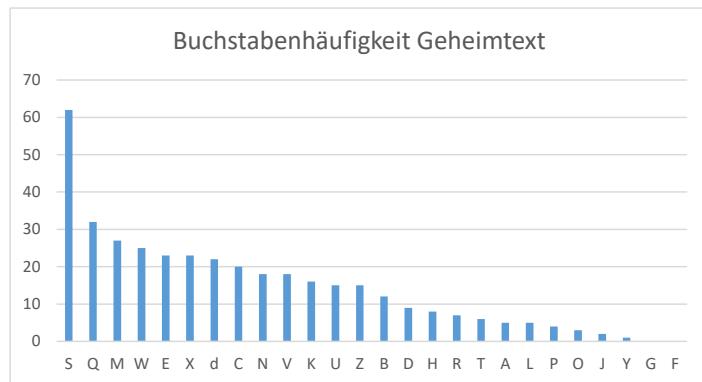


Abbildung 8: Buchstabenhäufigkeit im Geheimtext

¹⁴Daten aus Beutelspacher 2009.

¹⁵Daten aus Beutelspacher 2009.

Bei der Analyse der Buchstabenhäufigkeiten in diesem Geheimtext erhalten wir die Daten in Abbildung 8. Schnell erraten wir S=e. Zudem ist n entweder Q oder M. Da die Buchstaben i, s, r und a etwa gleich verteilt sind, müssen sie durch Q, M, W, E oder X dargestellt werden.

$$n \in \{Q, M\}, i, s, r, a \in \{Q, M, W, E, X\}$$

Durch Zählen der Bigramme, die mit e, also in unserem Geheimtext mit S, beginnen, erhalten wir die Häufigkeitsverteilungen in Abbildung 9. Daraus folgt, dass die drei häufigsten Bigramme SE, SM und SQ die Klartextbigramme er, en und ei darstellen.

$$n, i, r \in \{Q, M, E\}$$

Bigramm	Häufigkeit	Bigramm	Häufigkeit
SE	15	SW	3
SM	9	SI	2
SQ	9	SR	1
SH	6	SL	1
SV	5	SX	1
SZ	5		

Abbildung 9: Häufigkeit der Bigramme, die mit dem Geheimtextbuchstaben „S“ beginnen

Wir suchen ie, welches entweder ES, MS oder QS heissen muss und vermuten MS, da dieses mit fünfmal am häufigsten vertreten ist. Also ist M=i und damit Q=n und E=r. Somit bleiben für s und a nur noch W und X.

$$s, a \in \{W, X\}$$

Weiter kommt das Bigramm UC siebenmal vor, die Kombination CU aber nie. Das lässt uns auf U=c und C=h schliessen. Durch Einsetzen erhalten wir den Text:

BnihKcDeH iWN eine ZXnnWchXANWWPKENXEN XBW leE AXZiVie leE WNKcDRXVV-WPiVe. eW WNXZZN BeReE RXnIH OKZ hKcDeH XR, XBW leZ eRenWK IXW EKVvhKc-DeH BnI IXW eiWhKcDeH heEOKELeLXnLen Winl. BnihKcDeH TBEle in WchTelen, AinnVX-nl BnI leE WchTeiJ LeZeinWXZ enNTicDeVN, BnNeE XnleEeZ OKZ WchTeiJeE NeXZVeiNeE leE DVKNen AVHeEW, EKVA hBENi TielZeE. eW hXnleVN Wich IXRei BZ ein leZ hXVVen-hKcDeH XehnVicheW WPiVe, Rei leZ XBch hinNeE len NKEen LeWPiVeVN TeElen DXnn.

Die zwei W hintereinander und das Vorkommen des Wortes „eW“ lassen auf den Buchstaben s schliessen. Damit steht fest: W=s und X=a. Zudem kommt der Buchstabe D achtmal nach einem c vor (ck) und das letzte Wort „Dann“ könnte „kann“ heissen. D=k.

BnihKckeH isN eine ZannschaANssPKENaEN aBs leE AaZiVie leE sNKckRaVVVsPieVe. es sNaZZN BeReE RanIH OKZ hKckeH aR, aBs leZ eRensK las EKVvhKckeH BnI las eis-hKckeH heEOKELeLanLen sinl. BnihKckeH TBEle in schTelen, AinnVanl BnI leE schTeiJ LeZeinsaZ enNTickeVN, BnNeE anleEeZ OKZ schTeiJeE NeazVeiNeE leE kVKNen AVHeEs, EKVA hBENi TielZeE. es hanleVN sich laRei BZ ein leZ haVVenhKckeH aehnViches sPieV, Rei leZ aBch hinNeE len NKEen LesPieVN TeElen kann.

Jetzt geht alles durch Versuche:

V=l, R=b, B=u, I=d, P=p, N=t, E=r, K=o, H=y, Z=m, L=g, T=w, A=f, O=v, J=z

Nach Beachtung der Gross- und Kleinschreibung und der Wiederherstellung der Umlaute erhalten wir folgenden Text:

*Unihockey ist eine Mannschaftssportart aus der Familie der Stockballspiele. Es stammt über Bandy vom Hockey ab, aus dem ebenso das Rollhockey und das Eishockey hervorgegangen sind. Unihockey wurde in Schweden, Finnland und der Schweiz gemeinsam entwickelt, unter anderem vom Schweizer Teamleiter der Kloten Flyers, Rolf Hurti Wiedmer. Es handelt sich dabei um ein dem Hallenhockey ähnliches Spiel, bei dem auch hinter den Toren gespielt werden kann.*¹⁶

Dieser Text war relativ einfach zu knacken. Das ist aber nicht immer so. Der französische Autor Georges Perec schrieb zum Beispiel den Roman „La disparition“, in welchem kein einziges Mal der Buchstabe e vorkommt. Wäre dieses Buch verschlüsselt, würde man mit einer einfachen Häufigkeitsanalyse ins Leere laufen. Eine möglichst sicher verschlüsselte Nachricht sollte deshalb immer kurz sein und einige Fehler beinhalten. Zudem sollten die Wortzwischenräume weggelassen werden und es ist von Vorteil, wenn der Kryptoanalytiker nicht weiß, in welcher Sprache die Botschaft verfasst wurde.¹⁷

4.2 Kryptographen gegen Kryptoanalytiker

Es gab nun also einen Weg, einen verschlüsselten Text ohne Kenntnis des Schlüssels zu lesen. Das war der Beginn des ewigen Wettstreites zwischen Kryptographen und Kryptoanalytikern. Gegen Ende des 16. Jahrhunderts wurde die Kryptoanalyse ein eigenes Gewerbe. Jede europäische Macht hatte ihre eigene **Schwarze Kammer**, ein Nervenzentrum, in dem Botschaften entschlüsselt und Informationen zusammengetragen wurden. Kaum wurde eine neue Chiffriermethode erfunden, kamen die Codeknacker und versuchten, die Schwäche der Variante zu finden. War das gelungen, musste, so wie im oben beschriebenen Fall, wieder eine neue Methode her. Der Schritt, den die Kryptographen darauf machten, war die Einführung von **Codes**, also von Zeichen, die oft verwendete Wörter ersetzten. So wurden zum Beispiel die Zahlen von 001 bis 999 verwendet. 26 Zeichen waren für die Buchstaben, der Rest für Wörter wie die, ein, und, Tod, viel, etc. Zudem wurden oftmals Nummern definiert, die gar keine Bedeutung hatten und nur die Kryptoanalytiker in die Irre führen sollten, sogenannte **Füller**. So wurden ganze Codebücher erstellt und verteilt. Das war eine sehr aufwändige Arbeit, die immer noch relativ schnell entschlüsselt werden konnte. So wurden trotz der tiefen Sicherheit viele der älteren Methoden weiter verwendet.¹⁸

¹⁶Didym 2018.

¹⁷Singh 2017.

¹⁸Kippenhahn 2012.

5 Polyalphabetische Verschlüsselung

Der Mathematiker Leon Battista Alberti hatte um das Jahr 1460 die Idee für eine neue, revolutionäre Chiffriermethode. Er schlug vor, zwei Geheimtextalphabete zu verwenden und jeweils einen Buchstaben mit dem einen und den nächsten mit dem anderen zu verschlüsseln.¹⁹ Mit dem Schlüsselwort „ZENTRIPETALBESCHLEUNIGUNG“ und dem Schlüsselbuchstaben „C“ für das erste und dem Wort „VIGENERE“ und dem Buchstaben „Z“ für das zweite Geheimtextalphabet ergeben sich die in Abbildung 10 dargestellten Stellvertreter. Wollen wir nun das Wort „super“ verschlüsseln, nehmen wir den Ersatzbuchstaben für das „s“ aus dem ersten Alphabet, also „F“, den Buchstaben für „u“ aus dem zweiten Alphabet („U“), den Buchstaben aus dem oberen Alphabet für „p“ („U“) und so weiter. So erhalten wir den Geheimtext „FUURD“.

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

Abbildung 10: Verschlüsselung mit zwei Geheimtextalphabeten

Oben: Klartextalphabet

Mitte: Schlüsselwort ZENTRIPETALBESCHLEUNIGUNG und Schlüsselbuchstabe C

Unten: Schlüsselwort VIGENERE und Schlüsselbuchstabe Z

Alle vorherigen Arten der Chiffrierung waren monoalphabetisch. Jeder Buchstabe des Klartextes wird immer mit dem selben Buchstaben des Geheimtextalphabets ersetzt. Die Erfindung von Alberti ist dagegen eine **polyalphabetische Verschlüsselung**. Dabei kann ein Buchstabe mit zwei verschiedenen Stellvertretern verschlüsselt werden (rr=DQ). Zudem kann ein Geheimtextbuchstabe Stellvertreter für zwei verschiedene Klartextbuchstaben sein (KK=um). Die Häufigkeitsanalyse ist damit wertlos. Die Idee von Alberti war der bedeutendste Durchbruch der Kryptographie seit über einem Jahrtausend. Der französische Diplomat Blaise de Vigenère entwickelte diese Idee weiter zur **Vigenère-Chiffrierung**.²⁰

5.1 Le chiffre indéchiffrable

Für die Chiffrierung mit Vigenère benötigt man ein Vigenère-Quadrat (Abbildung 12) und ein Schlüsselwort oder einen Schlüsselsatz.²¹

Beispiel.

Schlüsselwort: BUCH

Klartext: guten morgen

Zuerst wird der Schlüssel periodisch unter den Klartext geschrieben (Abbildung 11). Nun wird jeder Buchstabe mit dem Geheimtextalphabet von Abbildung 12 verschlüsselt, an dessen Zeilenanfang sein Schlüsselbuchstabe steht. Um den Buchstaben „g“ zu verschlüsseln, gehen wir in die Zeile, an welcher das „B“ am Anfang steht und fahren waagrecht nach rechts, bis wir in der Spalte landen, in welcher der Buchstabe „g“ an oberster Stelle steht (gelb markiert in Abbildung 12). Der Buchstabe „H“, an welchem wir angekommen sind, vertritt nun das „g“. Genauso verfahren wir mit dem Buchstaben „u“ (grün markiert) und allen anderen. Die erhaltene Chiffre heisst „HOVLOGQYHYP“. Um sie zu entschlüsseln, geht man den umgekehrten Weg. Man fährt auf der Zeile mit dem Schlüsselbuchstaben („B“) ganz links nach rechts, bis man auf

¹⁹Kippenhahn 2012.

²⁰Singh 2017.

²¹Wassmer 2016.

den Geheimtextbuchstaben („H“) trifft. Der oberste Buchstabe in dieser Spalte ist der Buchstabe des Klartextes („g“).

g	u	t	e	n	m	o	r	g	e	n
B	U	C	H	B	U	C	H	B	U	C
H	O	V	L	O	G	Q	Y	H	Y	P

Abbildung 11: Verschlüsselung von „guten morgen“ mit Vigenère mit dem Schlüsselwort „BUCH“

Klartextbuchstaben																									
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Abbildung 12: Vigenère-Quadrat
gelb: „g“ verschlüsselt mit „B“ ergibt den Geheimtextbuchstaben „H“
grün: „u“ verschlüsselt mit „U“ ergibt den Geheimtextbuchstaben „O“

Aufgabe 4. Verschlüssele mit Vigenère:

Schlüssel: MATURA

Nachricht: Kryptologie

5.2 Homophone Verschlüsselung

Für private Nachrichten reichte die monoalphabetische Verschlüsselung auch im 17. Jahrhundert noch vollkommen aus. Für den staatlichen und militärischen Nachrichtenverkehr mussten die Chiffriermethoden aber sicherer sein. Da die Vigenère-Verschlüsselung sehr kompliziert war, wurde sie lange Zeit nicht benutzt. Stattdessen suchte man nach einem Kompromiss zwischen Sicherheit und Einfachheit und traf auf die sogenannte **homophone Verschlüsselung** (griechisch: homos; gleich, phone; Klang). Dabei wird jeder Buchstabe durch mehrere

Stellvertreter ersetzt, wobei die Anzahl der Vertreter proportional zur Häufigkeit der Buchstaben gewählt wird. So kann man beim Verschlüsseln des „r“, wenn man die Ziffern 00 bis 99 benutzt, zwischen sieben verschiedenen Zeichen auswählen, da von einhundert Buchstaben etwa jeder siebte ein „r“ ist. Das „q“ wird hingegen nur von einer Zahl aus dem Geheimtextalphabet ersetzt (Abbildung 13). So kommt im Geheimtext jede Zahl mit einer Häufigkeit von etwa einem Prozent vor. Dabei gibt es aber zwei Probleme: Erstens ist der Schlüssel nun wieder länger und zweitens kann ein geübter Kryptoanalytiker mit Hilfe der typischen Charaktereigenschaften der Buchstaben immer noch den Geheimtext unerlaubt entschlüsseln. Ein Beispiel dafür sind der Buchstabe „q“, auf welchen immer ein „u“ folgt, oder das bereits erwähnte „ch“. Obwohl ein Klartextbuchstabe nun mit verschiedenen Geheimtextzeichen verschlüsselt werden kann, ist diese Chiffrierart nicht polyalphabetisch. Der entscheidende Unterschied ist, dass bei einer homophonen Verschlüsselung jedes Zeichen nur einen Klartextbuchstaben darstellen kann, während ein solches bei der polyalphabetischen Verschlüsselung Stellvertreter für verschiedene Klartextbuchstaben sein kann. Trotzdem bot die homophone Verschlüsselung für den Alltag eine ziemlich grosse Sicherheit. Noch sicherer wurde sie durch Ergänzungen wie Zeichen, die das vordere Zeichen wieder löschten, oder durch Füllwörter.²²

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	
88	42	60	87	32	76	94	21	57	20	29	38	65	01	82	9	18	27	90	53	07	43	52	61	70	79	
97	51	69	96	41	85	03	30	66		47	74	10	91			36	99	62	16							
06	78	05	50		12	39	75			56	83	19	00			45	08	71	25							
15		14	59		48	84				92	28				54	17	80	34								
24		23	68			93					37				63	26	89									
33			77			02					46				72	35	98									
			86			11					55				81	44										
			95								64															
			04								73															
			13																							
			22																							
			31																							
			40																							
			49																							
			58																							
			67																							

Abbildung 13: Homophone Verschlüsselung²³

5.3 Entschlüsselung von Vigenère

Im 19. Jahrhundert wurde die Vigenère-Chiffrierung, so unmöglich das auch klingen mag, gleich zweimal unabhängig voneinander geknackt. Zuerst im Jahr 1854 vom Briten Charles Babbage. Dieser veröffentlichte seine Entdeckung jedoch nie; vermutlich, weil er von der britischen Regierung zur Geheimhaltung gezwungen wurde. Das Verfahren von Babbage beruht auf den Wiederholungen von Kurzwörtern wie „der“ oder „mit“, die zufälligerweise mit demselben Teil des Schlüssels chiffriert worden sind und deshalb denselben Geheimtext ergeben. Der Schlüssel wiederholt sich zwischen zwei gleichen Wörtern oder Wortteilen mehrere Male und landet schliesslich mit Beginn des zweiten Wortes wieder am genau gleichen Ort. So kann man mit etwas Geschick die Anzahl Buchstaben des Schlüsselwortes ausrechnen und den Klartext herausfinden. 1863 hatte der preussische Offizier Friedrich Wilhelm Kasiski genau den gleichen Ansatz zur Kryptoanalyse der Vigenère-Chiffrierung, weshalb dieses Verfahren heute als **Kasiski-Test** bekannt ist.²⁴

²²Singh 2017.

²³Brätz 2015.

²⁴Kippenhahn 2012.

Die Kryptoanalytiker hatten ihre Aufgabe gelöst; jetzt war der Ball wieder bei den Kryptographen. Gute Verschlüsselungen wurden mit der Erfindung des Telegraphen und der Funkwellen wichtiger denn je. Das Abhören von Nachrichten war so einfach wie noch nie. Private und geschäftliche Nachrichten mussten geschützt werden. Die einzigen neuen Chiffriermethoden, die erfunden wurden, waren jedoch Kombinationen oder Weiterentwicklungen von bereits bestehenden Varianten. Erst gegen Ende des ersten Weltkrieges entdeckten die Kryptographen eine Verschlüsselung auf der Grundlage der Vigenère-Verschlüsselung, die wirklich sicher war.²⁵

5.4 Das One-Time-Pad

Die Schwäche der Vigenère-Chiffrierung ist das Schlüsselwort, das sich laufend wiederholt. So werden in regelmässigen Abständen Buchstaben mit demselben Geheimtextalphabet verschlüsselt. Kann der Feind die Länge des Schlüsselwortes ausfindig machen, hat er eine monoalphabetisch verschlüsselte Reihe an Buchstaben, die er durch Häufigkeitsanalyse lösen kann. Je kleiner die Chance ist, dass das geschieht, das heisst je länger das Schlüsselwort ist, desto schwieriger wird das für ihn. Haben wir einen Schlüssel, der so lang ist wie die Nachricht, funktioniert der Kasiski-Test nicht. Um einen so langen Schlüssel zu erhalten, könnte man zum Beispiel ein Buch nehmen oder den Text eines Liedes. Auch diese Variante ist aber noch nicht vollständig sicher: Um auf den Schlüssel zu kommen, kann man oft verwendete Wörter an verschiedenen Stellen als Klartext ausprobieren und erhält den Teil des Schlüssels, mit dem sie verschlüsselt werden müssten. Natürlich kann „XTCP“ kein Teil des Schlüssels sein, „QUAL“ aber vielleicht schon. So könnte man unter Umständen den Schlüssel, der ja hier einen Sinn ergibt, herausfinden. Ein Schlüssel, der so lang ist wie die Botschaft selbst, garantiert also noch keine absolute Sicherheit. Wollen wir eine Verschlüsselung, die man ohne Schlüssel auf keinen Fall knacken kann, müssen wir einen Zufallsschlüssel verwenden, der die Länge des zu verschlüsselnden Textes hat. Dieser Schlüssel wird dem Empfänger zum Beispiel bei einem persönlichen Treffen sicher zugestellt. Der Absender verwendet ihn zum Chiffrieren, der Empfänger zum Dechiffrieren, danach werden sie vernichtet. Es kann mathematisch bewiesen werden, dass dieses sogenannte **One-Time-Pad** absolute Sicherheit bietet. Ein Angreifer könnte zwar alle möglichen Schlüssel nacheinander auf den Geheimtext anwenden, doch er erhält dabei einfach alle überhaupt möglichen Klartexte mit der Länge der Chiffre. So kann er nicht zwischen den Richtigen und den Falschen unterscheiden und muss sich geschlagen geben. In Abbildung 14 ist dieser Gedankengang dargestellt.²⁶

Schlüssel 1:	P	N	I	F	D	Y	F	Y	D	J	P	A
Ergibt Klartext 1:	a	n	g	r	i	f	f	h	e	u	t	e
Schlüssel 2:	F	A	Z	O	S	J	Z	F	O	V	U	R
Ergibt Klartext 2:	k	a	p	i	t	u	l	a	t	i	o	n

Abbildung 14: Durch das Ausprobieren von verschiedenen Schlüsseln für das „One-Time-Pad“ kommt man mit dem Geheimtext „PAOWLDKFHDIE“ auf die Klartexte „Angriff heute“ und „Kapitulation“.

Auch das vollkommen sichere One-Time-Pad hat einen Mangel. Dieser liegt darin, dass der Schlüssel zufällig gewählt sein muss. Das ist jedoch nicht so einfach, da der Schlüssel wirklich keinerlei Muster aufweisen darf. Um dies zu erreichen, kann man nicht einfach wild auf der Tastatur herumtippen, da man mit der Zeit in das Muster verfällt, immer einen Buchstaben mit

²⁵Singh 2017.

²⁶Singh 2017.

der rechten und danach einen mit der linken Hand zu tippen. Man könnte aber Zettel mit den Nummern 1 bis 26 in einen Hut legen, blind einen ziehen, ihn wieder hineinlegen und erneut ziehen. Das Erzeugen von solchen Zufallsschlüsseln war zur Zeit des ersten Weltkriegs, als das One-Time-Pad erfunden wurde, eine zeitaufwändige, kostspielige und mühselige Arbeit. Selbst wenn es möglich gewesen wäre, schnell genügend Zufallsschlüssel für die ganze Armee zu generieren, wäre da immer noch das Problem der Schlüsselverteilung gewesen. Niemals hätte man alle diese Schlüssel in einer sinnvollen Zeit sicher übermitteln können. Deshalb fand das One-Time-Pad in der Praxis nicht wirklich Anwendung.²⁷

²⁷Kippenhahn 2012.

6 Mechanische Verschlüsselung

6.1 Die Chiffrierscheibe

Das erste kryptographische Gerät war die **Chiffrierscheibe**. Sie wurde im 15. Jahrhundert vom italienischen Architekten Leon Alberti erfunden. Grundbestandteil sind zwei Scheiben, die eine etwas grösser als die andere. Am Rand sind die Buchstaben in alphabetischer Reihenfolge geschrieben. In der Mitte befindet sich eine Achse, um die sich die Scheiben drehen können. Um mit Caesar zu verschlüsseln, dreht man den Schlüsselbuchstaben, zum Beispiel „D“, der inneren Scheibe zum „a“ der Äusseren Scheibe. Nun hat man aussen das Klartext- und innen das Geheimtextalphabet und kann den zu verschlüsselnden Buchstaben auf der äusseren Scheibe suchen und durch den auf der inneren Scheibe stehenden ersetzen.²⁸



Abbildung 15: Die Chiffrierscheibe²⁹

6.2 Die Enigma

Am 23. Februar 1918 liess der deutsche Elektroingenieur Arthur Scherbius eine Verschlüsselungsmaschine patentieren, die **Enigma** (griechisch: *aínigma*; Rätsel). Sie besteht im Wesentlichen aus einer Tastatur, drei miteinander verdrahteten Walzen, einem Reflektor und einem Lampenfeld. Gibt man auf der Tastatur einen Klartextbuchstaben ein, wird ein elektrisches Signal abgegeben. Jede der drei hintereinander angeordneten Walzen leitet dieses zu einem anderen Buchstaben um. Nach den drei Walzen kommt ein Reflektor, der den Strom wieder durch die Walzen zurückschickt. Am Ende landet das Signal bei einer anderen Taste, deren zugehörige Lampe aufleuchtet. Der eingegebene Buchstabe wird durch den Buchstaben ersetzt, der aufleuchtet. Bei jedem Tastenanschlag dreht sich die vorderste Walze um 1/26 Umdrehung. Wird der nächste Buchstabe eingegeben, geht dasselbe von vorne los. Nach jeder 26. Eingabe dreht sich die zweite Walze einen Buchstaben weiter, nach der 676. Eingabe die Dritte. So kann man einen Text mit 17 576 Zeichen verschlüsseln und die Walzenlage wird immer eine andere sein. Es handelt sich also um eine polyalphabetische Verschlüsselung, die so komplex ist, dass bei der Verschlüsselung von Hand unweigerlich Flüchtigkeitsfehler auftreten würden.³⁰ So wie die Enigma hier beschrieben ist, ist sie noch nicht sehr sicher. Ein Gegner, der sich eine Enigma beschaffen kann, wird einfach nacheinander jede Walzeneinstellung durchprobieren, ein

²⁸Kippenhahn 2012.

²⁹Südwestrundfunk 2005.

³⁰Schäfer, Putsch, Träumner, Caplan, John 2002.

paar Zeichen des Geheimtextes eingeben und schauen, ob der Klartext einen Sinn ergibt. Wenn er pro Minute eine Variante prüfen kann, benötigt er etwa zwei Wochen, um den Schlüssel zu finden. Wenn der Feind aber ein Dutzend Leute zur Verfügung hat, ist das in einem Tag geschafft. Deshalb entschloss sich Scherbius dazu, die Anzahl möglicher Schlüssel zu vergrößern. Da er die Handlichkeit der Enigma beibehalten wollte, konnte er nicht einfach zusätzliche Walzen einführen. Stattdessen sollten die Walzen herausgenommen und vertauscht werden können. So konnte der Kryptograph aus verschiedenen Walzen drei auswählen und in beliebiger Reihenfolge einfügen. Zudem wurde zwischen der Tastatur und der ersten Walze ein Steckbrett eingeführt, mit dem zwei Buchstaben vertauscht werden konnten. Dank diesen Änderungen gibt es etwa 10 000 000 000 000 verschiedene Grundstellungen, was diese mechanische Verschlüsselungsmaschine zu jener Zeit sehr sicher machte.³¹ ³²

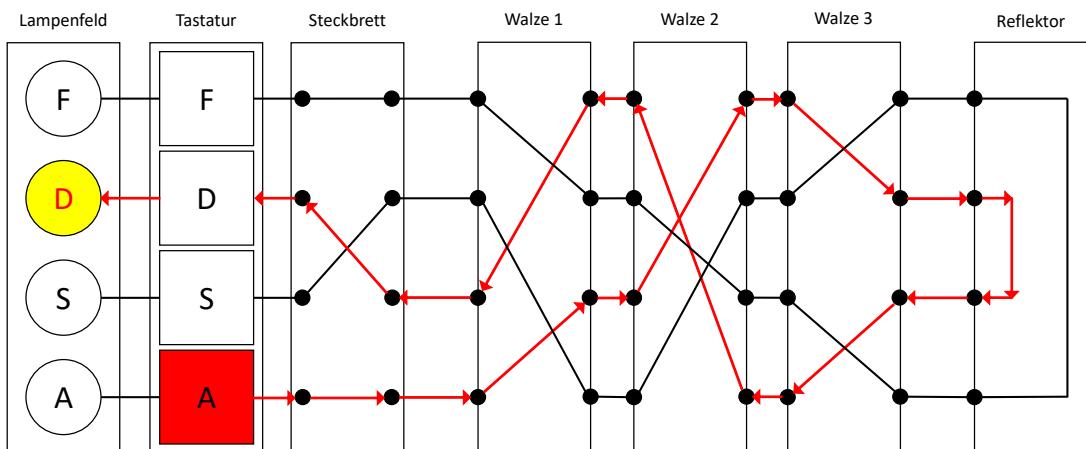


Abbildung 16: Schaltplan einer Enigma: Ein „a“ wird als „D“ verschlüsselt.

Auf den ersten Blick scheint der Reflektor ein sinnloser Zusatz zu sein, weil er unbeweglich ist und keine zusätzliche Sicherheit bietet. Der Nutzen liegt aber bei der Dechiffrierung. Der Vorteil des Reflektors ist, dass so immer zwei Buchstaben einander zugeordnet werden. Wird also ein „a“ als „D“ verschlüsselt, wird mit der gleichen Einstellung auch ein „d“ als „A“ chiffriert (Abbildung 16). Haben wir vor uns den Geheimtextbuchstaben „D“, können wir also einfach dieselbe Einstellung der Walzen wählen wie der Kryptograph, drücken die Taste „D“ und heraus kommt der Klartextbuchstabe „a“. Der Schlüssel, den die beiden Parteien wissen müssen, ist also die Reihenfolge und Anfangseinstellung der Walzen und die Buchstaben, die mit dem Steckbrett vertauscht werden.³³

³¹Singh 2017.

³²Eine detaillierte Dokumentation zum Aufbau und zur Funktionsweise der Enigma ist auf der Webseite <http://www.matheprisma.uni-wuppertal.de/Module/Enigma/index.htm> zu finden.

³³Singh 2017.



Abbildung 17: Die Enigma³⁴

Zuerst wollte niemand diese neue Erfindung kaufen. Weder die Enigma noch die vielen ähnlichen Maschinen, die etwa zur selben Zeit auf den Markt kamen fanden Interessenten. Als Winston Churchill 1923 das Buch „The World Crisis“ herausbrachte, in welchem beschrieben wird, wie die Briten im ersten Weltkrieg in den Besitz von wertvollem deutschem kryptographischem Material gelangt waren, wurde den Deutschen bewusst, dass ihre Verschlüsselungsmethoden nicht mehr sicher waren. Von nun an benutzten sie die Enigma, die damit doch noch einen Verwendungszweck hatte. Dank riesigem Aufwand der Schwarzen Kammer der Engländer gelang es während dem zweiten Weltkrieg, die Enigma zu knacken. Einen wesentlichen Beitrag dazu leisteten Alan Turing und seine „Bombe“, ein erster Vorläufer des Computers.^{35 36}

³⁴Nassiri o.D.

³⁵Kippenhahn 2012.

³⁶Darüber wurde ein Film gedreht: „The Imitation Game“, Jahr 2014.

7 Kryptologie und Computer

Mit der Erfindung des Computers wurde ein neues Werkzeug für die Kryptologie geschaffen. Er ist viel schneller als ein Mensch und kann Schlüssel mit einer unglaublichen Geschwindigkeit durchprobieren. Doch auch für die Schaffung deutlich komplexerer Verschlüsselungen ist er der entscheidende Faktor. Mit seiner Hilfe können mechanische Maschinen von enormer Komplexität simuliert werden. Man könnte etwa eine Enigma nachahmen, die 80 Walzen besitzt, von denen sich einige bei jedem siebten Tastenanschlag mit der nächsten vertauschen, andere manchmal verschwinden und an anderer Stelle wieder auftauchen sowie die einen sich im Uhrzeigersinn und die anderen in der Gegenrichtung drehen.³⁷

7.1 Binäre Zahlen und der ASCII-Code

Ausser der Geschwindigkeit und der möglichen Komplexität der simulierten Maschinen gibt es noch einen weiteren Unterschied zur herkömmlichen Verschlüsselung. Der Computer chiffriert im **Binärcode**, also einer Folge von Einsen und Nullen (lateinisch: bi; zwei). Für die Umwandlung von Buchstaben in Zahlen gibt es verschiedene Möglichkeiten. Die am häufigsten angewendete ist der **American Standard Code for Information Interchange** (ASCII). Er enthält 2^7 (128) Buchstaben, Zahlen und Sonderzeichen (Abbildung 18). Jedem Zeichen wird eine siebenstellige Zahlenfolge zugeordnet. Eine solche Folge besteht aus 7 **Bit**, also 7 Stellen, an welchen entweder eine 0 oder eine 1 steht.³⁸

ASCII-Code	Buchstabe	ASCII-Code	Buchstabe
1000001	A	1001110	N
1000010	B	1001111	O
1000011	C	1010000	P
1000100	D	1010001	Q
1000101	E	1010010	R
1000110	F	1010011	S
1000111	G	1010100	T
1001000	H	1010101	U
1001001	I	1010110	V
1001010	J	1010111	W
1001011	K	1011000	X
1001100	L	1011001	Y
1001101	M	1011010	Z

Abbildung 18: Die Grossbuchstaben im ASCII-Code³⁹

Die Verschlüsselung der Zahlen erfolgt immer noch durch Substitution oder Transposition. Nach der Entschlüsselung der Nachricht werden die Zahlen wieder in Buchstaben umgewandelt. Bei einer Transposition können zum Beispiel die erste und die zweite Zahl vertauscht werden, die Dritte und die Vierte und so weiter.⁴⁰ Wollen wir einen Klartext durch Substitution chiffrieren, kann das wie folgt aussehen:

Beispiel. Klartext: buch

Klartext ASCII: 1000010 1010101 1000011 1001000

Schlüssel: GANS

Schlüssel ASCII: 1000111 1000001 1001110 1010011

Die Verschlüsselung erfolgt nach dem folgenden Schema: Sind die Bausteine im Klartext

³⁷Singh 2017.

³⁸Kippenhahn 2012.

³⁹Daten aus Singh 2017.

⁴⁰Singh 2017.

und im Schlüssel gleich, werden sie durch eine 0 im Geheimtext ersetzt, sind sie verschieden, werden sie durch eine 1 ersetzt (Abbildung 19). Zur Dechiffrierung werden derselbe Schlüssel und dasselbe Verfahren angewandt.

Klartext:	1	0	0	0	0	1	0	1	0	1	0	1	0	1	1	0	0	0	0	1	1	1	0	1	0	0
Schlüssel:	1	0	0	0	1	1	1	1	0	0	0	0	1	1	0	0	1	1	1	0	1	0	1	0	0	1
Geheimtext:	0	0	0	0	1	0	1	0	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1

Abbildung 19: Binäre Verschlüsselung durch Substitution

Aufgabe 5. Entschlüssle die Botschaft, die mit dem Schlüssel „WIEN“ chiffriert wurde.

0010010 0001000 0010110 0010111

1973 führte die amerikanische Normenbehörde die Verschlüsselungsart Lucifer als **Data Encryption Standard** (DES) ein. Blöcke von 64 Bit werden nach einem komplizierten Algorithmus verschlüsselt. Zahlen werden in mehreren Runden vertauscht, sie werden in Halbblöcke von 32 Bit zerschnitten, die wiederum substituiert und addiert werden. In den raffinierteren Modi werden die Blöcke dann miteinander noch so verknüpft, dass zwei gleiche Blöcke niemals dieselbe Chiffre ergeben. Die **National Security Agency** (NSA) wollte die Schlüssellänge unbedingt auf 56 Bit beschränken, da sie für den zivilen Gebrauch genügend Sicherheit bot. Damals hatte nämlich noch keine nichtmilitärische Organisation einen genügend leistungsfähigen Computer, um diese Anzahl möglicher Schlüssel in einer vernünftigen Zeit durchzuprobieren. Sie selbst jedoch war gerade noch in der Lage, in den Nachrichtenverkehr einzubrechen.⁴¹

Da ein Computer in Sekundenschnelle ver- und entschlüsseln kann, ermutigte die Einführung von DES Unternehmen, die Verschlüsselung zu nutzen. Heute kann der DES-Algorithmus bereits in weniger als einem Tag geknackt werden, weshalb mächtigere Verschlüsselungen wie der **Advanced Encryption Standard**⁴² (AES) oder der **International Data Encryption Algorithm**⁴³ (IDEA) verwendet werden.⁴⁴

⁴¹Kippenhahn 2012.

⁴²Informationen zur Funktionsweise des AES sind auf der Webseite <http://www.korelstar.de/informatik/aes.html> zu finden.

⁴³Informationen zur Funktionsweise des IDEA sind auf der Webseite <http://atterer.org/uni/crypto.html> zu finden.

⁴⁴Singh 2017.

8 Das Problem der Schlüsselverteilung

Mit der Erfindung des Internets konnten Nachrichten schnell auf der ganzen Welt verschickt werden. Doch ein Problem, das bislang zwar lästig, aber nicht unumgänglich war, schien dieser Entwicklung einen Strich durch die Rechnung zu machen: Die Schlüsselverteilung. Wie sollte ein Europäer einem Amerikaner den Schlüssel sicher übergeben? Wie sollte eine Bank, um die Kunden zu schützen, jedem einen Schlüssel zukommen lassen?⁴⁵

8.1 Alice, Bob und Eve

In den 70er-Jahren wurden Boten zur Überbringung von Schlüsseln eingesetzt. Doch die Sache entwickelte sich zu einem logistischen Albtraum. Es galt als Tatsache, dass zwei Parteien, die - ohne sich zu treffen - sicher miteinander kommunizieren wollten, mindestens einer dritten Person vertrauen mussten, die den Schlüssel überbrachte. Wollte eine Person A (**Alice**) einer Person B (**Bob**) eine Nachricht zukommen lassen, ohne dass eine dritte Person E (**Eve**)⁴⁶ sie lesen konnte, musste sie die Nachricht verschlüsseln. Das tat sie mit einem Schlüssel, der geheim war und der wiederum der Person B sicher übermittelt werden musste. Es war ein scheinbar unlösbare Paradoxon. Doch der 1944 geborene Whitfield Diffie glaubte nicht an die Unlösbarkeit. Er machte das folgende Gedankenexperiment:⁴⁷

Alice schreibt eine Nachricht, legt sie in eine Kiste und verschliesst sie mit ihrem Vorhängeschloss. Die Kiste kann gefahrlos verschickt werden, denn sie ist ja fest verschlossen. Sobald Bob die Box erhält, fügt er zusätzlich sein eigenes Vorhängeschloss hinzu und schickt die Kiste an Alice zurück. Diese entfernt das eigene Schloss und sendet die Box wieder an Bob, welcher sie nun öffnen kann, da nur noch sein eigenes Schloss dranhängt (Abbildung 20).⁴⁸

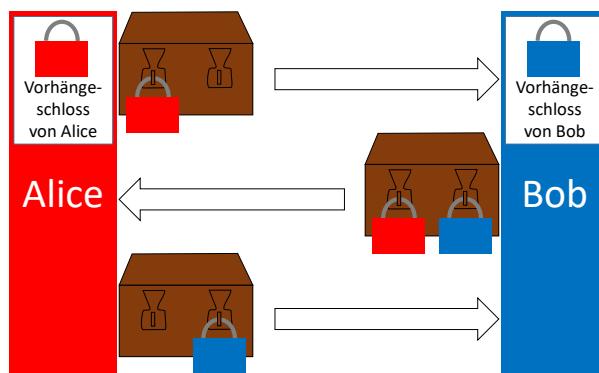


Abbildung 20: Alice kann Bob die Nachricht in der Kiste sicher übermitteln, ohne dass sie sich treffen müssen.

Aufgabe 6. Spiele das Szenario mit der Caesar-Chiffre durch.

Schlüssel 1 (Alice): 4

Schlüssel 2 (Bob): 23

Klartext: Caesar works

Dieses Gedankenexperiment zeigt, dass es möglich ist, jemandem eine Nachricht sicher zu kommen zu lassen, ohne den Schlüssel tauschen zu müssen. In der elektronischen Praxis

⁴⁵Singh 2017.

⁴⁶In der Kryptographie werden oft die Namen Alice, Bob und Eve verwendet. Alice versucht, Bob eine Nachricht zukommen zu lassen, während Eve versucht, die Botschaft abzufangen oder zu belauschen und aufzuzeichnen.

⁴⁷Singh 2017.

⁴⁸Wassmer 2016.

funktioniert das leider nicht, weil bei den Verschlüsselungen, die sicher genug sind, die Reihenfolge eine wichtige Rolle spielt. Bei sicheren Chiffriermethoden gilt der Grundsatz: Die letzte Chiffriermethode muss die erste Dechiffriermethode sein.⁴⁹ Man müsste also die Verschlüsselung, die zuletzt dazugekommen ist, auch zuerst rückgängig machen. Das kann man mit einem Beispiel aus dem Alltag verdeutlichen: Am Morgen zieht man zuerst das T-Shirt und dann den Pullover an. Am Abend muss man aber zuerst den Pullover und danach das T-Shirt wieder ausziehen.

8.2 Modulare Arithmetik

Whitfield Diffie verbündete sich mit Martin Hellman. Die beiden begannen, sich für mathematische Funktionen zu interessieren. Die meisten dieser Funktionen sind **umkehrbar**, das heisst, sie lassen sich ohne weiteres wieder rückgängig machen. Wenn ich $5 * 7 = 35$ rechne, kann ich einfach $35 / 7$ rechnen, um wieder 5 zu erhalten. Das kann man mit einer alltäglichen Situation vergleichen: Wenn man den Lichtschalter kippt, geht das Licht an. Um wieder in die Ausgangssituation zu gelangen, muss man ihn einfach zurückkippen.⁵⁰

Die Kryptographen interessierten sich aber nicht für umkehrbare, sondern für **Einwegfunktionen**. Diese lassen sich zwar leicht anwenden, aber nur mit sehr viel Mühe wieder rückgängig machen. Beim Mischen von blauer und roter Farbe entsteht violett. Das ist einfach. Es ist aber fast unmöglich, die violette Farbe wieder in ihre Bestandteile rot und blau zu zerlegen. Noch schwieriger ist es, ein in die Pfanne geschlagenes Ei wieder zusammenzusetzen.⁵¹

Solche Einwegfunktionen findet man in der **modularen Arithmetik**. Wenn wir um 20 Uhr abends wissen wollen, wie spät es in 5 Stunden ist, finden wir heraus, dass es dann ein Uhr morgens ist. Was haben wir getan? Wir haben $20 + 5$ gerechnet und 25 erhalten. Da es 25 Uhr aber nicht gibt, haben wir 24 Stunden abgezogen und sind auf den *Rest 1* gekommen. Mathematisch wird das so geschrieben:

$$20 + 5 \pmod{24} \equiv 25 \pmod{24} \equiv 1 \pmod{24}$$

Bemerkung. *Mod* wird „modulo“ ausgesprochen. *Modulo 24* heisst, dass der gewählte Modulus 24 ist. Das Symbol \equiv bezeichnet Kongruenz. 25 und 1 sind kongruent oder äquivalent in modulo 24.

Um solche Rechnungen mit höheren Zahlen schneller durchführen zu können, als so oft 24 abzuziehen, bis ein Rest entsteht, der kleiner als 24 ist, müssen wir uns an die Primarschule zurückerinnern. Mussten wir damals $45 / 7$ rechnen, sagten wir, dass das nicht möglich sei. Wir erhielten

$$\frac{45}{7} = \frac{42+3}{7} = \frac{42}{7} \text{ Rest } 3 = 6 \text{ Rest } 3$$

Dieser *Rest 3* ist kongruent zu 45 modulo 7.

$$45 \equiv 3 \pmod{7}$$

Jetzt kann man alle Elemente, die $\pmod{7}$ Rest 3 ergeben, zusammenfassen zu einer Äquivalenzrestklasse.

$$\bar{z} = \{\dots, -4, 3, 10, 17, 24, \dots\}$$

\bar{z} heisst Restklasse 3 ($\pmod{7}$). Alle Elemente dieser Restklasse sind äquivalent in modulo 7. Gerechnet wird dabei immer mit ganzen Zahlen.

⁴⁹Singh 2017.

⁵⁰Beutelspacher 2009.

⁵¹Beutelspacher 2009.

Definition 1. Zwei ganze Zahlen a und b heißen kongruent modulo m , falls m die Differenz $a - b$ teilt, d.h., falls es eine ganze Zahl k gibt, so dass $a - b = k * m$, $m \in \mathbb{N}$, $k \in \mathbb{Z}$. Mathematisch ausgedrückt:

$$a \equiv b \pmod{m}, \quad a, b \in \mathbb{Z}, \quad m \in \mathbb{N}$$

$$\Leftrightarrow m \mid (a - b)$$

$$\Leftrightarrow \exists k \in \mathbb{Z} : a - b = k * m$$

Beispiel.

$$22 \equiv 7 \pmod{5}, \text{ da } 22 - 7 = 15 = k * 5 \text{ (} k = 3 \text{)}$$

$$23 \equiv (-3) \pmod{13}, \text{ da } 23 - (-3) = 26 = k * 13 \text{ (} k = 2 \text{)}$$

Bemerkung. Normalerweise wird die kleinste positive kongruente Zahl modulo m geschrieben.

Beispiel.

$$22 \equiv 2 \pmod{5}$$

$$23 \equiv 10 \pmod{13}$$

Grundsätzlich darf in der modularen Arithmetik normal gerechnet werden. Ausnahme:

Satz 1. Sei $a * b \equiv a * c \pmod{m}$, $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$

$$\text{falls } \text{ggT}(a, m) = 1 \Rightarrow b \equiv c \pmod{m}$$

Es darf also nur durch eine Zahl a dividiert werden, falls der ggT von Modulus m und Divisor a gleich 1 ist.

Beispiel.

$$20 \equiv 30 \pmod{5}$$

- (a) Wenn man auf beiden Seiten durch 10 dividiert, erhält man $2 \equiv 3 \pmod{5}$. Das ist **falsch!**
Grund: $\text{ggT}(10, 5) = 5 \neq 1$.
- (b) Wenn man auf beiden Seiten durch 2 dividiert, erhält man $10 \equiv 15 \pmod{5}$. Das ist **richtig!** Grund: $\text{ggT}(2, 5) = 1$.

Aufgabe 7. Berechne die kleinste positive kongruente Zahl.

(a) $42 \pmod{13}$

(b) $11 \pmod{2}$

(c) $174 \pmod{3}$

(d) $-2 \pmod{9}$

(e) $-50 \pmod{4}$

(f) $1111 \pmod{27}$

Aufgabe 8. Beschreibe, wie mit Hilfe der modularen Arithmetik bestimmt werden kann, ob das Ergebnis einer Addition oder einer Multiplikation zweier Zahlen gerade oder ungerade ist, ohne es auszurechnen. Nimm dazu alle Kombinationen von geraden und ungeraden Ausgangszahlen an.

8.3 Gruppen

Definition 2. Eine Gruppe $\langle \mathbb{G}, \circ, e \rangle$ ist eine algebraische Struktur, die aus einer Menge \mathbb{G} , einer Verknüpfung \circ (bildet eine Zahl der Menge \mathbb{G} wieder auf die Menge \mathbb{G} ab, z. B. Multiplikation) und einem neutralen Element e besteht. Dabei müssen die folgenden Eigenschaften erfüllt sein:

Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in \mathbb{G}$

Neutrales Element: $\exists e \in \mathbb{G} \text{ mit } a \circ e = e \circ a = a \quad \forall a \in \mathbb{G}$

Inverses Element: $\exists \bar{a} \in \mathbb{G}, \text{ so dass } a \circ \bar{a} = \bar{a} \circ a = e \quad \forall a \in \mathbb{G}$

Ist die Operation \circ zudem kommutativ, d.h. es gilt

$$a \circ b = b \circ a \quad \forall a, b \in \mathbb{G},$$

nennt man die Gruppe kommutativ.

Beispiel. $\langle \mathbb{Z}_3^*, *, 1 \rangle$ ist eine kommutative Gruppe. Dabei bedeutet die 3 als Index, dass \mathbb{G} die Menge der Restklassen modulo 3 beinhaltet und der Stern bei \mathbb{Z} bedeutet, dass die 0 weggelassen wird.

$$\mathbb{Z}_3^* = (\mathbb{Z}(\text{mod } 3) \setminus \{0\}) = \{1, 2\}$$

Die Verknüpfung ist die Multiplikation, das neutrale Element ist die Eins. 2 und 1 sind jeweils zu sich selbst invers. Kleinere Gruppen werden oftmals mit Verknüpfungstabellen dargestellt (Abbildung 21).

*	1	2
1	1	2
2	2	1

Abbildung 21: Verknüpfungstabelle der kommutativen Gruppe \mathbb{Z}_3^*

Aufgabe 9. Erstelle eine Verknüpfungstabelle von $\langle \mathbb{Z}_6^*, *, 1 \rangle$ und entscheide, ob es eine Gruppe ist. Mache dasselbe mit $\langle \mathbb{Z}_7^*, *, 1 \rangle$.

Aufgabe 10. Finde das neutrale Element e und entscheide, ob es sich um eine Gruppe handelt. Begründe.

- (a) $\langle \mathbb{N}, +, e \rangle$
- (b) $\langle \mathbb{Z}, +, e \rangle$
- (c) $\langle \mathbb{Z}, *, e \rangle$
- (d) $\langle \mathbb{Q}, *, e \rangle$
- (e) $\langle \mathbb{Q}^*, *, e \rangle$

8.4 Einwegfunktionen

Dass Funktionen in der Modul-Arithmetik zu Einwegfunktionen werden können, wird klar, wenn wir uns folgendes Beispiel anschauen:

Beispiel. Nehmen wir die Funktion

$$f(x) = 3^x.$$

Wenn $x = 2$ ist, wandelt die Funktion f die Zahl 2 in die Zahl 9 um. Auch die Umkehrung ist nicht so schwierig. Ist $f(x) = 81$, nehmen wir einfach den $\log_3(81)$ und erhalten 4 als Resultat für x . Schauen wir uns nun die Funktion in ($\text{mod } 17$) an:

$$f(x) = 3^x (\text{mod } 17)$$

Für $x = 2$ ist das Resultat immer noch 9. Haben wir nur die Basis 3 und das Resultat 13($\text{mod } 17$), wird es schon schwieriger, x zu finden. Wir können raten, zum Beispiel $x = 5$. So erhalten wir $3^5 \equiv 243 \equiv 5 (\text{mod } 17)$. Die Zahl ist zu tief. Wäre es eine normale Funktion, würden wir das nächste Mal höher raten, doch der richtige Wert für x ist vier und damit kleiner als fünf. Das erhaltene Resultat sagt uns also nur, dass die Vermutung falsch ist, klärt jedoch nicht die Frage, ob die richtige Zahl höher oder tiefer liegt. Wir können nur weiter raten.

Definition 3. Die Funktion der Form $b^x (\text{mod } m)$ heisst **diskrete Exponentialfunktion**. Die Umkehrung davon heisst **diskreter Logarithmus**. Erstere lässt sich selbst für grosse Zahlen effizient ausrechnen.

Beispiel. Wir wollen $17^{553} (\text{mod } 31)$ ausrechnen. Dazu suchen wir eine Zahl der Form 17^x , die Modulo 31 den Wert 1 oder (-1) ergibt. Wir finden $17^{30} (\text{mod } 31) \equiv 1$.⁵² Jetzt wird umgeschrieben⁵³:

$$\begin{aligned} 17^{553} (\text{mod } 31) &\equiv 17^{30*18+13} (\text{mod } 31) \equiv (17^{30} (\text{mod } 31))^{18} * 17^{13} (\text{mod } 31) \\ &\equiv 1^{18} * 17^{13} (\text{mod } 31) \equiv 17^{13} (\text{mod } 31) \equiv 3 (\text{mod } 31) \equiv 3 \end{aligned}$$

Aufgabe 11. Berechne:

- (a) $2^{55} (\text{mod } 9)$
- (b) $7^{1223} (\text{mod } 18)$
- (c) $3^{1023} (\text{mod } 10)$

Der Weg, um den diskreten Logarithmus auszurechnen, ist sehr viel langwieriger, da wir nur ausprobieren können. Bei einem sehr hohen Modulus kann das äusserst lange dauern.

8.5 Das Diffie-Hellman-Merkle-Verfahren

Im Jahr 1976 hatte Hellman die Idee für ein Konzept zum Schlüsselaustausch, das auf obengenanntem Prinzip aufbaut. Es erlaubt Alice und Bob, einen Schlüsselaustausch vorzunehmen, ohne sich dazu treffen zu müssen. Mit Farben erklärt, funktioniert das Prinzip so:

Alice und Bob wählen eine gemeinsame Farbe, die sie jedem verraten dürfen und deshalb unverschlüsselt versenden können. Zudem wählen sie beide noch eine geheime Farbe. Nachdem sie je einen Liter geheime mit einem Liter gemeinsamer Farbe vermischt haben, tauschen sie die erhaltenen Farben aus. Falls Eve die Farbe in die Finger bekommt, weiss sie nur eine Ausgangs- und die Zielfarbe. Wie beim diskreten Logarithmus ist es aber praktisch unmöglich, die geheime Farbe zu finden. Kaum haben Alice und Bob die vermischte Farbe des jeweils

⁵²Vorteil: $1^x = 1$, $(-1)^x = 1$ (x gerade) oder $(-1)^x = (-1)$ (x ungerade).

⁵³Die Umschreibung beruht darauf, dass die Potenzgesetze auch in der modularen Arithmetik gelten: $a^{b*c} (\text{mod } d) \equiv (a^b (\text{mod } d))^c (\text{mod } d)$ und $e^{f+g} (\text{mod } h) \equiv e^f (\text{mod } h) * e^g (\text{mod } h)$.

anderen erhalten, kippen sie einen Liter der eigenen geheimen Farbe dazu. Beide haben jetzt ein Gemisch aus einem Liter gemeinsamer Farbe, einem Liter der geheimen eigenen und einem Liter der geheimen Farbe des anderen. Sie haben also eine einheitliche Farbe, die nur sie kennen und können diese als Schlüssel verwenden.⁵⁴

In Wirklichkeit wählen Alice und Bob gemeinsam eine Primzahl p und eine kleinere natürliche Zahl g . Alice wählt zudem eine natürliche Geheimzahl $a \in \mathbb{Z}_p^*$ und Bob macht dasselbe mit einer Zahl $b \in \mathbb{Z}_p^*$. Jetzt berechnen sie die Schlüssel, die jeder sehen darf:

$$Alice : A = g^a \pmod{p}$$

$$Bob : B = g^b \pmod{p}$$

Sie schicken einander die Schlüssel A und B , die nicht geheim gehalten werden müssen, da man aufgrund des diskreten Logarithmus nicht auf die Geheimzahlen schliessen kann. Jetzt berechnen sie K_A beziehungsweise K_B :

$$Alice : K_A = B^a \pmod{p}$$

$$Bob : K_B = A^b \pmod{p}$$

Man kann sehr einfach zeigen, dass $K_A = K_B$ gilt:

Beweis.

$$K_A = B^a \pmod{p} \equiv (g^b)^a \pmod{p} \equiv g^{ba} \pmod{p} \equiv g^{ab} \pmod{p} \equiv (g^a)^b \pmod{p} \equiv A^b \pmod{p} = K_B$$

$$K = K_A = K_B$$

□

Dieses K kann nun als Schlüssel verwendet werden.

Beispiel. $p = 31$, $g = 2$, $a = 3$, $b = 6$

$$A = 2^3 \pmod{31} \equiv 8 \pmod{31} \equiv 8 \pmod{31}$$

$$B = 2^6 \pmod{31} \equiv 64 \pmod{31} \equiv 2 \pmod{31}$$

$$K_A = B^a \pmod{31} \equiv 2^3 \pmod{31} \equiv 8 \pmod{31}$$

$$K_B = A^b \pmod{31} \equiv 8^6 \pmod{31} \equiv 8 \pmod{31}$$

Falls Eve die Zahl $B = 2$ (oder $A = 8$) abfängt, muss sie ausprobieren. Sie weiss nur, dass für $B 2^x \pmod{31} \equiv 2$ gilt. Erster Versuch:

$$2^1 \pmod{31} \equiv 2 \pmod{31}$$

Jetzt hat sie bereits das richtige Resultat erhalten, obwohl eigentlich $b = 6$ gewählt wurde. Das liegt daran, dass $2^x \pmod{31}$ immer entweder 2, 4, 8, 16 oder 1 ergibt (Abbildung 22).

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$2^x \pmod{31}$	2	4	8	16	1	2	4	8	16	1	2	4	8	16	1

Abbildung 22: 2 ist keine Primitivwurzel der zyklischen Gruppe \mathbb{Z}_{31}^* .

Es müssen also nur fünf Möglichkeiten geprüft werden, um auf die richtige Zahl zu kommen. Um diese Schwäche zu beheben, sollte g so gewählt werden, dass für $g^x \pmod{p}$ alle natürlichen Zahlen von 1 bis $(p - 1)$ in Frage kommen. Somit gibt es für jedes Resultat A nur ein mögliches a .

⁵⁴Freiermuth, Hromkovic, Keller, Steffen 2014.

Definition 4. Eine zu $k \in \mathbb{N}$ teilerfremde natürliche Zahl g heisst **Primitivwurzel** oder Generator ($\text{mod } k$), falls gilt

$$a \equiv g^m (\text{mod } k), m \in \mathbb{N} \quad \forall a \in \mathbb{Z}_k^*.$$

Eine Gruppe, für die es eine Primitivwurzel gibt, heisst **zyklische Gruppe**.

Satz 2. Eine Gruppe mit Menge \mathbb{Z}_k^* ist genau dann zyklisch, wenn k von der Form

$$\{k \in \mathbb{N} \mid k \in \{2, 4, p^\alpha, 2 * p^\alpha\}, \alpha \in \mathbb{N}, p \in \mathbb{P} \setminus \{2\}\}$$

ist.⁵⁵

Beispiel. \mathbb{Z}_5^* ist eine zyklische Gruppe, da 5 eine Primzahl ist. Primitivwurzeln sind die Zahlen 2 und 3.

$$\begin{array}{llll} 2^1 \equiv 2 & 2^2 \equiv 4 & 2^3 \equiv 3 & 2^4 \equiv 1 \\ 3^1 \equiv 3 & 3^2 \equiv 4 & 3^3 \equiv 2 & 3^4 \equiv 1 \end{array}$$

Definition 5. Für $n \in \mathbb{N}$ gibt die eulersche Phi-Funktion $\varphi(n)$ die Anzahl natürlicher Zahlen k mit $\text{ggT}(k, n) = 1$, $k \leq n$ an.

Satz 3. Wenn Primitivwurzeln in \mathbb{Z}_k^* existieren, dann gibt es genau $\varphi(\varphi(k))$ in modulo k inkongruente davon. Jede dieser Primitivwurzeln ist modulo k kongruent zu einem Element der Menge

$$\{a^m \mid 1 \leq m \leq \varphi(k) \mid \text{ggT}(m, \varphi(k)) = 1\}$$

wobei a eine Primitivwurzel modulo k ist.⁵⁶

Beispiel. \mathbb{Z}_{11}^* ist eine zyklische Gruppe, da 11 eine Primzahl ist. In dieser Gruppe gibt es $\varphi(\varphi(11)) = \varphi(10) = 4$ Primitivwurzeln. Die Erste finden wir durch Ausprobieren, es ist die 2:

$$\begin{array}{lllll} 2^1 \equiv 2 & 2^2 \equiv 4 & 2^3 \equiv 8 & 2^4 \equiv 5 & 2^5 \equiv 10 \\ 2^6 \equiv 9 & 2^7 \equiv 7 & 2^8 \equiv 3 & 2^9 \equiv 6 & 2^{10} \equiv 1 \end{array}$$

Jetzt suchen wir alle Zahlen m_i mit $\text{ggT}(m_i, \varphi(11)) = \text{ggT}(m_i, 10) = 1$:

$$m_1 = 1 \quad m_2 = 3 \quad m_3 = 7 \quad m_4 = 9$$

Mit $2^{m_i} (\text{mod } 11)$ finden wir alle Primitivwurzeln in \mathbb{Z}_{11}^* .

$$2^1 \equiv 2 \quad 2^3 \equiv 8 \quad 2^7 \equiv 7 \quad 2^9 \equiv 6$$

Die vier Primitivwurzeln in \mathbb{Z}_{11}^* lauten 2, 6, 7 und 8.

Aufgabe 12. Bestimme mit Hilfe des Diffie-Hellmann-Merkle-Verfahrens den Schlüssel $K = K_A = K_B$.

$$p = 23, g = 5, a = 4, b = 13$$

Aufgabe 13. Finde alle Primitivwurzeln für $p = 17$.

Aufgabe 14. Zeige, dass 7 eine Primitivwurzel ($\text{mod } 13$) ist. Nutze dazu eine Tabelle wie die aus Abbildung 22.

Nebst der vorhin genannten Bedingung, dass g eine Primitivwurzel modulo p sein muss, sollte p natürlich möglichst gross gewählt werden, damit die Anzahl möglicher Zahlen für a und b ins Unermessliche steigen. Dieses sogenannte **Diffie-Hellman-Merkle-Verfahren** war zwar ein gewaltiger Sprung nach vorne, ist aber recht umständlich. Um spontan eine verschlüsselte E-Mail zu verschicken, müssen beide Parteien gleichzeitig online sein, da sie beide etwas tun müssen. Der erste Schritt war zwar getan, doch es musste ein effizienteres Verfahren zur Schlüsselverteilung gefunden werden.

⁵⁵Auf der Webseite <https://mathematik.oeunigraz.at/files/2012/07/Existenz-von-Primitivwurzeln.pdf> wird der Satz 2 bewiesen.

⁵⁶Auf der Webseite http://www.mathematik.uni-muenchen.de/~forster/v/zth/inzth_09.pdf wird der Satz 3 bewiesen.

9 Asymmetrische Verschlüsselung

Wieder war Whitfield Diffie der erste mit einer genialen Idee. Er erfand ein Verschlüsselungsverfahren, das mit einem **asymmetrischen Schlüssel** arbeitet. Alle bisher beschriebenen Chiffriervorgänge sind symmetrisch, da die Entschlüsselung einfach die Umkehrung der Verschlüsselung ist und beide Parteien dieselben Informationen zur Verfügung haben. Die Enigma beispielsweise funktionierte mit einem Schlüssel, der die Stellung der Walzen und die Buchstaben, die auf dem Steckbrett verbunden wurden, festlegte. Beide Parteien mussten nur die Maschine so einstellen und mit dem Eintippen der Buchstaben beginnen. Bei einem asymmetrischen Schlüssel kann Alice zwar eine Botschaft verschlüsseln, hat aber nicht die nötigen Informationen, um die Nachricht wieder zu entschlüsseln.⁵⁷

9.1 Funktionsweise

Damit Alice eine Botschaft an Bob schicken kann, muss dieser zuerst seinen **öffentlichen Schlüssel** (public key) für alle zugänglich machen. Alice kann die Botschaft mit diesem Schlüssel verschlüsseln und nur Bob kann ihre Nachricht mit seinem **privaten Schlüssel** (private key) wieder entschlüsseln. Alle anderen, die nur den öffentlichen Schlüssel kennen, einschließlich Alice, haben keine Möglichkeit, die Nachricht wieder zu dechiffrieren, da dieser Schlüssel dazu nicht taugt. Wenn wir zum Beispiel der Vorhängeschlösser zurückkehren, heißt das, dass Bob unzählige Kopien seines Vorhängeschlosses herstellt und sie mit der Post verteilt, den Schlüssel aber geheim hält. Jeder, der ein solches Schloss hat, kann ihm eine Nachricht schreiben, sie in eine Kiste legen und mit dem Schloss sichern. Aber nur Bob kann das Schloss und die Kiste öffnen und die Nachricht lesen, weil er als einziger einen Schlüssel hat. Ein grosser Vorteil dieses Verfahrens ist, dass das Hin und Her, wie es beim Diffie-Hellman-Merkle-Verfahren notwendig ist, überflüssig wird.⁵⁸

Diffie hatte zwar die asymmetrische Verschlüsselung entwickelt, das konkrete Beispiel dafür fehlte ihm aber noch. Gefunden werden musste eine Einwegfunktion mit einer Hintertür. Die Funktion musste effizient berechenbar sein, die Umkehrfunktion durfte es nicht sein. Mit einer bestimmten Information sollte die Bestimmung des Klartextes trotzdem schnell aus dem Geheimtext möglich sein.⁵⁹

9.2 RSA

Im April 1977 suchte Ron Rivest, der eine Publikation von Diffie gelesen hatte, zusammen mit Leonard Adleman und Adi Shamir nach einer ebensolchen Einwegfunktion. Das gefundene Verschlüsselungsverfahren sollte ARS heißen, nach den Namen der drei Freunde. Doch Adleman fand, dass sein Name nicht auftauchen sollte, da er zu wenig dazu beigetragen habe. Sie einigten sich darauf, das „A“ am Schluss zu schreiben und so heißt diese Verschlüsselungsmethode heute **RSA**.⁶⁰

RSA basiert auf dem Problem der Faktorisierung. Dabei soll eine natürliche Zahl n in ihre Primfaktoren zerlegt werden. Bis heute ist noch kein Algorithmus bekannt, der diese Aufgabe effizient lösen kann. Die Multiplikation von zwei Primzahlen p und q zu einer natürlichen Zahl n ist somit eine Einwegfunktion, die aber leider keine Hintertür besitzt. Deswegen ist das nur der Grundbaustein für RSA.

⁵⁷Singh 2017.

⁵⁸Beutelspacher 2009.

⁵⁹Freiermuth, Hromkovic, Keller, Steffen 2014.

⁶⁰Singh 2017.

9.2.1 Die eulersche Phi-Funktion für Primzahlen

Satz 4. Für $p \in \mathbb{P}$ ist $\varphi(p) = p - 1$

Beweis. Jede Primzahl p ist nur durch die Zahlen 1 und p teilbar. Für jede natürliche Zahl a mit $a < p$ gilt deswegen

$$\text{ggT}(a, p) = 1.$$

Da jede Zahl durch sich selbst teilbar ist und es genau $p - 1$ natürliche Zahlen gibt, die kleiner sind als p , gilt $\varphi(p) = p - 1$. \square

Satz 5. (Multiplikativität)⁶¹ Für zwei teilerfremde natürliche Zahlen s und t gilt:

$$\varphi(s * t) = \varphi(s) * \varphi(t)$$

Insbesondere gilt für $n = p * q$, $p, q \in \mathbb{P}$:

$$\varphi(n) = \varphi(p * q) = \varphi(p) * \varphi(q) = (p - 1) * (q - 1)$$

Beispiel. $\varphi(15) = \varphi(3 * 5) = \varphi(3) * \varphi(5) = 2 * 4 = 8$

9.2.2 Euklidischer Algorithmus

Der **euklidische Algorithmus**⁶² wird zur effizienten Berechnung des grössten gemeinsamen Teilers (ggT) zweier Zahlen a und b benutzt. Dabei geht man wie folgt vor:

Seien a und b zwei natürliche Zahlen mit $a > b$. Solange $a \neq 0$ ist, sollen die Operationen (1) und (2) wiederholt werden.

- (1) Ersetze a durch $a(\text{mod } b)$
- (2) Vertausche die Zahlen a und b

Der $\text{ggT}(a, b)$ ist die am Ende erhaltene Zahl b .

Um den Überblick zu behalten, wird der Rechenweg detailliert aufgeschrieben. Wichtig wird die Schreibweise vor allem beim erweiterten euklidischen Algorithmus (Seite 32).

Beispiel. $\text{ggT}(765, 675)$

$$765 = 1 * 675 + 90 \quad (a = 765, b = 675, a(\text{mod } b) = 90)$$

$$675 = 7 * 90 + 45 \quad (a = 675, b = 90, a(\text{mod } b) = 45)$$

$$90 = 2 * 45 + 0 \quad (a = 90, b = 45, a(\text{mod } b) = 0)$$

$$\text{ggT}(765, 675) = 45$$

Aufgabe 15. Berechne mit Hilfe des euklidischen Algorithmus.

- (a) $\text{ggT}(234, 566)$
- (b) $\text{ggT}(357, 131)$
- (c) $\text{ggT}(728, 1339)$

⁶¹Die Multiplikativität der eulerschen Phi-Funktion wird auf der folgenden Webseite bewiesen:

http://www.mathematik.uni-muenchen.de/~forster/v/zth/inzth_07.pdf

⁶²Der euklidische Algorithmus wird auf Seite 47 bewiesen.

9.2.3 Erweiterter euklidischer Algorithmus

Um das inverse Element d zu $e \pmod{\varphi(n)}$ herauszufinden, wird der **erweiterte euklidische Algorithmus** verwendet. Dabei gilt:

$$d * e \pmod{\varphi(n)} \equiv 1$$

Beispiel. $p = 31$, $q = 71$, $n = 2201$, $e = 37$

$$\varphi(n) = (p-1) * (q-1) = 30 * 70 = 2100$$

Zuerst suchen wir den ggT von $\varphi(n)$ und e mit Hilfe des euklidischen Algorithmus:

$$2100 = 56 * 37 + 28 \Rightarrow 28 = 2100 - 56 * 37$$

$$37 = 1 * 28 + 9 \Rightarrow 9 = 37 - 1 * 28$$

$$28 = 3 * 9 + 1 \Rightarrow 1 = 28 - 3 * 9$$

Jetzt wird von unten nach oben substituiert, so dass wir am Ende eine Gleichung der Form

$$1 = x * \varphi(n) + d * e$$

erhalten:

$$1 = 28 - 3 * 9$$

$$1 = 28 - 3 * (37 - 1 * 28) = 28 - 3 * 37 + 3 * 28 = 4 * 28 - 3 * 37$$

$$1 = (-3) * 37 + 4 * (2100 - 56 * 37) = (-3) * 37 + 4 * 2100 - 224 * 37$$

$$1 = (-227) * 37 + 4 * 2100$$

Jetzt haben wir die Zahl 1 mit Hilfe der Summanden $4 * \varphi(n)$ und $-227 * e$ geschrieben.

$$1 = 4 * 2100 - 227 * 37$$

Modulo $\varphi(n)$ ergibt der Summand mit der Zahl $\varphi(n)$ als Faktor immer null, also bleibt $(mod 2100)$ nur noch

$$-227 * 37 \pmod{2100} \equiv 1.$$

Das ist die Bedingung für das inverse Element d :

$$d * e \pmod{\varphi(n)} \equiv 1$$

Der letzte Faktor vor e ist deswegen das inverse Element d . Hier ist d negativ, nämlich -227 . Um einen positiven Wert zu erhalten, rechnen wir:

$$-227 \pmod{\varphi(n)}, \text{ also } -227 \pmod{2100} \equiv 1873 = d$$

Aufgabe 16. $e = 59$, $n = 222$. Finde das inverse Element d zu e modulo $\varphi(n)$.⁶³

Mit diesem Wissen kann nun RSA erläutert werden.

⁶³Auf der Webseite <https://rechneronline.de/primfaktoren/> kann man eine (nicht allzu grosse) Zahl eingeben, die dann in ihre Primfaktoren zerlegt wird.

9.2.4 Anleitung RSA

- (a) Wähle zwei Primzahlen p und q
- (b) Berechne $n = p * q$
- (c) Berechne den Wert der eulerschen Phi-Funktion $\varphi(n) = (p - 1) * (q - 1)$
- (d) Wähle eine natürliche Zahl e mit $\text{ggT}(e, \varphi(n)) = 1$
- (e) Berechne d , das inverse Element zu $e(\text{mod } \varphi(n))$, mithilfe des erweiterten euklidischen Algorithmus. Es gilt: $d * e(\text{mod } \varphi(n)) \equiv 1$
- (f) Öffentlicher Schlüssel: (n, e)
- (g) Privater Schlüssel: (n, d)

Der öffentliche Schlüssel wird veröffentlicht, so dass jeder, der eine verschlüsselte Nachricht verschicken will, darauf Zugriff hat. Der Klartext wird mit Hilfe der ASCII-Tabelle in eine binäre Zahl m umgewandelt. Der eigentliche Verschlüsselungsvorgang funktioniert wie folgt:

Verschlüsselung (message m zu cipher c):

$$c \equiv m^e (\text{mod } n)$$

Entschlüsselung (cipher c zu message m):

$$m \equiv c^d (\text{mod } n)$$

Bemerkung. In der Praxis wird für e oftmals $2^{16} + 1$ gewählt. Die Message m muss kleiner sein als die Zahl n , weshalb sie unter Umständen in kleineren Blöcken verschlüsselt werden muss.

Beispiel. Wir haben von Alice eine verschlüsselte Nachricht c erhalten. Zu finden sind der private Schlüssel (d, n) und der Klartext m .

Unsere Zahlen:

$$p = 43, q = 47, e = 19, c = 74$$

$$n = p * q = 43 * 47 = 2021$$

$$\varphi(n) = (p - 1) * (q - 1) = 42 * 46 = 1932$$

$$d = ?, m = ?$$

Wir rechnen d aus mit dem erweiterten euklidischen Algorithmus:

$$1932 = 101 * 19 + 13 \Rightarrow 13 = 1932 - 101 * 19$$

$$19 = 1 * 13 + 6 \Rightarrow 6 = 19 - 1 * 13$$

$$13 = 2 * 6 + 1 \Rightarrow 1 = 13 - 2 * 6$$

Rückwärts eingesetzt:

$$1 = 13 - 2 * 6$$

$$1 = 13 - 2 * (19 - 1 * 13) = 13 - 2 * 19 + 2 * 13 = 3 * 13 - 2 * 19$$

$$1 = (-2) * 19 + 3 * (1932 - 101 * 19) = (-2) * 19 + 3 * 1932 - 303 * 19 = 3 * 1932 - 305 * 19$$

Modulo 1932:

$$1 \equiv 3 * 1932 - 305 * 19 (\text{mod } 1932) \equiv (-305) * 19 (\text{mod } 1932) \equiv 1627 * 19 (\text{mod } 1932)$$

Demnach ist $d = 1627$.

Zuletzt wird m ausgerechnet:

$$m = c^d (\text{mod } n) \equiv 74^{1627} (\text{mod } 2021) \equiv 1371$$

Aufgabe 17. $p = 11$, $q = 5$ und $e = 7$. Finde d und n und verschlüssle die Zahl 15 mit RSA.⁶⁴

Aufgabe 18. $p = 83$, $q = 113$, $e = 29$. Entschlüssle die Zahl 4029.

9.2.5 Korrektheit RSA

Satz 6. (Satz von Euler)⁶⁵ Für $\text{ggT}(a, n) = 1$ gilt: $a^{\varphi(n)} \pmod{n} \equiv 1$

Damit gilt auch der „Kleine Satz von Fermat“⁶⁶:

Satz 7. $a^{(p-1)} \pmod{p} \equiv 1$, $p \in \mathbb{P}$

Wir wollen zeigen, dass man, wenn man die verschlüsselte Nachricht $m^e \pmod{n}$ mit $(m^e)^d \pmod{n}$ entschlüsselt und davon die ursprüngliche Nachricht m abzieht, null erhält.

$$(m^e)^d - m \pmod{n} \equiv 0$$

Beweis RSA.

$$e * d \pmod{(p-1)*(q-1)} \equiv 1 \quad (1)$$

$$\exists k \in \mathbb{Z} \text{ mit } e * d = k * (p-1) * (q-1) + 1 \quad (2)$$

Betrachte (\pmod{p}) :

$$(m^e)^d - m \equiv m^{ed} - m \equiv m^{k*(p-1)*(q-1)+1} - m \quad (3)$$

$$\equiv (m^{(p-1)})^{k*(q-1)} * m - m \quad (4)$$

$$\equiv 1^{k*(q-1)} * m - m \equiv m - m \equiv 0 \quad (5)$$

(1) Nach Konstruktion

(2) Folgt direkt aus (1) nach Definition modulo

(3) Aus (2)

(4) Potenzregel

(5) Kleiner Satz von Fermat, $1^x = 1$

Das heisst, p teilt $(m^e)^d - m$, weil $(m^e)^d - m \pmod{p} \equiv 0$. Für (\pmod{q}) gilt dasselbe (Beweis analog). Insgesamt teilen p und q $(m^e)^d - m$, also teilt $p * q$ auch $(m^e)^d - m$. Daraus folgt, dass

$$(m^e)^d - m \pmod{p * q} \equiv (m^e)^d - m \pmod{n} \equiv 0$$

□

⁶⁴Auf der Website <http://www.wolframalpha.com/> kann die Funktion „powermod[a,b,c]“ benutzt werden, um $a^b \pmod{c}$ schnell zu berechnen.

⁶⁵Der „Satz von Euler“ wird auf folgender Webseite bewiesen:

<https://www.informatik.hu-berlin.de/de/forschung/gebiete/algorithmenII/Lehre/ws05/kryptot1/skript/kap6.pdf>

⁶⁶Der „Kleine Satz von Fermat“ wird auf Seite 48 bewiesen.

9.2.6 Das RSA-Rätsel

Im August 1977 wurde mit der Veröffentlichung des RSA-Algorithmus im „Scientific American“ ein Rätsel gestellt:

Gegeben ist:

$$\begin{aligned} n = & 114 \ 381 \ 625 \ 757 \ 888 \ 867 \ 669 \ 235 \ 779 \ 976 \ 146 \ 612 \ 010 \ 218 \ 296 \ 721 \\ & 242 \ 362 \ 562 \ 561 \ 842 \ 934 \ 706 \ 935 \ 245 \ 733 \ 897 \ 830 \ 597 \ 123 \ 563 \ 958 \ 705 \ 058 \ 989 \\ & 075 \ 147 \ 599 \ 290 \ 026 \ 879 \ 543 \ 541 \end{aligned}$$

$$\begin{aligned} c = & 96 \ 869 \ 613 \ 754 \ 622 \ 061 \ 477 \ 140 \ 922 \ 254 \ 355 \ 882 \ 905 \ 759 \ 991 \ 124 \ 574 \ 319 \\ & 847 \ 695 \ 120 \ 930 \ 816 \ 298 \ 225 \ 145 \ 708 \ 356 \ 931 \ 476 \ 622 \ 883 \ 989 \ 628 \ 013 \ 391 \ 990 \\ & 551 \ 829 \ 945 \ 157 \ 815 \ 154 \end{aligned}$$

$$e = 9 \ 007$$

Man entschlüssle die Botschaft c .

Damals ergab sich eine grobe Abschätzung, dass es etwa $4 * 10^{16}$ (40 000 000 000 000 000) Jahre dauern würde, um n zu faktorisieren. Nach einem Zusammenschluss von 1600 Rechnern dauerte es aber nur ein halbes Jahr, bis klar war:

$$\begin{aligned} p = & 3 \ 490 \ 529 \ 510 \ 847 \ 650 \ 949 \ 147 \ 849 \ 619 \ 903 \ 898 \ 133 \ 417 \ 764 \ 638 \ 493 \ 387 \ 849 \\ & 390 \ 820 \ 577 \end{aligned}$$

$$\begin{aligned} q = & 32 \ 769 \ 132 \ 993 \ 266 \ 709 \ 549 \ 961 \ 988 \ 190 \ 834 \ 461 \ 413 \ 177 \ 642 \ 967 \ 992 \ 942 \ 539 \\ & 798 \ 288 \ 533 \end{aligned}$$

Die verschlüsselte Botschaft konnte nun leicht ermittelt werden.⁶⁷ Sie lautete:

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE
(Die magischen Worte sind zimperliche Lämmergeier)⁶⁸

Obwohl diese Nachricht ohne die Kenntnis des privaten Schlüssels dechiffriert wurde, muss man sich keine Sorgen über die Sicherheit von RSA machen. Diese basiert darauf, dass es sehr lange Zeit dauert, bis man von der Zahl n auf die Primfaktoren p und q kommt. Für wichtige Geschäfte wird heute die Zahl n mit mindestens 600 Dezimalstellen gewählt. Aus p und q kann ein Computer diese Zahl in kürzester Zeit ausrechnen. Um n jedoch zu faktorisieren, würden selbst die vereinten Kräfte von 100 Millionen aktueller Computer über tausend Jahre benötigen. Die einzige Chance, RSA unsicher zu machen, wäre die Entwicklung von besseren Algorithmen zur Primfaktorzerlegung. Allerdings sind Mathematiker schon seit dem Bekanntwerden, dass jede natürliche Zahl eine eindeutige Primfaktorzerlegung besitzt⁶⁹, an der Lösungssuche zur effizienten Primfaktorzerlegung.⁷⁰

⁶⁷Engleder, Kowalski, Lorenz o.D.

⁶⁸Engleder, Kowalski, Lorenz o.D.

⁶⁹Fundamentalsatz der Arithmetik

⁷⁰Singh 2017.

9.3 Die asymmetrische Verschlüsselung und der Geheimdienst

Britischen Regierungsquellen zufolge waren es die Mitarbeiter des **Government Communications Headquarters** (GCHQ), einer hochgeheimen Organisation nach dem zweiten Weltkrieg, die die Public-Key-Kryptographie zuerst erfunden haben. Der Funk machte in den späten sechziger Jahren das Problem der Schlüsselverteilung aktueller denn je. Deshalb wurde James Ellis damit beauftragt, Lösungen zu suchen. Dabei stiess er auf einen Artikel, in dem ein unbekannter Autor erklärte, wie man Telefongespräche abhörsicher machen konnte. Der Empfänger sollte ein Rauschen auf die Leitung legen. Nach Erhalt der Nachricht würde das Rauschen wieder abgezogen und die Nachricht verständlich abgespielt. Der Einzige, der das tun konnte, war der Empfänger, da er die Störung ja selbst verursacht hatte. Die offensichtlichen Nachteile verhinderten die Einführung der Methode, doch die Idee der Verschlüsselung von Seiten des Empfängers war damit in der Welt. Ellis bewies innerhalb von Minuten mit Hilfe eines Existenzsatzes,⁷¹ dass das Chiffrieren ohne Schlüsselaustausch auch bei gewöhnlichen Verschlüsselungsmethoden funktioniert. Diesen Ansatz hatte er schon Jahre vor Diffie. Die Arbeitsgruppe des GCHQ machte sich daran, die Idee konkret umzusetzen und schliesslich stiess der Mathematiker Clifford Cocks auf die Variante, die vier Jahre später als RSA noch ein zweites Mal gefunden wurde. Damals gab es noch keine Computer, die leistungsfähig genug gewesen wären, um RSA zu nutzen und weil Cocks für eine militärische Organisation arbeitete, war er zu Geheimhaltung verpflichtet. Schweigend musste er mit ansehen, wie statt seiner die drei Amerikaner Rivest, Shamir und Adleman berühmt wurden.⁷²

⁷¹Ein Existenzsatz beweist, dass ein Problem gelöst werden kann, ohne zu sagen, wie diese Lösung aussieht.

⁷²Singh 2017.

10 Hybride Verschlüsselung

RSA hat das Problem der Schlüsselverteilung gelöst, in dem es die geheime Übermittlung eines Schlüssels überflüssig machte. Man muss nur einen öffentlichen Schlüssel publizieren, den jeder sehen darf und mit dem jeder verschlüsseln kann. Entschlüsseln kann aber nur derjenige mit dem privaten Schlüssel. Der Nachteil dabei ist, dass viel leistungsfähigere Computer benötigt werden, als bei symmetrischen Verfahren. Je nach Länge der Botschaft dauert der Vorgang mehrere Minuten. Symmetrische Chiffrierungen benötigen zwar trotz sehr hoher Sicherheit weniger Rechenleistung, setzen aber die Kenntnis des Schlüssels für alle Parteien voraus. Um die Vorteile beider Verfahren nutzen zu können, wird heute eine Kombination verwendet, die **hybride Verschlüsselung**. Ein bekanntes Beispiel ist das von Hans Zimmermann entwickelte Verfahren **Pretty Good Privacy** (PGP).⁷³

10.1 Pretty Good Privacy

Bei der Verschlüsselung mit PGP in ihrer ursprünglichen Form werden der symmetrische IDEA- und der asymmetrische RSA-Algorithmus verwendet. Alice verschlüsselt zuerst die Nachricht mit IDEA und schickt sie an Bob. Damit dieser weiß, wie er sie entschlüsseln muss, sucht sie sich Bobs öffentlichen RSA-Schlüssel heraus, verschlüsselt damit den IDEA-Schlüssel, der wesentlich kürzer ist als die Nachricht, und schickt ihm auch diesen. Bob muss, um die Nachricht lesen zu können, nur den IDEA-Schlüssel mit seinem privaten RSA-Schlüssel entschlüsseln und kann danach die eigentliche Botschaft mit dem eben erhaltenen Schlüssel dechiffrieren. Eve ist machtlos, sie kann nur die verschlüsselten Botschaften abfangen, lesen geht nicht.⁷⁴

10.1.1 Elektronische Unterschrift

Wie kann Bob sicher sein, dass die Nachricht wirklich von Alice stammt und nicht von Eve abgefangen und durch eine andere ersetzt wurde? Das wäre möglich, weil Eve ja ebenfalls den öffentlichen Schlüssel von Bob kennt. Hier zeigt sich, wie genial das RSA-Verfahren ist. Damit kann nämlich eine elektronische Unterschrift gemacht werden.⁷⁵ Zuerst wird mithilfe einer Hashfunktion der **Hashwert** (kurz: Hash) der Nachricht generiert. Hashfunktionen bilden beliebig lange Eingaben nach einem bestimmten Algorithmus auf einen Datenraum fester Größe ab. Eine einfache Hashfunktion ist zum Beispiel die einstellige Quersumme, die jede Zahl auf eine einstellige Ziffer abbildet. Dabei kann es auch sein, dass zwei unterschiedliche Datensätze denselben Hashwert ergeben (Kollision). Das verhindert, dass man vom Hash auf die ursprüngliche Eingabe schließen kann. Wichtig ist zudem, dass der Hash sensibel auf kleine Unterschiede reagiert. Die Funktion muss aber deterministisch sein, das heißt, dass dieselbe Eingabe immer zum gleichen Hashwert führt. Dieser ist wie ein **Fingerabdruck** der Daten, auf die die Hashfunktion angewendet wurde.⁷⁶

Den Hash h der Nachricht signiert Alice mit ihrem privaten Schlüssel d .

$$s \equiv h^d \pmod{n}$$

Weil $(h^d)^e \pmod{n} \equiv h$ gilt, kann Bob den signierten Hashwert s mit dem öffentlichen Schlüssel e von Alice entschlüsseln.

$$h \equiv s^e \pmod{n}$$

⁷³Singh 2017.

⁷⁴Gallenbacher 2017.

⁷⁵Gallenbacher 2017.

⁷⁶Schmitz 2017.

Damit erhält er wieder den Hashwert und kann sich jetzt sicher sein, dass er von Alice stammt, weil er mit ihrem privaten Schlüssel signiert wurde, den nur sie kennt. Um zu überprüfen, ob die Nachricht tatsächlich von Alice stammt, erzeugt Bob den Hash der Nachricht und vergleicht ihn mit dem von Alice signierten Wert. Sind sie identisch, wurde die Nachricht tatsächlich von Alice verfasst.⁷⁷

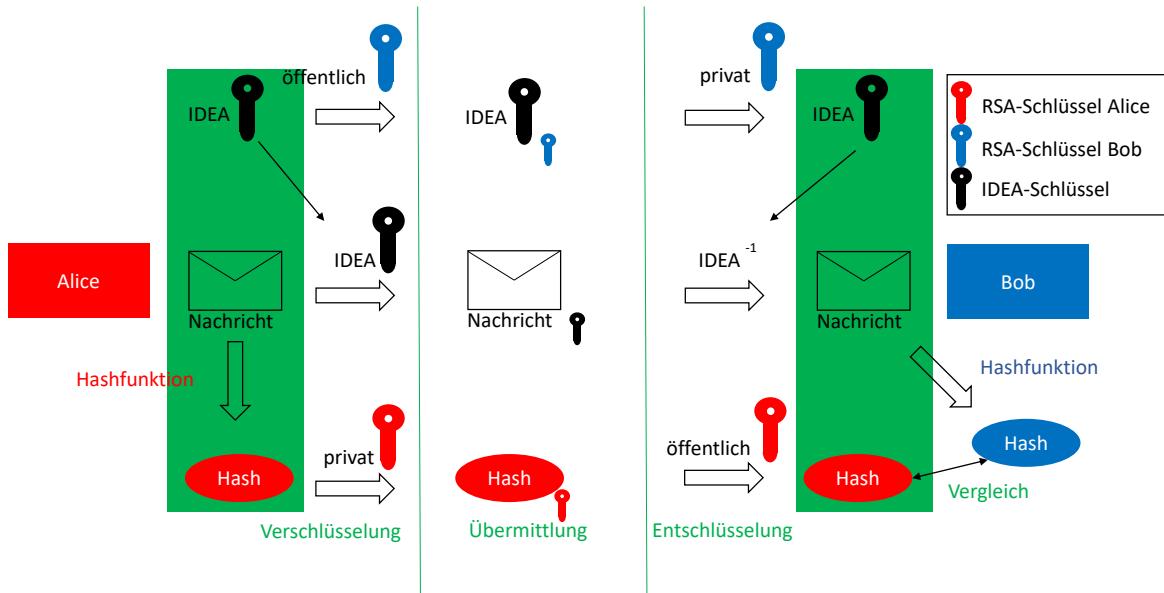


Abbildung 23: Pretty Good Privacy

Aufgabe 19. Alice hat dir eine Nachricht c geschickt. Sie ist mit Caesar verschlüsselt. Den Schlüssel k für Caesar hast du ebenfalls erhalten. Er ist mit deinem öffentlichen RSA-Schlüssel verschlüsselt. Zudem hat sie den Hashwert h_A generiert und mit ihrem privaten RSA-Schlüssel signiert. Berechne deinen privaten Schlüssel, bestimme k und die Nachricht m , generiere den Hashwert h von m und vergleiche ihn mit dem von Alice.

Verschlüsseltes $k = 243$

$c = DOOHVRN$

Signiertes $h_A = 262$

Öffentlicher Schlüssel Alice $= (N, E) = (341, 11)$

Deine Zahlen: $p = 37, q = 163, e = 5$

Dein privater Schlüssel $= (n, d) = (6031, ?)$

$d = ?, k = ?, m = ?, h = ?$

Bemerkung. Den Hashwert h generierst du in Aufgabe 19, indem du bei der Nachricht m die Buchstaben $a = 1, b = 2, \dots, z = 26$ setzt und die Zahlen addierst. Die erhaltene Zahl rechnest du ($\text{mod } 11$) und erhältst den Hashwert h .

Beispiel. Der Hashwert von „du“ ist: $d + u = (4 + 21)(\text{mod } 11) \equiv 3$

10.2 Zertifikate

Ein Fall wurde bisher ausgeklammert: Es kann sein, dass der Betrug schon zu Beginn geschah. Vielleicht hat Eve bereits die Nachricht von Alice abgefangen, in der sie den öffentlichen Schlüssel von Bob verlangt hat und hat ihr stattdessen in Bobs Namen den eigenen Schlüssel

⁷⁷Kippenhahn 2012.

untergejubelt. Jetzt kann Eve sich als Bob ausgeben und in seinem Namen alle Nachrichten abfangen, lesen und beantworten. Alice realisiert nichts, weil sie ja davon ausgeht, mit Bob zu kommunizieren. Damit das nicht geschieht, gibt es sogenannte **Zertifikate**. Ein Zertifikat ist wie ein Personalausweis und enthält den Namen und den öffentlichen Schlüssel des Inhabers. Dazu gehört immer die Zertifizierungsstelle (CA), die es ausgestellt hat und ein Ablaufdatum (Abbildung 24).⁷⁸

Feld	Wert
Signaturhashalgorithmus	sha256
Aussteller	QuoVadis EV SSL ICA G1, Quo...
Gültig ab	Freitag, 27. April 2018 18:56:59
Gültig bis	Montag, 27. April 2020 19:06:00
Antragsteller	www.migros.ch, MITS, Migros ...
Öffentlicher Schlüssel	RSA (2048 Bits)
Parameter für öffentlichen ...	05 00
Zugriff auf Stelleninformationen	11 Stelleninformationszurri...

30	82	01	0a	02	82	01	01	00	c8	dc	75	a7	0a
56	fe	6c	e7	d5	4d	85	42	69	bf	b6	aa	7f	7e
9c	e8	8c	e0	68	01	2e	06	70	19	a5	24	c3	03
85	9d	a8	33	0d	c1	08	a2	30	49	ff	0d	26	7b
c0	fe	99	35	25	27	b0	17	9d	b9	5e	5f	ca	ce
c7	67	0b	18	d7	6e	69	09	b5	6b	02	11	50	69
0a	e9	7c	64	78	96	09	32	b5	d5	72	b8	e0	00
ea	9b	f3	83	3a	53	7b	88	2c	84	27	56	95	ae
b1	fc	2b	81	f3	ee	57	9f	24	78	02	fc	76	dc

Abbildung 24: Teil des Zertifikats der Webseite <https://www.migros.ch/de.html>

Je nach Geschäftsart können noch weitere Merkmale enthalten sein. Signiert wird der Hashwert des Zertifikats mit dem privaten Schlüssel der Zertifizierungsstelle und diese bürgt für die Richtigkeit der Informationen auf dem Zertifikat. Jeder kann bei der Zertifizierungsstelle das Zertifikat von Alice oder Bob verlangen und weil es von der CA verifiziert ist, kann er sich sicher sein, dass er mit jener Person kommuniziert, auf welche das Zertifikat ausgestellt ist. Die Zertifikate der wichtigsten Zertifizierungsstellen sind auf dem Computer vorinstalliert. Man kann ihnen vertrauen.⁷⁹ Damit sind jetzt drei wichtige Dinge gewährleistet:

- **Vertraulichkeit**; niemand kann sich unerlaubt Informationen beschaffen
 - Übergabe des IDEA-Schlüssels mit RSA
 - Verschlüsselung mit IDEA
- **Integrität**; jede Datenmanipulation wird bemerkt
 - Übermittlung des signierten Hashwertes der Nachricht
- **Authentizität**; Identitätsnachweis des Kommunikationspartners
 - Von der CA signiertes Zertifikat mit Personalien und öffentlichem RSA-Schlüssel⁸⁰

⁷⁸Gallenbacher 2017.

⁷⁹Kippenhahn 2012.

⁸⁰Wolfram Alpha LLC 2017.

Will Alice eine Mail an Bob schreiben, funktioniert das so: Der Computer fragt die oberste Zertifizierungsstelle nach dem Zertifikat von Bob. Diese leitet ihn an eine Tochter-CA weiter. Die CA schickt Alice das Zertifikat von Bob und den mit dem eigenen privaten Schlüssel signierten Hashwert. Alice entschlüsselt den Hashwert des Zertifikats mit dem öffentlichen Schlüssel der CA und vergleicht ihn mit dem selbst erzeugten Hash. Danach schreibt sie ihre Nachricht und verschlüsselt sie mit IDEA. Den Schlüssel zu IDEA chiffriert sie mit Bobs öffentlichem Schlüssel, den sie auf dem Zertifikat findet, und sendet ihn zusammen mit der chiffrierten Nachricht an Bob. Zuletzt generiert sie den Hashwert der Nachricht, signiert ihn mit ihrem privaten Schlüssel und lässt auch diesen ihrem Kommunikationspartner zukommen.⁸¹

Bob entschlüsselt den IDEA-Schlüssel mit seinem privaten Schlüssel. Danach dechiffriert er die Nachricht mit dem Schlüssel, den er eben entschlüsselt hat. Er berechnet den Hashwert der Nachricht und vergleicht ihn mit dem Hashwert, den ihm Alice geschickt hat. Diesen dechiffriert er mit dem öffentlichen Schlüssel von Alice, den er ihrem Zertifikat entnommen hat.⁸²

Beim E-Banking und Online-Bestellungen geschieht all dies mittlerweile automatisch. Wird etwas mit der Kreditkarte bezahlt, verschlüsselt der Computer die PIN und die Kartennummer, ohne dass man etwas dafür tun muss. Für die Verschlüsselung von privaten Nachrichten kann man sich ein Programm herunterladen, das sie auf Knopfdruck verschlüsselt oder signiert.⁸³ So kann heute jeder verschlüsseln und signierte Meldungen verschicken.

⁸¹Gallenbacher 2017.

⁸²Gallenbacher 2017.

⁸³Ein solches Programm kann man auf der Webseite <https://www.gpg4win.de/> herunterladen.

11 Rückblick

In meiner Maturaarbeit habe ich viele verschiedene Verschlüsselungsmethoden von der Antike bis in die heutige Zeit erklärt. Angefangen bei der Steganographie, dem Verschleiern der Existenz der Nachricht, über die Chiffrierung mittels Transposition bis hin zur monoalphabetischen Verschlüsselung durch Substitution. Nach einem kurzen Ausflug in die Welt der Kryptoanalytiker habe ich über die polyalphabetische Verschlüsselung und das unknackbare One-Time-Pad geschrieben. Auch die Enigma ist in dieser Arbeit zu finden. Die Computer verhalfen der Kryptologie zu einer schnelleren Entwicklung und eröffneten neue Möglichkeiten. Das Diffie-Hellman-Merkle-Verfahren war die erste Lösung für das Schlüsselaustauschproblem. RSA als asymmetrische Verschlüsselung und deren Anwendung in der hybriden Verschlüsselung bilden den letzten Teil der vorliegenden Arbeit.

Es war mir ein Anliegen, die wichtigsten Schritte in der Geschichte der Verschlüsselung nachvollziehbar und logisch aufzuschreiben. Natürlich muss man sehr aufmerksam lesen, um alles zu verstehen, doch die Arbeit sollte mit gewissen mathematischen Vorkenntnissen selbsterklärend sein.

Bereits im Frühling begann ich mit dem Schreiben eines Grundgerüstes. Dadurch hatte ich genügend Zeit für die Überarbeitung, worüber ich sehr froh bin. Die Anwendungsaufgaben habe ich selbst entwickelt. Alle Grafiken ohne Quellenangabe sind meine eigenen Kreationen. Wie von meiner Betreuungsperson vorgegeben, habe ich die Maturaarbeit auf dem Programm „LaTex“ geschrieben. Es kostete mich einige Zeit und Mühe, bis ich vernünftig damit arbeiten konnte. Trotzdem war es eine tolle Erfahrung, ein neues Textverarbeitungsprogramm kennenzulernen.

In dieser Arbeit ist natürlich nur eine Auswahl an Verschlüsselungsverfahren zu finden, es gibt noch zahlreiche weitere. Die Arbeit bietet einen Einblick in die Welt der Kryptologie, welche im Moment ein sehr aktuelles Thema ist. Die fortschreitende Globalisierung und der technologische Fortschritt zwingen uns dazu, immer stärkere Algorithmen zur Verschlüsselung zu nutzen. Angst um die Sicherheit der Daten im Netz sollte man aber erst haben, wenn in der Zeitung die Schlagzeile „Problem der Primfaktorzerlegung gelöst“ auftaucht.

Zum Schluss bedanke ich mich bei allen, die mir bei meiner Maturaarbeit in irgendeiner Form geholfen haben. Ein spezieller Dank geht dabei an Herrn Jorma Wassmer für die Betreuung dieser Arbeit. Ich erlaube ihm gerne, meine Arbeit im Rahmen des Mathematikunterrichts einzusetzen.

Bemerkung. *TQENLFKLCCDPZGANQAHVSUJUPDVLCHPISIDNIGHYAGBNTDFLCBU.*⁸⁴

⁸⁴Verschlüsselt mit dem One-Time-Pad.

Abbildungsverzeichnis

1	Steganographie	6
2	Die Skytale	7
3	Die „Gartenzauntransposition“	7
4	Klar- und Geheimtextalphabet der Caesar-Chiffre	8
5	Verschlüsselung mit Schlüsselwort und Schlüsselbuchstabe	8
6	Buchstabenhäufigkeit in der deutschen Sprache	10
7	Die häufigsten Bigramme in der deutschen Sprache	10
8	Buchstabenhäufigkeit im Geheimtext	10
9	Häufigkeit der Bigramme, die mit dem Geheimtextbuchstaben „S“ beginnen	11
10	Verschlüsselung mit zwei Geheimtextalphabeten	13
11	Verschlüsselung mit Vigenère	14
12	Vigenère-Quadrat	14
13	Homophone Verschlüsselung	15
14	Das One-Time-Pad	16
15	Die Chiffrierscheibe	18
16	Schaltplan einer Enigma	19
17	Die Enigma	20
18	Die Grossbuchstaben in ASCII-Code	21
19	Binäre Verschlüsselung durch Substitution	22
20	Sichere Nachrichtenübermittlung ohne Treffen	23
21	Verknüpfungstabelle der kommutativen Gruppe \mathbb{Z}_3^*	26
22	\mathbb{Z}_{31}^*	28
23	Pretty Good Privacy	38
24	Zertifikat	39

Literatur

Bücher

- Beutelspacher, A. (2009). *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. 9. Aufl. Wiesbaden.
- Freiermuth, K., Hromkovic, J., Keller, L., Steffen, B. (2014). *Einführung in die Kryptologie: Lehrbuch für Unterricht und Selbststudium*. 2. Aufl. Wiesbaden.
- Gallenbacher, J. (2017). *Abenteuer Informatik: IT zum Anfassen für alle von 9 bis 99 – vom Navi bis Social Media*. 4. Aufl. Wiesbaden.
- Kippenhahn, R. (2012). *Verschlüsselte Botschaften: Geheimschrift, Enigma und digitale Codes*. 2. Aufl. Reinbek bei Hamburg.
- Singh, S. (2017). *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. 14. Aufl. München.

Internetliteratur

- Didym (9. Apr. 2018). *Unihockey*. URL: <https://de.wikipedia.org/w/index.php?title=Unihockey&action=history> (Aufgerufen am 20.04.2018).
- Engleider, M., Kowalski, E., Lorenz, M. (o.D.). *Das Verschlüsselungsverfahren nach Rivest, Shamir und Adleman*. URL: <http://www.univie.ac.at/NuHAG/FEICOURS/ws0203/PROSEM/RSA.doc> (Aufgerufen am 25.06.2018).
- Schäfer, K., Putsch, B., Träumner, M., Caplan, C., John, C. (Juli 2002). *Enigma*. URL: <http://www.matheprisma.uni-wuppertal.de/Module/Enigma/index.htm> (Aufgerufen am 11.08.2018).
- Schmitz, P. (23. Aug. 2017). *Was ist ein Hash?* URL: <https://www.security-insider.de/was-ist-ein-hash-a-635712/> (Aufgerufen am 26.06.2018).
- Schöchtel, G. (o.D.). *Der kleine Satz von Fermat*. URL: <https://wwwdid.mathematik.tu-darmstadt.de/mathezirkel/content/download/Der%20kleine%20Satz%20von%20Fermat2.pdf> (Aufgerufen am 11.08.2018).
- Wolfram Alpha LLC (10. März 2017). *Kryptologie, Kryptographie und Kryptoanalyse*. URL: <http://www.kryptowissen.de/schutzziele.php> (Aufgerufen am 11.08.2018).

Unveröffentlichte Quellen

- Wassmer, J. (2016). *Kryptologie: Unterricht im Schwerpunkt fach Anwendungen der Mathematik*. Köniz.

Abbildungen

Homophone Verschlüsselung, Abbildung 13 (Seite 15):

Brätz, M. (13. Juli 2015). URL: <https://www.kryptographiespielplatz.de/index.php?aG=739f6e7032f25b44f223f2791b2ae15bdb1c9bb4> (Aufgerufen am 11.08.2018).

Die Skytale, Abbildung 2 (Seite 7):

Hebisch, U. (7. Apr. 2010). URL: <http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/skytale.html> (Aufgerufen am 10.08.2018).

Beispielzertifikat Migros, Abbildung 24 (Seite 39):

Migros-Genossenschafts-Bund (2018). URL: <https://www.migros.ch/de.html> (Aufgerufen am 12.08.2018).

Die Enigma, Abbildung 17 (Seite 20 und Titelseite):

Nassiri, A. (o.D.). URL: <https://www.faithandleadership.com/edgar-moore-transforming-yesterdays-tools-war-museum-relics> (Aufgerufen am 10.08.2018).

Die Chiffrierscheibe, Abbildung 15 (Seite 18 und Titelseite):

Südwestrundfunk (2005). URL: <https://www.kindernetz.de/infonetz/laenderundkulturen/geheimschriften/-/id=25340/property=download/nid=22494/1vpb4gn/index.pdf> (Aufgerufen am 10.08.2018).

Weiterführende Literatur

Atterer, R. (22. Mai 2010). *IDEA*. URL: <http://atterer.org/uni/crypto.html> (Aufgerufen am 03.08.2018).

Forster, O. (6. Juni 2004a). *Einführung in die Zahlentheorie*. URL: http://www.mathematik.uni-muenchen.de/~forster/v/zth/inzth_09.pdf (Aufgerufen am 25.08.2018).

Forster, O. (24. Mai 2004b). *Einführung in die Zahlentheorie*. URL: http://www.mathematik.uni-muenchen.de/~forster/v/zth/inzth_07.pdf (Aufgerufen am 25.08.2018).

Hamann, K. (2002). *AES*. URL: <http://www.korelstar.de/informatik/aes.html> (Aufgerufen am 03.08.2018).

Humboldt-Universität Berlin (o.D.). *Zahlentheoretische Grundlagen*. URL: <https://www.informatik.hu-berlin.de/de/forschung/gebiete/algorithmenII/Lehre/ws05/krypto1/skript/kap6.pdf> (Aufgerufen am 25.08.2018).

Kniely, M. (Nov. 2009). *Existenz von Primitivwurzeln*. URL: <https://mathematik.oehunigraz.at/files/2012/07/Existenz-von-Primitivwurzeln.pdf> (Aufgerufen am 25.08.2018).

Schäfer, K., Putsch, B., Träumner, M., Caplan, C., John, C. (Juli 2002). *Enigma*. URL: <http://www.matheprisma.uni-wuppertal.de/Module/Enigma/index.htm> (Aufgerufen am 11.08.2018).

Nützliche Webseiten

Hier kann man sich ein Programm für die Verschlüsselung von privaten Nachrichten herunterladen:

Herzog, B. u. a. (2006). URL: <https://www.gpg4win.de/> (Aufgerufen am 26.07.2018).

Ein Rechner, der eine beliebige (nicht allzu grosse) natürliche Zahl in seine Primfaktoren zerlegt:

Kummer, J. (2007). URL: <https://rechneronline.de/primfaktoren/> (Aufgerufen am 11.08.2018).

Ein Rechner, der die modulare Arithmetik beherrscht:

Wolfram Alpha LLC (2009). URL: <http://www.wolframalpha.com/> (Aufgerufen am 11.08.2018).

12 Anhang

12.1 Zeichenerklärung

Im Folgenden ist eine kurze Zusammenstellung der in dieser Arbeit verwendeten mathematischen Zeichen zu finden.

$ggT(a, b)$	Grösster gemeinsamer Teiler der Zahlen a und b , $a, b \in \mathbb{Z}$ (Die grösste natürliche Zahl, durch die sich zwei ganze Zahlen a und b ohne Rest teilen lassen)
\exists	Es existiert...
\forall	Für alle...
\mathbb{N}	Menge der natürlichen Zahlen ($\mathbb{N} = \{1, 2, 3, \dots\}$)
\mathbb{Z}	Menge der ganzen Zahlen ($\mathbb{Z} = \{\dots, (-2), (-1), 0, 1, 2, \dots\}$)
\setminus	Ohne... ($\mathbb{N} \setminus \{1\}$ ist die Menge der Natürlichen Zahlen ohne die Eins, also die Menge $\{2, 3, \dots\}$)
\in	Ist Element der Menge... ($a \in \mathbb{N}$ heisst, dass a eine natürliche Zahl ist.)
\mathbb{Q}	Menge der rationalen Zahlen, d.h. aller Zahlen, die sich in einem Bruch der Form $\frac{a}{b}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$ darstellen lassen.
\mathbb{P}	Menge der Primzahlen
\Leftrightarrow	Genau dann, wenn...
$ $	Teilt... ($a b$ heisst, dass die Zahl a die Zahl b teilt) oder: Mit der Eigenschaft... ($\{2z \mid z \in \mathbb{Z}\}$ ist die Menge der geraden ganzen Zahlen)
\Rightarrow	Daraus folgt, dass... ($a * b = c \Rightarrow a = \frac{c}{b}$)
\circ	Verknüpfung (Verknüpft zwei Elemente miteinander, z. B. durch Multiplikation oder Addition)
\mathbb{Z}_k^*	Menge der ganzen Zahlen modulo k ohne die Null ($\mathbb{Z}(mod k) \setminus \{0\} = \{1, 2, \dots, k\}$)
$OEdA$	Ohne Einschränkung der Allgemeinheit

12.2 Euklidischer Algorithmus - Beweis

OEdA $a \geq b$

Es sei

$$a = q_1 * b + r_1$$

$$b = q_2 * r_1 + r_2$$

$$r_1 = q_3 * r_2 + r_3$$

$$r_2 = q_4 * r_3 + r_4$$

...

$$r_{i-2} = q_i * r_{i-1} + r_i$$

$$r_{i-1} = q_{i+1} * r_i + 0$$

$$r_i = 0 * 0 + r_i$$

Satz 8. Der letzte nicht triviale Rest r_i im euklidschen Algorithmus liefert den ggT der beiden ganzen Zahlen a und b .

Beweis. Wir zeigen zuerst $\text{ggT}(a, b) = \text{ggT}(b, r_1)$. Dafür setzen wir $q_1 =: k$ und damit

$$r_1 = a - kb, \text{ggT}(a, b) =: t_1 \text{ und } \text{ggT}(b, a - kb) =: t_2.$$

Jetzt zeigen wir $\text{ggT}(a, b) \leq \text{ggT}(b, a - kb)$.

$$t_1 \mid a \Rightarrow t_1 * n = a, n \in \mathbb{Z}$$

$$t_1 \mid b \Rightarrow t_1 * m = b, m \in \mathbb{Z}$$

$$a - kb = t_1 * n - k * t_1 * m = t_1 * (n - km)$$

Weil n, k und m ganze Zahlen sind, ist $(n - km)$ auch eine ganze Zahl und damit ist t_1 Teiler der Zahl $a - kb$. Weil t_1 der $\text{ggT}(a, b)$ ist, teilt er auch b und ist deswegen $\leq \text{ggT}(b, a - kb)$. Jetzt zeigen wir $\text{ggT}(a, b) \geq \text{ggT}(b, a - kb)$.

$$t_2 \mid b \Rightarrow t_2 * p = b, p \in \mathbb{Z}$$

$$t_2 \mid a - kb \Rightarrow t_2 * q = a - kb, q \in \mathbb{Z}$$

$$a = t_2 * q + k * b = t_2 * q + k * t_2 * p = t_2 * (q - kp)$$

Weil q, k und p ganze Zahlen sind, ist $(q - kp)$ auch eine ganze Zahl und damit ist t_2 Teiler der Zahl a . Weil t_2 der $\text{ggT}(b, a - kb)$ ist, teilt er auch b und ist deswegen $\leq \text{ggT}(a, b)$.

Insgesamt haben wir damit gezeigt, dass $\text{ggT}(a, b) = \text{ggT}(b, a - kb)$ gilt. Das gilt immer für zwei aufeinanderfolgende Zeilen, bis im letzten Schritt gilt:

$$\text{ggT}(a, b) = \text{ggT}(r_i, 0) = r_i$$

□

Bemerkung. Beweisführung nach Wassmer 2016.

12.3 Kleiner Satz von Fermat - Beweis

Um den „Kleinen Satz von Fermat“ zu beweisen, benötigen wir zuerst einen Hilfssatz.

Satz 9 (Hilfssatz). *Beim Teilen der ersten $(p-1)$ Vielfachen von $a \in \mathbb{N}$, d. h. der Zahlen $1a, 2a, 3a, \dots, (p-1)a$, durch $p \in \mathbb{P}$ mit $\text{ggT}(a, p) = 1$ tritt jeder Rest $r_i = 1, 2, 3, \dots, (p-1)$ genau einmal auf.*

$$i * a \equiv r_i \pmod{p}, r_i \in \{1, 2, 3, \dots, (p-1)\}$$

Beweis Hilfssatz. Indirekter Beweis.

Wären zwei der Reste gleich, also $r_i = r_j$ mit $i \neq j$, $i, j \in \{1, 2, 3, \dots, (p-1)\}$, würde $(\text{mod } p)$ aus $i * a \equiv r_i$ und $j * a \equiv r_j$ direkt $i * a \equiv j * a$ folgen. Wegen $\text{ggT}(a, p) = 1$ wäre $i \equiv j$ und damit $i = j$, weil $i, j < p$. Widerspruch. \square

Satz 10 (Kleiner Satz von Fermat). *Für $p \in \mathbb{P}$ und $a \in \mathbb{N}$ mit $\text{ggT}(a, p) = 1$ gilt*

$$a^{p-1} \equiv 1 \pmod{p}$$

Beweis. Multipliziert man alle möglichen Reste modulo p ($i * a \equiv r_i \pmod{p}$), erhält man:

$$1a * 2a * 3a * \dots * (p-1)a \equiv r_1 * r_2 * r_3 * \dots * r_{p-1} \pmod{p}$$

Mit $r_i \neq r_j$, $i, j \in \{1, 2, 3, \dots, (p-1)\}$ folgt:

$$1 * 2 * 3 * \dots * (p-1) * a^{p-1} \equiv 1 * 2 * 3 * \dots * (p-1) \pmod{p}$$

Wegen $\text{ggT}(r_i, p) = 1$ dürfen wir kürzen und erhalten damit:

$$a^{p-1} \equiv 1 \pmod{p}$$

\square

Bemerkung. Beweisführung nach Schöchtel o.D.

12.4 Lösungen zu den Aufgaben

Aufgabe 1. Das ergibt den Satz „Das ist die erste Aufgabe“.

```
D S S D E R T A F A E
A I T I E S E U G B
```

Aufgabe 2. Gaius Julius Caesar

Aufgabe 3. Aus „so einfach, so schoen“ wird der Geheimtext „MH KEGAVXZ, MH MXZHKG“.

Bemerkung. Achtung: ö ist als oe zu verschlüsseln.

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

Aufgabe 4.

Klartext	k	r	y	p	t	o	l	o	g	i	e
<i>Schlüssel</i>	M	A	T	U	R	A	M	A	T	U	R
Geheimtext	W	R	R	J	K	O	X	O	Z	C	V

Aufgabe 5. WIEN: 1010111 1001001 1000101 1001110

Geheimtext ASCII:	0	0	1	0	0	1	0	0	0	0	1	0	0	1	1	0	0	0	1	0	1	1	1	1
Schlüssel ASCII:	1	0	1	0	1	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1	1	1	0	0
Klartext ASCII:	1	0	0	0	1	0	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	0	0
Klartext:	E																S							Y

Nachricht: 1000101 1000001 1010011 1011001: EASY

Aufgabe 6.

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
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

Abbildung 25: Verschlüsselungstafel Alice

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
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

Abbildung 26: Verschlüsselungstafel Bob

Alice verschlüsselt: caesarworks zu GEIWEVASVOW und sendet die Botschaft an Bob.

Bob verschlüsselt: geiwevasvow zu DBFTBSXPSLT und schickt die Cipher zurück zu Alice.

Alice entschlüsselt: DBFTBSXPSLT zu zxbpxotlohp und sendet die Nachricht ein letztes Mal an Bob.

Bob entschlüsselt: ZXBPXOTLOHP zu caesarworks

Aufgabe 7.

- (a) $42 \pmod{13} \equiv 3$
- (b) $11 \pmod{2} \equiv 1$
- (c) $174 \pmod{3} \equiv 0$
- (d) $-2 \pmod{9} \equiv 7$
- (e) $-50 \pmod{4} \equiv 2$
- (f) $1111 \pmod{27} \equiv 4$

Aufgabe 8. Alle natürlichen Zahlen a mit

$$a \pmod{2} \equiv 0$$

sind gerade. Jede natürliche Zahl b ist ungerade, falls

$$b \pmod{2} \equiv 1$$

gilt. Mit modulo 2 kann deswegen gezeigt werden, dass die Addition zweier gerader Zahlen wieder eine gerade Zahl gibt.

$$0 + 0 \pmod{2} \equiv 0$$

Die Addition von zwei ungeraden Zahlen führt zu einer geraden Zahl:

$$1 + 1 \pmod{2} \equiv 2 \pmod{2} \equiv 0$$

Die Addition einer geraden und einer ungeraden Zahl führt zu einer ungeraden Zahl:

$$0 + 1 \pmod{2} \equiv 1 + 0 \pmod{2} \equiv 1$$

Multiplikation:

Gerade Zahl und gerade Zahl:

$$0 * 0 \pmod{2} \equiv 0$$

Ungerade Zahl und ungerade Zahl:

$$1 * 1 \pmod{2} \equiv 1$$

Ungerade Zahl und gerade Zahl:

$$1 * 0 \pmod{2} \equiv 0 * 1 \pmod{2} \equiv 0$$

Aufgabe 9.

Die Verknüpfungstabelle zeigt, dass $\langle \mathbb{Z}_6^*, *, 1 \rangle$ keine Gruppe ist. Die Zahlen 2, 3 und 4 haben kein inverses Element. Zudem kommt bei der Verknüpfung von $2 * 3$ und $3 * 4$ die Null vor, was nicht der Fall sein darf, da sie mit dem Stern eliminiert werden soll. $\langle \mathbb{Z}_7^*, *, 1 \rangle$ ist eine Gruppe. $e = 1$. Die inversen Elemente sind 1 mit 1, 2 mit 4, 3 mit 5 und 6 mit sich selbst.

.	1	2	3	4	5	.	1	2	3	4	5	6
1	1	2	3	4	5	1	1	2	3	4	5	6
2	2	4	0	2	4	2	2	4	6	1	3	5
3	3	0	3	0	3	3	3	6	2	5	1	4
4	4	2	0	4	2	4	4	1	5	2	6	3
5	5	4	3	2	1	5	5	3	1	6	4	2
6	6	5	4	3	2	6	6	5	4	3	2	1

Abbildung 27: links: $\langle \mathbb{Z}_6^*, *, 1 \rangle$, rechts: $\langle \mathbb{Z}_7^*, *, 1 \rangle$

Aufgabe 10.

- (a) $\langle \mathbb{N}, +, e \rangle$ Keine Gruppe. (Keine inversen Elemente und kein neutrales Element, da die Null nicht in der Menge \mathbb{N} enthalten ist.)
- (b) $\langle \mathbb{Z}, +, 0 \rangle$ Gruppe. $e = 0$. Das inverse Element von a ist jeweils $(-a)$.
- (c) $\langle \mathbb{Z}, *, 1 \rangle$ Keine Gruppe. (Keine inversen Elemente.)
- (d) $\langle \mathbb{Q}, *, 1 \rangle$ Keine Gruppe. (0 hat kein inverses Element, da $0 * a = 0$ ergibt.)
- (e) $\langle \mathbb{Q}^*, *, 1 \rangle$ Gruppe. $e = 1$. Das inverse Element von a ist jeweils $\frac{1}{a}$.

Aufgabe 11.

- (a) $2^{55} \pmod{9} \equiv 2^{3*18+1} \pmod{9} \equiv (2^3)^{18} * 2^1 \pmod{9} \equiv (-1)^{18} * 2 \pmod{9} \equiv 2 \pmod{9}$
- (b) $7^{1223} \pmod{18} \equiv 7^{3*407+2} \pmod{18} \equiv (7^3)^{407} * 7^2 \pmod{18} \equiv 1^{407} * 49 \pmod{18} \equiv 13 \pmod{18}$
- (c) $3^{1023} \pmod{10} \equiv 3^{2*511+1} \pmod{10} \equiv (3^2)^{511} * 3^1 \pmod{10} \equiv (-1)^{511} * 3 \pmod{10} \equiv (-3) \pmod{10} \equiv 7 \pmod{10}$

Aufgabe 12.

$$\begin{aligned} p &= 23, g = 5, a = 4, b = 13 \\ A &= g^a \pmod{p} \equiv 5^4 \pmod{23} \equiv 4 \pmod{23} \\ B &= g^b \pmod{p} \equiv 5^{13} \pmod{23} \equiv 21 \pmod{23} \\ K_A &= B^a \pmod{23} \equiv 21^4 \pmod{23} \equiv 16 \pmod{23} \\ K_B &= A^b \pmod{23} \equiv 4^{13} \pmod{23} \equiv 16 \pmod{23} \end{aligned}$$

Aufgabe 13. Modulo 17 gibt es genau $\varphi(\varphi(17)) = \varphi(16) = 8$ Primitivwurzeln. Die erste findet man durch ausprobieren: 3. Demnach sind alle Primitivwurzeln mit $3^m \pmod{17}$ zu finden, wobei $ggT(m, \varphi(17)) = ggT(m, 16) = 1$ gelten muss. Für m kommen deshalb nur die Zahlen 1, 3, 5, 7, 9, 11, 13 und 15 in Frage. Durch einsetzen erhält man:

$$\begin{aligned} 3^1 \pmod{17} &\equiv 3 \\ 3^3 \pmod{17} &\equiv 10 \\ 3^5 \pmod{17} &\equiv 5 \\ 3^7 \pmod{17} &\equiv 11 \\ 3^9 \pmod{17} &\equiv 14 \\ 3^{11} \pmod{17} &\equiv 7 \\ 3^{13} \pmod{17} &\equiv 12 \\ 3^{15} \pmod{17} &\equiv 6 \end{aligned}$$

Die Primitivwurzeln zum Modulus 17 sind also 3, 5, 6, 7, 10, 11, 12 und 14.

Aufgabe 14.

x	1	2	3	4	5	6	7	8	9	10	11	12	13
$7^x \pmod{13}$	7	10	5	9	11	12	6	3	8	4	2	1	7

Aufgabe 15.

(a) $ggT(234, 566)$

$$\begin{aligned} 566 &= 2 * 234 + 98 \\ 234 &= 2 * 98 + 38 \\ 98 &= 2 * 38 + 22 \\ 38 &= 1 * 22 + 16 \\ 22 &= 1 * 16 + 6 \\ 16 &= 2 * 6 + 4 \\ 6 &= 1 * 4 + 2 \\ 4 &= 2 * 2 + 0 \\ ggT(234, 566) &= 2 \end{aligned}$$

(b) $ggT(357, 131)$

$$\begin{aligned} 357 &= 2 * 131 + 95 \\ 131 &= 1 * 95 + 36 \\ 95 &= 2 * 36 + 23 \\ 36 &= 1 * 23 + 13 \\ 23 &= 1 * 13 + 10 \\ 13 &= 1 * 10 + 3 \\ 10 &= 3 * 3 + 1 \\ 3 &= 3 * 1 + 0 \\ ggT(357, 131) &= 1 \end{aligned}$$

(c) $ggT(728, 1339)$

$$\begin{aligned} 1339 &= 1 * 728 + 611 \\ 728 &= 1 * 611 + 117 \\ 611 &= 5 * 117 + 26 \\ 117 &= 4 * 26 + 13 \\ 26 &= 2 * 13 + 0 \\ ggT(728, 1339) &= 13 \end{aligned}$$

Aufgabe 16. $e = 59$, $n = 222$

Wir berechnen $\varphi(n)$:

Primfaktorzerlegung: $n = 2 * 3 * 37$

$$\varphi(n) = \varphi(2 * 3 * 37) = \varphi(2) * \varphi(3) * \varphi(37) = (2 - 1) * (3 - 1) * (37 - 1) = 1 * 2 * 36 = 72$$

$$72 = 1 * 59 + 13 \Rightarrow 13 = 72 - 1 * 59$$

$$59 = 4 * 13 + 7 \Rightarrow 7 = 59 - 4 * 13$$

$$13 = 1 * 7 + 6 \Rightarrow 6 = 13 - 1 * 7$$

$$7 = 1 * 6 + 1 \Rightarrow 1 = 7 - 1 * 6$$

Rückwärts eingesetzt:

$$1 = 7 - 1 * 6$$

$$1 = 7 - 1 * (13 - 1 * 7) = (-1) * 13 + 2 * 7$$

$$1 = (-1) * 13 + 2 * (59 - 4 * 13) = (-1) * 13 + 2 * 59 - 8 * 13 = 2 * 59 - 9 * 13$$

$$1 = 2 * 59 - 9 * (75 - 1 * 59) = 2 * 59 - 9 * 75 + 9 * 59 = 11 * 59 - 9 * 75$$

$$d = 11$$

Aufgabe 17. $p = 11, q = 5, e = 7, n = 55$

$$\varphi(n) = (p-1) * (q-1) = 40$$

$$40 = 5 * 7 + 5 \Rightarrow 5 = 40 - 5 * 7$$

$$7 = 1 * 5 + 2 \Rightarrow 2 = 7 - 1 * 5$$

$$5 = 2 * 2 + 1 \Rightarrow 1 = 5 - 2 * 2$$

Rückwärts eingesetzt:

$$1 = 5 - 2 * 2$$

$$1 = 5 - 2 * (7 - 1 * 5) = 5 - 2 * 7 + 2 * 5 = 3 * 5 - 2 * 7$$

$$1 = (-2) * 7 + 3 * (40 - 5 * 7) = (-2) * 7 + 3 * 40 - 15 * 7 = (-17) * 7 + 3 * 40$$

$$d = (-17) \pmod{40} \equiv 23 \pmod{40}$$

$$d = 23$$

$$c = m^e \pmod{n} \equiv 15^7 \pmod{55} = 5$$

Aufgabe 18. $p = 83, q = 113, e = 29, n = 83 * 113 = 9379$

$$\varphi(n) = (p-1) * (q-1) = 9184$$

$$9184 = 316 * 29 + 20 \Rightarrow 20 = 9184 - 316 * 29$$

$$29 = 1 * 20 + 9 \Rightarrow 9 = 29 - 1 * 20$$

$$20 = 2 * 9 + 2 \Rightarrow 2 = 20 - 2 * 9$$

$$9 = 4 * 2 + 1 \Rightarrow 1 = 9 - 4 * 2$$

Rückwärts eingesetzt:

$$1 = 9 - 4 * 2$$

$$1 = 9 - 4 * (20 - 2 * 9) = 9 - 4 * 20 + 8 * 9 = 9 * 9 - 4 * 20$$

$$1 = (-4) * 20 + 9 * (29 - 1 * 20) = (-4) * 20 + 9 * 29 - 9 * 20 = (-13) * 20 + 9 * 29$$

$$1 = 9 * 29 - 13 * (9184 - 316 * 29) = 9 * 29 - 13 * 9184 + 4108 * 29 = 4117 * 29 - 13 * 9184$$

$$d = 4117$$

$$m = c^d \pmod{n} \equiv 4029^{4117} \pmod{9379} \equiv 472$$

Aufgabe 19.

Verschlüsseltes $k = 243$

$c = DOOHVRN$

Signiertes $h_A = 262$

Öffentlicher Schlüssel Alice $= (N, E) = (341, 11)$

Deine Zahlen: $p = 37, q = 163, e = 5$

Dein privater Schlüssel $= (n, d) = (6031, ?)$

$d = ?, k = ?, m = ?, h = ?$

Zuerst bestimmen wir den privaten Schlüssel d :

$$p = 37, q = 163, e = 5, n = 37 * 163 = 6031$$

$$\varphi(n) = (p-1) * (q-1) = 5832$$

$$5832 = 1166 * 5 + 2 \Rightarrow 2 = 5832 - 1166 * 5$$

$$5 = 2 * 2 + 1 \Rightarrow 1 = 5 - 2 * 2$$

Rückwärts eingesetzt:

$$1 = 5 - 2 * 2$$

$$1 = 5 - 2 * (5832 - 1166 * 5) = 5 - 2 * 5832 + 2332 * 5 = 2333 * 5 - 2 * 5832$$

$$d = 2333$$

Jetzt können wir den verschlüsselten Caesar-Schlüssel k_v entschlüsseln:

$$k = k_v^d \pmod{n} \equiv 243^{2333} \pmod{6031} \equiv 3$$

Damit sind wir in der Lage, die Nachricht m auszurechnen. Die Verschiebung um $k = 3$ Buchstaben gibt uns die Tabelle in Abbildung 28.

So wird aus der Chiffre $c = D O O H V R N$ der Klartext $m = \text{alles ok}$.

Zur Berechnung des Hashwertes können wir wieder die Tabelle zu Hilfe nehmen: Die Zahl, die den jeweiligen Buchstaben ersetzt, steht darüber. $h = (1 + 12 + 12 + 5 + 19 + 15 + 11) \pmod{11} \equiv 75 \pmod{11} \equiv 9$

Den Hashwert von Alice h_A berechnen wir aus dem signierten Hashwert h_s :

$$h_A = h_s^E \pmod{N} \equiv 262^{11} \pmod{341} \equiv 9$$

Wir wissen nun:

$$d = 2333$$

$$k = 3$$

$$m = \text{alles ok}$$

$$h = 9$$

$$h_A = 9$$

Weil die Hashwerte h und h_A übereinstimmen, wissen wir, dass die Nachricht unverfälscht von Alice zu uns übermittelt wurde. Alles OK.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	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
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 28: Oben: Zahl, durch welche der Klartextbuchstabe beim Kreieren des Hashwertes ersetzt wird,

Mitte: Klartextalphabet,

Unten: Geheimtextalphabet