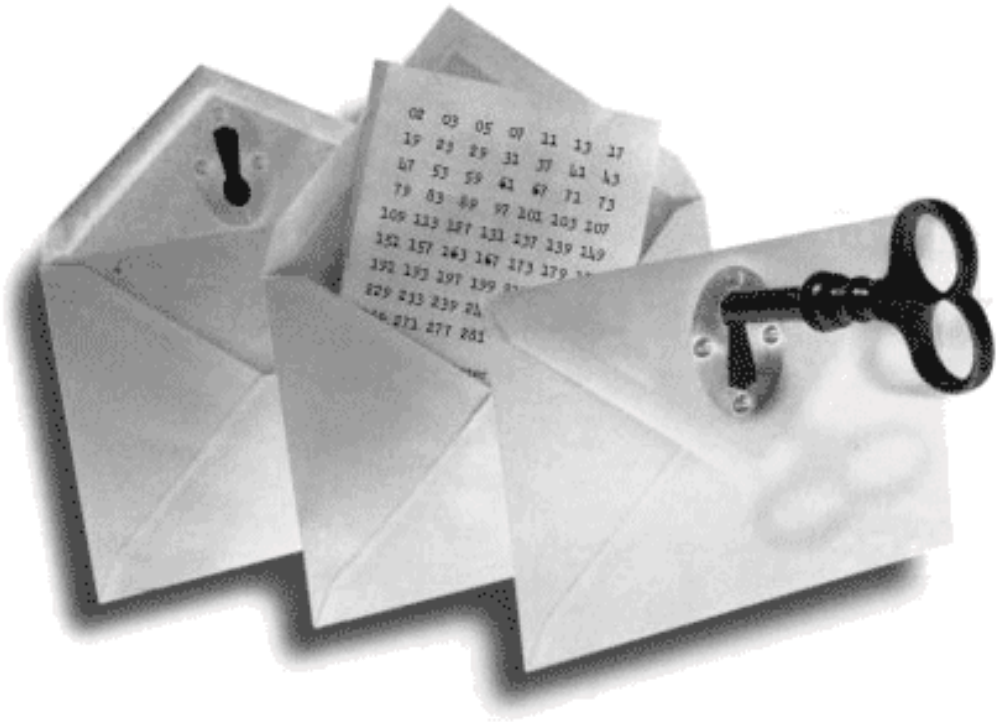
Facharbeit

Asymmetrische Verschlüsselungen am Beispiel des RSA-Verfahrens



Verfasserin: Sophie Duda

Fachlehrer: Herr Borzichowski

Schule: Gymnasium Petrinum Recklinghausen

Kurs: Leistungskurs Mathematik LK 1

Schuljahr: 2018/2019

Inhaltsverzeichnis

1. Einleitung

„Natürlich schützt man Daten am besten dadurch, dass man sie gar nicht erst erhebt."[1]

Dieses Zitat von Uwe Saint-Mont beantwortet eine Frage, mit der sich bereits Menschen im alten Rom beschäftigt haben: Wie schütze ich meine Informationen vor Dritten? Nicht nur in Bereichen der Spionage oder bei Geheimdiensten müssen bestimmte Informationen vor anderen geschützt werden, sondern auch im privaten, alltäglichen Gebrauch. Besonders geheime Botschaften sind über längere Distanzen schwierig zu übermitteln, ohne, dass sie in die Hände von Außenstehenden gelangen könnten. Um einen sicheren Datentransfer zu gewährleisten, haben sich im Verlauf der Geschichte bestimmte Systeme entwickelt. Diese Verschlüsselungsverfahren zählen zur Kryptologie, einem Teilbereich der Mathematik und Informatik. Bei diesem wird zwischen der Kryptografie, der Verschlüsselung von Daten und der Kryptoanalyse, der Entschlüsselung von Daten, unterschieden. Vor allem im Zeitalter der Technik und der Computer ist es für viele Menschen von immer größerer Bedeutung, dass private Informationen nicht an Fremde gelangen. Verschlüsselungen können sowohl im privaten, als auch öffentlichen Gebrauch verwendet werden.

Doch das Ziel, Botschaften zu verschlüsseln, kam nicht erst im digitalen Zeitalter der Technik auf. Bereits Julius Cäsar verschlüsselte geheime Botschaften und eine seiner verwendeten Techniken ist bis heute als Cäsar-Chiffre bekannt. Im Verlauf dieser Arbeit werde ich sie genauer erläutern.

Mein Interesse für das Thema Kryptografie wurde aus verschiedenen Gründen geweckt und ich habe mich dazu entschlossen mich näher mit ihrer Anwendung in der heutigen Zeit auseinanderzusetzen, da sie ein dauerhaft aktuelles Thema ist und sie sehr vielseitig verwendet wird. Ich möchte mich in dieser Arbeit vor allem auf asymmetrische Verschlüsselungen (also einem Teil der Kryptografie) konzentrieren und sie am Beispiel des RSA-Verfahrens vorstellen und mathematisch betrachten. Zunächst werde ich die verschiedenen Grundlagen erklären und auch kurz auf symmetrische Verschlüsselungen eingehen, damit ein besseres Grundverständnis für das Thema gegeben ist. Im Folgenden werde ich insbesondere auf das RSA-Verfahren eingehen, dieses zunächst mathematisch betrachten und dann anhand eines Beispiels veranschaulichen.

Eine detailliertere Betrachtung anderer Verfahren oder Attacken auf das RSA-Verfahren, wie beispielsweise durch Faktorisieren sind nicht möglich, da diese den Rahmen dieser Arbeit sprengen würden. Für ein tiefergehendes Wissen können die verwendeten Quellen hinzugezogen werden.

1.1 Grundbegriffe für Verschlüsselungen

Um eine Nachricht so zu verschicken, dass niemand anderes sie lesen kann, benötigt man mindestens einen so genannten Schlüssel (*key*). Im Gegensatz zu symmetrischen Verschlüsselungen haben asymmetrische (auch Public-Key-Verfahren) zwei, statt nur einen Schlüssel. Dafür wird ein so genanntes Schlüsselpaar, bestehend aus einem privaten Schlüssel (*private key*) und einem öffentlichen Schlüssel (*public key*), verwendet. Dies ist ein großer Vorteil gegenüber den wesentlich älteren, symmetrischen Verfahren, da hierbei die sichere Übertragung des Schlüssels eine Notwendigkeit ist.

[1] Uwe Saint-Mont: Die Macht der Daten. Nordhausen 2010. Seite 92.

Grundsätzlich gilt innerhalb der Kryptologie: *M* ist die zu verschlüsselnde Nachricht (*engl. Message*) oder auch der Klartext (*engl. Plaintext*). Die verschlüsselte Nachricht wird als *C* (*engl. Ciphertext*) bezeichnet. Der dabei verwendete Schlüssel ist *k* (*engl. key*). Bei der asymmetrischen Kryptologie wird der private Schlüssel *x* und der öffentliche Schlüssel *a* genannt. Der Exponent in der Funktion, der bei der Verschlüsselung verwendet wird, ist e und der Exponent in der Funktion zur Entschlüsselung ist d. Sie sind Teile der Schlüssel x und a. Eine Tabelle mit den Begriffserklärungen findet sich im Anhang.[2]

1.2 Das Alice-Bob-Mallory-Modell

Die in dieser Arbeit vorkommenden Verfahren werden zur besseren Veranschaulichung anhand personenbezogener Beispiele erklärt. Dabei greife ich auf ein in der Kryptologie häufig verwendetes Modell zurück. Es wird im Allgemeinen als „Alice-Bob-Mallory-Modell“[3] bezeichnet. In diesem tauschen zwei Personen (Alice und Bob) Informationen über einen abhörbaren Kanal aus. Eine dritte Person (Mallory) hat dabei technische Möglichkeiten die Informationen abzuhören und zu beeinflussen. Durch die Kryptografie soll eine Möglichkeit gefunden werden diese Angriffe aufzuhalten und einen gesicherten Datentransfer zwischen Alice und Bob zu gewährleisten.

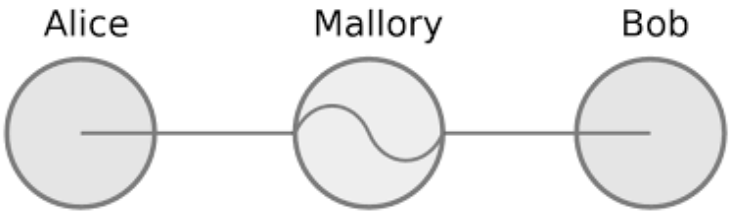


Abbildung 1: Das Alice-Bob-Mallory-Modell[4]

2. Das Prinzip symmetrischer Verschlüsselungen

Symmetrische Verschlüsselungen sind weitaus älter als asymmetrische Verschlüsselungen und zudem auch einfacher strukturiert. Sie verwenden nur einen Schlüssel, was sowohl Vor-, als auch Nachteile birgt. Zu den ältesten und bekanntesten symmetrischen Verfahren gehört die Cäsar-Chiffre.

2.1 Cäsar-Chiffre

Die Cäsar-Chiffre ist eine so genannte monoalphabetische Substitutionschiffre (*Substitution= Vertauschung*). Da die Zuordnung nicht zufällig, sondern nach einer zyklischen Rotation (*Drehung*) verläuft, muss man, um eine Botschaft zu verschlüsseln,

[2] VgL Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 36 f.
[3] Vgl. Klaus Schmeh: Kryptografie Verfahren-Protokolle-Infrastrukturen. Heidelberg 2016. Seite 10.
[4] Aghababaeetafreshi, Mona: A Security Architecture for a Wireless Memory. Tampere 2013. https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/21783/AghababaeeTafreshi.pdf (Stand 29.03.2019)

einen Schlüssel *k* wählen. Später wird zur Verschlüsselung jeder Buchstabe um den Wert *k* verschoben. Beim Alphabet ist der kleinste Schlüssel $k = 1$ und somit der größte Schlüssel die Anzahl der Buchstaben im Alphabet -1. Somit liegt *k* im Definitionsbereich $\boldsymbol{D} = [1; 25]$ (bei insgesamt 26 Buchstaben). Dieser Schlüssel muss dem Empfänger überbracht werden, ohne, dass er an Dritte weitergelangt.

Um das Ganze besser zu veranschaulichen, wird jedem Buchstaben zunächst eine Zahl zugeordnet. Also: $1 = A, 2 = B, \dots, 26 = Z$

Hiernach verschiebt man das gesamte Alphabet, also den Klartext *M,* um *k* Stellen. Dabei erhält man die Verschlüsselung *C*. Es gilt: $C = M + k.$ Da der Wertebereich von C bei $\boldsymbol{W} = [1; 26]$ liegt, wird aufgrund der zyklischen Rotation den Werten, welche größer als 26 sind, nicht $C = 27$, $C = 28$ … zugeordnet, sondern $C = 1$, $C = 2\dots$. Für $k = 5$ gilt also:

$A^* = 1 + 5 = F, B^* = 2 + 5 = G, \dots, Z^* = 26 + 5 = E$ (Das * steht hier für die codierte Version der Buchstaben).

An einem konkreten Beispiel sieht es dann wie folgt aus: Wenn Alice Bob die Botschaft „TREFFEN UM DREI IM PARK“ verschlüsselt zukommen lassen möchte, wählt sie zunächst einen Schlüssel, zum Beispiel $k = 3$. Im Alphabet werden also alle Buchstaben um drei Stellen verschoben. Als Verschlüsselung lautet die Nachricht folgendermaßen: „WHUIIHQ XP GUHL LP SDUN“. Bob entschlüsselt diese Nachricht wieder mit dem Schlüssel $k = 3$ rückwärts und erhält so den Klartext *M* (=TREFFEN UM DREI IM PARK).

Ein großer Nachteil von Verschlüsselungen dieser Art ist die einfache Dechiffrierung. Da die Cäsar-Chiffre allgemein bekannt ist, kann Mallory zur Entschlüsselung alle möglichen Schlüssel ausprobieren um *k* zu finden. Eine solche vollständige Schlüsselsuche wird in der Kryptografie als *Brute-Force-Attacke*[5] bezeichnet. In diesem Beispiel kann der Schlüssel nur zwischen 1 und 25 liegen, wodurch k ohne großen Aufwand schnell gefunden werden kann. Auch die Häufigkeitsberechnung der Buchstaben im deutschen Alphabet und der Vergleich mit der Codierung ist eine Möglichkeit der Kryptoanalyse, welche ohne viel Mühe betrieben werden kann. Anhand von Kerckhoffs‘ Maxime kann man die Nachteile einer solchen Codierung deutlich machen.

2.2 Kerckhoffs‘ Maxime

Ein Grundsatz der modernen Kryptografie ist das 1883 vom Niederländer Auguste Kerckhoffs verfasste *Kerckhoffs’sche Prinzip* (oder *Kerckhoffs‘ Maxime*). Dieses Prinzip beruht auf der Idee, dass „allein die Geheimhaltung des Schlüssels die Sicherheit eines Verfahrens garantieren muss“[6]. Dieser Grundsatz verweist auf die Unsicherheiten einiger symmetrischer Kryptosysteme, wie beispielsweise der Cäsar-Chiffre, da diese bei Kenntnis des Verfahrens sehr leicht zu Decodieren ist, auch wenn man hierbei den Schlüssel zu Beginn nicht kennt. Eine Lösung für dieses Problem soll das RSA-Verfahren bieten.

[5] VgL Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 40.
[6] Klaus Schmeh: Kryptografie Verfahren-Protokolle-Infrastrukturen. Heidelberg 2016. Seite 40.

3. Das RSA-Verfahren

3.1 Geschichtliche Einleitung

Ein Grundlegendes Problem der Kryptoanalyse stellt, wie bereits zuvor erkannt, die Schlüsselübertragung dar. Dieses Problem wird häufig auch als *Schlüsselaustauschproblem*[7] bezeichnet. Natürlich besteht immer eine Möglichkeit des manuellen Schlüsselaustauschs, welcher auch *Out-of-Band-Schlüsselaustausch*[8] genannt wird. Insbesondere bei einer größeren Gruppe von Personen oder bei großen Distanzen stößt das Verfahren an seine Grenzen.

Das RSA-Verfahren zählt zu den asymmetrischen Verschlüsselungen und wurde erstmals 1978 im Paper „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“[9] veröffentlicht. Der Name RSA setzt sich aus den Anfangsbuchstaben der Nachnamen der Entwickler Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman zusammen. Durch dieses System wird das Schlüsselaustauschproblem umgangen, da es sich hierbei um eine Kombination aus einem öffentlichen Schlüssel (*public key*) und einem privaten Schlüssel (*private key*) handelt. Aus diesem Grund wird diese Chiffre auch *Public-Key-Methode* oder *Public-Key-Verschlüsselung* genannt. Mithilfe solcher asymmetrischer Verschlüsselungen können digitale Signaturen erstellt werden.

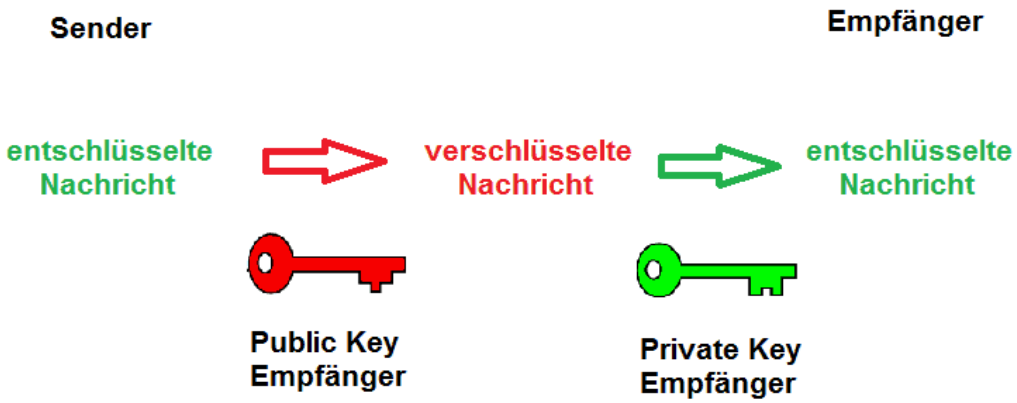


Abbildung 2: Public key Verschlüsselungen[10]

[7] Vgl. Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 47.
[8] Vgl. Klaus Schmeh: Kryptografie Verfahren-Protokolle-Infrastrukturen. Heidelberg 2016. Seite 190.
[9] R.L. Rivest, A. Shamir, L.Adelman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Cambridge. (o.A.). https://people.csail.mit.edu/rivest/Rsapaper.pdf (Stand 16.03.2019)
[10] Jonas Hellmann: SSL-Zertifikate | Verschlüsselte Kommunikation im Internet.(o. A.) 2017. https://blog.jonas-hellmann.de/ssl-zertifikate-verschluesselte-kommunikation-im-internet/ (Stand 24.03.2019)

3.2 Zahlentheoretische Grundlagen

3.2.1 Definition von Primzahlen

Für die Berechnung eines Schlüssels nach dem RSA-Verfahren werden unter anderem Primzahlen verwendet. „Eine Primzahl ist eine natürliche Zahl, die genau zwei Teiler (in den natürlichen Zahlen) hat, nämlich 1 und sich selber. Natürliche Zahlen ungleich 1, die keine Primzahlen sind, heißen zusammengesetzt.“[11] So ist, wenn $p \in \mathbb{N}$ und als Teiler *p* und 1 gegeben sind, *p* eine Primzahl. Als weitere Möglichkeit zum Erkennen einer Primzahl, wird der Primzahltest in Kapitel 3.3.2 erläutert.

3.2.2 Modulo-Rechnen und Restklassen

Um asymmetrische Verschlüsselungen, speziell auch das RSA-Verfahren, verstehen zu können, benötigt man bestimmtes mathematisches Grundwissen. Dafür wird im Folgenden das so genannte Modulo-Rechnen erläutert. Im Grunde genommen ist das Modulo-Rechnen einfach gesagt das Rechnen mit Rest.[12] Dabei werden nur ganze Zahlen zwischen 0 und einer beliebig großen Zahl *n* betrachtet. Der Definitionsbereich liegt also bei $\mathbf{D} = \{0; n\}$. Nach Erreichen von n wird wieder bei 0 angefangen zu rechnen. Ein einfaches Beispiel für Modulo-Rechnen ist eine Digitaluhr, die einen Modulo-24-Zähler hat.

Modulo kann, wie auch Addition oder Subtraktion, als Rechenoperation verwendet werden. Dabei bildet nur der Rest einer Teilung das Ergebnis. Bei der Division der natürlichen Zahlen 20 und 6 ist das Ergebnis $20 \div 6 = 3 \text{ Rest } 2$. Als Modulo-Rechnung aufgeschrieben gilt demzufolge $20\%6 = 2$. Das %-Zeichen ist dabei das Modulo-Rechenzeichen. Man teilt folglich eine ganze Zahl x durch eine weitere ganze Zahl $y \neq 0$ und erhält einen Rest $r \in \mathbb{N}$. Alle Zahlen y können nun anhand aller Reste in Teilmengen eingeteilt werden. Diese nennt man auch Restklassen.[13] Jede Zahl, die bei der Teilung durch y den gleichen Rest r erhält, gehört der Restklasse Modulo y an. Ein Beispiel aus dem Alltag sind dabei gerade und ungerade Zahlen. Gerade Zahlen haben beim Teilen durch 2 den gleichen Rest von 0. Sie gehören also der Restklasse Modulo 2 an.

3.2.3 Der erweiterte Euklidiktische Algorithmus

Mithilfe des euklidiktischen Algorithmus‘ aus dem Bereich der mathematischen Zahlentheorie des griechischen Mathematikers Euklid lässt sich der größte gemeinsame Teiler (geschrieben ggT) zweier Zahlen berechnen. Die Linearkombination des ggT wird mit dessen Erweiterung ermittelt. Eine genauere Erklärung, welche den Umfang dieser Arbeit überschreiten würde, findet sich in den verwendeten Quellen.

3.2.4 Die Euler Phi Funktion

Die Euler Phi Funktion ist ein Funktion, welche nach dem Mathematiker Leonhard Euler benannt wurde. Sie gibt die Anzahl aller natürlichen Zahlen an, die kleiner als die Zahl *n*

[11] Dr. Michael Welter: Primzahlen. Bonn 2007. http://www.math.uni-bonn.de/people/welter/primzahlen.pdf (Stand 21.03.2019).
[12] o. V.: Modulo rechnen EINFACH erklärt, inkl. BEISPIEL. (o. A.). https://www.youtube.com/watch?v=zWcegz6rwxg (Stand 29.03.2019).
[13] o. V.: Modulo-Teilen mit Rest?-Grundlagen: (o. A.) 2015. https://www.youtube.com/watch?v=rVGrds7AbPw (Stand 29.03.2019).

und gleichzeitig teilerfremd zu dieser sind.[14] Das heißt, die Anzahl aller Zahlen $0 < x < n$, die zu n teilerfremd sind. Das Zeichen für die Phi-Funktion ist das φ. So ist $\varphi(10) = 4$, da die Zahlen 1,3,7,9 alle teilerfremd zu 10 sind und der größte gemeinsame Teiler 1 ist. Eine nähere Definition der Euler Phi Funktion findet sich in Kapitel 3.2.9.

3.2.5 Der Satz von Euler

Der Satz von Euler, aufgestellt von dem zuvor bereits erwähnten Leonhard Euler, beweist, dass nach dem Entschlüsseln mit dem RSA-Verfahren tatsächlich der ursprüngliche Klartext herauskommt. Dieser Satz besagt folgendes:

„Sei $n \in \mathbb{N}$. Dann gilt für alle $n \in \mathbb{N}$., die teilerfremd zu n sind $a^{\varphi(n)} \equiv 1 \pmod{n}$."[15]

3.2.6 Modifizierter Satz von Euler

Um die Bedingungen des RSA-Verfahrens zu erfüllen, ist jedoch eine leicht abgeänderte Form des Satzes von Nöten. Diese lautet folgendermaßen:

„Sei $n = p \times q$, wobei p und q zwei verschiedene Primzahlen sind. Dann gilt für alle $a \in \mathbb{N}$: $a^{k \times \varphi(n)+1} \equiv a \pmod{n}$ mit beliebiger ganzer Zahl $k \geq 0$."[16]

3.2.7 Der Satz von Fermat

Neben dem Satz von Euler ist der Satz von Fermat für das RSA-Verfahren von Bedeutung. Er wurde bereits wesentlich früher als der Satz von Euler gefunden, resultiert jedoch unmittelbar aus ihm. Für ihn gilt:

Sei p eine Primzahl. Dann gilt für alle $a \in \mathbb{N}$, die nicht durch p teilbar sind $a^{p-1} \equiv 1 \bmod p$[17].

3.2.8 Einwegfunktionen

„Eine Funktion, die einfach zu berechnen ist, deren Umkehrung jedoch nur mit großem Aufwand berechnet werden kann, nennt man Einwegfunktion."[18] Im Englischen werden diese Einwegfunktionen auch *one way function* genannt. Sie bedeuten, dass $y = f(x)$ leicht zu berechnen ist, das Auflösen der Umkehrfunktion $x = f^{-1(y)}$ jedoch mit sehr viel Aufwand verbunden ist. Die Sicherheit des RSA-Verfahrens stützt sich auf den derzeitigen Kenntnissen, nach denen es bisher keinen Algorithmus gibt, der das Faktorisieren sehr großer Zahlen wesentlich vereinfacht und so den zeitlichen Aufwand begrenzt. Das Faktorisieren (Umkehren von Funktionen) wird in dieser Arbeit aufgrund des gegebenen Rahmens nicht genauer erläutert.

---

[14] Andreas Kirchner: Euler Phi Funktion. (o. A.). https://www.mathe-lerntipps.de/euler-phi-funktion/ (Stand 29.03.2019).
[15] Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 87.
[16] Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 89.
[17] Vgl. H.W. Lang: Sätze von Fermat und Euler. Flensburg 2018. http://www.inf.fh-flensburg.de/lang/krypto/grund/fermat-euler.htm (Stand 17.03.19).
[18] Klaus Schmeh: Kryptografie Verfahren-Protokolle-Infrastrukturen. Heidelberg 2016. Seite 198.

3.2.9 Gruppenaxiome

Um die Gruppentheorie zu verstehen muss man zuerst wissen, was mathematisch betrachtet eine Gruppe ist. Jede Rechenoperation in der Mathematik beinhaltet zunächst Elemente einer Menge, die miteinander verknüpft werden. M ist die Menge der natürlichen Zahlen. So sind die Elemente a und b aus der Menge M stammend und können mit der Verknüpfung $\times$ (Multiplikation) verbunden werden. Das Ergebnis ist c, eine natürliche Zahl, also auch ein Element aus der Menge M ist. Es gilt also $a, b \in M$ und $c \in M$. Gerechnet wird $a \times b = c$. Es gibt auch weitere Verknüpfungen wie + (Addition) oder „hoch" (Potenzierung)[19].

Des Weiteren wird zwischen bestimmten Verknüpfungen unterschieden. Bei Verknüpfungen dreier Elemente *a, b, c* $\in$ M durch Multiplikation oder durch Addition gilt $(a \times b) \times c = a \times (b \times c)$ beziehungsweise $(a + b) + c = a + (b + c)$. Es handelt sich um eine assoziative Verknüpfung. Die Verknüpfung einer Menge mit einem Rechenoperator wird mit (M, Rechenoperator) bezeichnet. Eine Menge mit einer assoziativen Verknüpfung wird als Halbgruppe bezeichnet[20].

Eine Gruppe hingegen muss insgesamt drei Bedingungen erfüllen: Zunächst muss die Verknüpfung assoziativ sein. Außerdem muss die Menge ein neutrales Element enthalten. Zuletzt gibt es zu jedem Element a $\in$ M ein inverses Element in M.

Ein neutrales Element wird entweder Nullelement (in der Addition) oder Einselement (in der Multiplikation) genannt. Diese bezeichnen die Zahlen 0 und 1, da sich bei jeder Addition an die man ein +0 hängt und bei jeder Multiplikation, welche man mit $\times 1$ rechnet, das Ergebnis nicht verändert.[21] Dieses neutrale Element wird als *e* bezeichnet und die Gruppe aus der Menge M, der Verknüpfung $\times$ und *e* als $(M, \times, e)$.

Für das inverse Element muss $a \times a' = e$ gelten. Dann bezeichnet man $a' \in M$ als invers zu a $\in$ M.

Die eulersche Phi-Funktion wird in einer Gruppe definiert durch: „Sei $n \in \mathbb{N}$. Die Menge $\mathbb{Z}_n^*$ besteht aus allen Elementen von $\mathbb{Z}_n$, die teilerfremd zu n sind. […] Mit $\varphi(n)$ wird die Anzahl der Elemente von $\mathbb{Z}_n^*$ bezeichnet. […] Die Anzahl der Elemente von wird durch die eulersche Phi-Funktion $\varphi(n)$ […] angegeben."[22]

3.3 Rechnung des RSA-Verfahrens

Grundsätzlich besteht das Public-Key-Verschlüsselungssystem aus zwei großen Schritten. Im ersten verschlüsselt der Sender (Bob) den Klartext mit dem öffentlichen Schlüssel, den der Empfänger (Alice) zuvor der Öffentlichkeit zur Verwendung gestellt hat. Dies erfolgt mit der Rechnung $C = M^e \bmod n$. Den Klartext kann man nur durch das Entschlüsseln mit Alices privaten Schlüssel erhalten. Sie berechnet zum Entschlüsseln $M = C^d \bmod n$. Dabei entfällt das Schlüsselaustauschproblem. Um als Empfänger die Schlüssel zu erzeugen sind mehrere Teilschritte erforderlich.

[19] Vgl. Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 73 ff.
[20] Vgl. Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 76.
[21] Vgl. Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 75.
[22] Hans Werner Lang: Kryptografie für dummies. Weinheim 2018. Seite 77.

3.3.1 Schlüssel erzeugen

Bevor Alice ihre öffentlichen Schlüssel zur Verfügung stellen kann, müssen diese zunächst erzeugt werden. Man benötigt hierfür zunächst eine bestimmte Block-Länge (eine bestimmte Bit-Größe) für den Schlüssel, wobei gilt: Je länger, desto sicherer. Gewöhnlicher Weise nimmt man dabei Zahlen mit etwa 200 Stellen.[23]

Zuerst erfolgt die Wahl zweier Primzahlen *p* und *q*. Dabei ist zu beachten: je größer die Zahl, desto sicherer ist die Chiffrierung. Aus deren Produkt wird die Zahl *n* gebildet: $\mathrm{n} = \mathrm{p} \times \mathrm{q}$. Um daraus eine φ-Funktion zu bilden, rechnet man $\varphi(\mathrm{n}) = (\mathrm{p}-1) \times (\mathrm{q}-1)$. Für *e*, den Exponenten in der späteren Gleichung des öffentlichen Schlüssels, gilt $\mathrm{ggT}\big(\mathrm{e}, \varphi(\mathrm{n})\big) = 1$ (ggT: größter gemeinsamer Teiler) und $1 < \mathrm{e} < \varphi(\mathrm{n})$. Der Exponent *d* als Teil des privaten Schlüssels wird berechnet mit $\mathrm{d} \times \mathrm{e} \bmod \varphi(\mathrm{n}) = 1$. Er kann ebenso mithilfe der Variablen g und h ermittelt werden, für die gilt: $\mathrm{ggT}(\mathrm{e}, \varphi(\mathrm{n}) = 1 = (\mathrm{g} \times \mathrm{e}) + (\mathrm{h} \times \varphi(\mathrm{n}))$. Dabei ist d der Rest von $\frac{\mathrm{g}}{\varphi(\mathrm{n})}$.

3.3.2 Primzahlen wählen

Die Primzahlen *p* und *q,* aus deren Produkt *n* entsteht, müssen beide sehr groß sein und dürfen nicht zu eng beieinander liegen, da sonst leicht die Faktorisierung von n möglich und so die Sicherheit des Verfahrens gefährdet ist. Zudem müssen sowohl $\mathrm{p}-1$ und $\mathrm{p}+1$ als auch $\mathrm{q}-1$ und $\mathrm{q}+1$ einen großen Primfaktor („ein Primfaktor ist eine nicht weiter zerlegbare Zahl“[24]) enthalten und nicht aus kleinen Primfaktoren bestehen. Um solche Primzahlen zu finden, gibt es den großen Primzahlentest. Dafür ist es nötig, herauszufinden, ob die Zahl *n* zusammengesetzt oder eine Primzahl ist. Um *n* als zusammengesetzt zu erkennen, muss ein Primfaktor in *n* gefunden werden. Falls dies zutrifft, muss gleichzeitig mindestens einer davon $\leq \sqrt{\mathrm{n}}$ sein. Falls dies nicht zutrifft, ist *n* eine Primzahl.

3.3.3 Verschlüsseln und Entschlüsseln

Für das Verschlüsseln und Entschlüsseln von Botschaften sind insgesamt mehrere Gleichungen nötig.

Zum Verschlüsseln des Klartextes rechnet Bob mithilfe der Schlüssel von Alice: $\mathrm{C} = \mathrm{M}^{\mathrm{e}} \bmod \mathrm{n}$. Das Ergebnis *C* ist der Geheimtext und *e* und *n* sind die öffentlichen Schlüssel, die für jeden zugänglich sind. Die Modulo-Rechnung ($\bmod \mathrm{n}$) die hier erfolgt, berechnet den Rest, der bei einer ganzzahligen Division durch *n* erhalten wird.

Um den erhaltenen Geheimtext wieder zu entschlüsseln benutzt die Empfängerin (Alice) den nur ihr bekannten, privaten Schlüssel *d*, das Gegenstück zum öffentlichen Schlüssel *e*. Die Rechnung dafür ist wie folgt: $\mathrm{M} = \mathrm{C}^{\mathrm{d}} \bmod \mathrm{n}$. Das Ergebnis *M* ist hierbei wiederum der Klartext, der zuvor verschlüsselt worden war.

---

[23] (o.V.):RSA-Verschlüsselungsverfahren. Berlin (o.A.). http://didaktik.mathematik.hu-berlin.de/files/krytographie.pdf (Stand 29.03.2019).

[24] O.V.: (o.A.) https://www.studienkreis.de/mathematik/primfaktorzerlegung-erklaerung/ (Stand 01.04.2019)

Einer außenstehenden Person, hier Mallory, ist es dabei nicht möglich auf den Klartext zuzugreifen, da für die Entschlüsselung der nur Alice bekannte private Schlüssel notwendig ist.

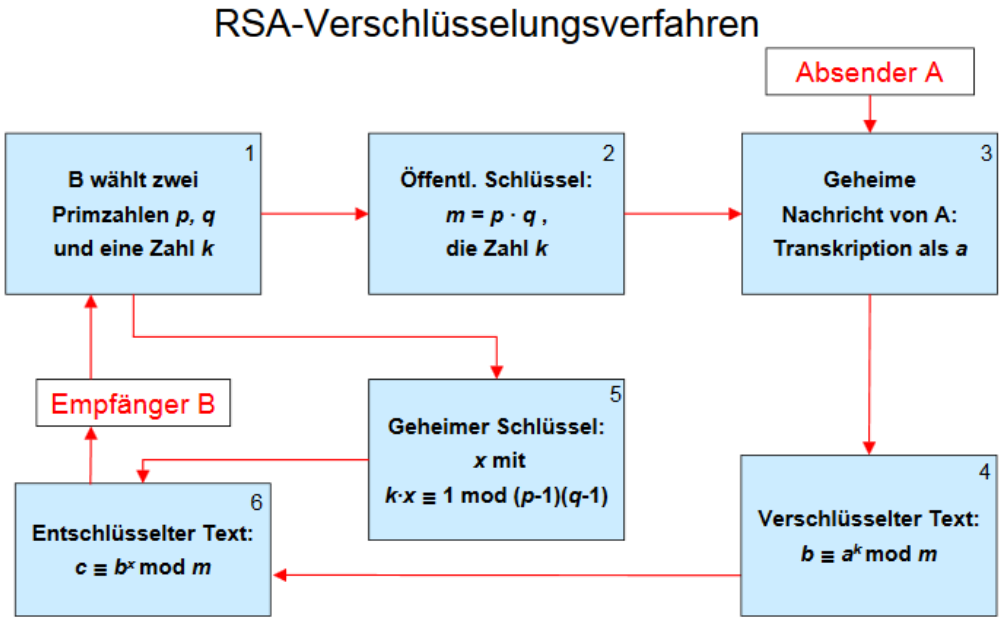


Abbildung 3: Das RSA-Verschlüsselungsverfahren[25]

4. Eine Beispielverschlüsselung

Um die gesamte Rechnung besser verständlich zu machen werde ich sie im Folgenden anhand eines Beispiels erläutern. Da es schwer möglich ist eine solche Chiffre anhand von sehr großen Zahlen zu erklären, werde ich Zahlen im kleinen Bereich verwenden.

Möchte Bob Alice die Nachricht „SECRET“ übermitteln, ohne, dass Mallory diese in Erfahrung bringen kann, müssen zunächst die Schlüssel von Alice erzeugt werden. Dies erfolgt zuerst mit der Wahl von zwei Primzahlen p und q. Dafür verwendet sie in diesem Beispiel $\mathrm{p} = 3$ und $\mathrm{q} = 11$. Hiernach berechnet sie $\mathrm{n} = \mathrm{p} \times \mathrm{q} = 3 \times 11 = 33$. Für den Exponenten der Verschlüsselung gilt die Voraussetzung $1 < \mathrm{e} < \varphi(\mathrm{n})$. Für φ(n) berechnet Alice $\varphi(\mathrm{n}) = (\mathrm{p} - 1) \times (\mathrm{q} - 1) = 2 \times 10 = 20$. Der Exponent e muss dabei teilerfremd zu φ(n) sein, es gilt also: $\mathrm{ggT}(\mathrm{e}, \varphi(\mathrm{n})) = (\mathrm{e}, 20) = 1$. Dies kann man mit der Primfaktorisierung von φ(n), oder aber mithilfe des euklidiktischen Algorithmus überprüfen. Es kann also $\mathrm{e} = 7$ gelten, da $1 < \mathrm{e} < 20 = 1 < 7 < 20$. Aus den Zahlen $\mathrm{n} = 33$ und $\mathrm{e} = 7$ ergibt sich der öffentliche Schlüssel.

Der private Schlüssel lässt sich nun mit g und h berechnen wobei für diese beiden Variablen gelten muss: $\mathrm{ggT}\big(\mathrm{e}, \varphi(\mathrm{n})\big) = \mathrm{g} \times \mathrm{e} + \mathrm{h} \times \mathrm{n}$. Wir erinnern uns, dass größte gemeinsame Teiler von e und $\varphi(\mathrm{n})$ hier 1 ist. Also: $\mathrm{ggT}\big(\mathrm{e}, \varphi(\mathrm{n})\big) = 1 = 3 \times 7 + (-1 \times 20)$. Daraus ergeben sich $\mathrm{g} = 3$ und $\mathrm{h} = -1$. Der Entschlüsselungsexponent d wird nun berechnet aus dem Divisionsrest von $\mathrm{g} \div \varphi(\mathrm{n})$. Es ergibt sich $\frac{3}{20} = 0\ \mathrm{Rest}\ 3$ und $\mathrm{d} = 3$. Es lässt sich überprüfen mit der Formel $\mathrm{d} \times \mathrm{e} \bmod \varphi(\mathrm{n}) = 1$ und $3 \times 7 \bmod 21 = 1$.

[25] o.V.: RSA-Verschlüsselungsverfahren. Berlin (o.A.). http://didaktik.mathematik.hu-berlin.de/files/krytographie.pdf (Stand 29.03.2019).

Folglich besteht das verwendete Schlüsselpaar aus dem öffentlichen Schlüssel $x = (n, e) = (33,7)$ und dem privaten Schlüssel $a = (p, q, d) = (3,11,3)$.

Jedes Klartextzeichen der Botschaft „SECRET“ wird nun, wie in der Tabelle aufgelistet, einer Zahl zugeordnet. Es gilt

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

M ist in diesem Beispiel also SECRET =195318520. Diese Nachricht muss Bob vor dem Verschlüsseln in Blöcke teilen, die nicht größer als n=33 sein dürfen. Als Blöcke legt er 19, 5, 3, 18, 5 und 20 fest. Um nun den Geheimtext C an Alice zu senden, benötigt Bob also folgende Formel: $C_{Block} = M^e (\mathrm{mod}\ n)$. Zum codieren der Botschaft muss er jeden Block einzeln verschlüsseln. So rechnet er:

$C_S = 19^7 (\mathrm{mod}\ 33) = 893871739 \bmod 33 = 13.$

$C_E = 5^7 (\mathrm{mod}\ 33) = 78125 \bmod 33 = 14,$

$C_C = 3^7 (\mathrm{mod}\ 33) = 2187 \bmod 33 = 9,$

$C_R = 18^7 (\mathrm{mod}\ 33) = 612220032 \bmod 33 = 6,$

$C_E = 5^7 (\mathrm{mod}\ 33) = 78125 \bmod 33 = 14$ und

$C_T = 20^7 (\mathrm{mod}\ 33) = 1280000000 \bmod 33 = 26.$

Der Geheimtext, den Bob nun an Alice senden kann ist $C_{SECRET} = 13\ 14\ 9\ 6\ 14\ 26.$

Wenn Alice diesen Geheimtext nun wieder entschlüsseln möchte, benötigt sie ihre privaten Schlüssel mit $d = 3$, $p = 11$, und $q = 17$. Hiernach kann mit der Formel $M = c^d \bmod n$ die Nachricht entschlüsselt werden. Sie rechnet wieder jeden Block einzeln, also:

$M = 13^3 \bmod 33 = 2197 \bmod 33 = 19,$

$M = 14^3 \bmod 33 = 2744 \bmod 33 = 5,$

$M = 9^3 \bmod 33 = 729 \bmod 33 = 3,$

$M = 6^3 \bmod 33 = 216 \bmod 33 = 18,$

$M = 14^3 \bmod 33 = 2744 \bmod 33 = 5,$

$M = 26^3 \bmod 33 = 217576 \bmod 33 = 20.$

Nun kann sie wiederum in der Tabelle die Zahlen 19 5 3 18 5 20 den Buchstaben zuordnen und erhält den Klartext „SECRET“.

5. Vor- und Nachteile der Sicherheit

Aufgrund der Tatsache, dass es sich beim RSA-Verfahren um eine Einwegfunktion handelt, ist es gewährleistet, dass es trotz eines bekannten, öffentlichen Schlüssels nicht möglich ist, diesen ebenfalls zum Entschlüsseln der Botschaft zu verwenden. Damit Mallory die verschlüsselte Nachricht dechiffrieren kann, müsste er den öffentlichen Schlüssel faktorisieren. Vor allem bei größeren Zahlen ist dies jedoch kaum möglich und daher ist, wie bereits erwähnt, die Sicherheit des Verfahrens von der Größe der

Primzahlen abhängig. Die Sicherheit des RSA-Verfahrens beruht also zum einen auf der Größe der Primzahlen p und q und zum anderen auf der Geheimhaltung von φ(n). Falls es Mallory gelingt, φ(n) zu berechnen, so kann er mithilfe des öffentlichen Schlüssels e den privaten Schlüssel d als das multiplikativ inverse Element Modulo (n) errechnen.

Ein so genannter Faktorisierungsangriff ist eine weitere Möglichkeit der Entschlüsselung von RSA. Dabei wird die bereits bekannte Zahl n in ihre beiden Primfaktoren p und q zerteilt. Dem Angreifer ist es so möglich über $\varphi(n) = (p-1) \times (q-1)$ den Schlüssel d zu finden. Bei sehr großen p und q Werten sind solche Angriffe jedoch sehr rechenaufwendig und werden somit selten durchgeführt.

Ein weiterer Nachteil einer RSA-Verschlüsselung ist die Kenntnis davon, wer eine Nachricht sendet. So kann Mallory auf dem Kanal zurückverfolgen, dass Bob eine Nachricht an Alice gesendet hat. Der Inhalt dieser Nachricht ist jedoch schwierig zu decodieren und kann so geheim gehalten werden.

Es gibt noch weitere Möglichkeiten einer Attacke, welche weder mit dem RSA-Verfahren, noch mit anderen Methoden der Kryptografie verhindert werden können. Zu diesen zählt beispielsweise eine *Denial-of-Service-Attacke*, bei der Mallory verhindert, dass überhaupt eine Kommunikation zwischen Alice und Bob stattfinden kann.

6. Anforderungen an Verschlüsselungen

Um ein „perfektes“ Verfahren zu entwickeln, sollten folgende Anforderungen erfüllt werden:

Authentizität (*authenticity*): Die Identität der Beteiligten und die Echtheit der Nachrichten soll sichergestellt sein

Geheimhaltung (*privacy*): Nur bestimmte Personen sollen die Nachricht lesen können

Forward-secrecy: Die Nachrichten sollen sich im Nachhinein nicht mehr entschlüsseln lassen

Abstreitbarkeit (*1 to 1 deniability*): Aussagen sollen sich gegenüber Dritten abstreiten lassen[26]

Das RSA-Verfahren erfüllt, wie zuvor festgestellt, nur einige der genannten Kriterien. So ist beispielsweise keine Authentizität gegeben, da es Mallory möglich ist Bob als Absender der Nachricht zu identifizieren. Die Geheimhaltung und die *Forward-secrecy* sind mithilfe von gut gewählten Primzahlen und dem RSA-Verfahren als Einwegfunktion fast vollständig gesichert. Auch die Abstreitbarkeit von Aussagen gegenüber Fremden ist bei einer Public Key Verschlüsselung möglich.

7. Ausblick in die Zukunft/ weitere Verschlüsselungsmöglichkeiten

Um eine höhere Sicherheit von Verschlüsselungen zu gewährleisten, bieten sich mehrere Möglichkeiten an. So kann zum Beispiel eine Kombination mehrerer Systeme eine höhere Sicherheit bieten. Eine solche Fusion mehrerer Verfahren wird als *Hybride*

[26] Vgl. Georg Krause: Quantenkryptographie. Heidelberg 2014/15. https://www.thphys.uni-heidelberg.de/~wolschin/qms14_3.pdf (Stand 17.03.19).

Verschlüsselung[27] bezeichnet. Dabei gilt: je mehr Verfahren man miteinander verbindet, desto höher ist die Sicherheit der versendeten Nachricht.

In der heutigen Zeit und mit Ausblick auf die Zukunft werden neue Verschlüsselungstechniken entwickelt. Da bereits bekannte Verfahren mithilfe von verschiedenen Algorithmen gelöst werden können, greift die Wissenschaft heute auf ein neues Verfahren zurück: Quantenkryptografie. Mithilfe von dieser sollen alle im vorherigen Kapitel 6 genannten Anforderungen erfüllt und so ein Maximum an Sicherheit gewährleistet werden.

8. Fazit

Abschließend ist somit festzuhalten, dass es verschiedene mathematische Möglichkeiten gibt, Nachrichten zu verschlüsseln. Manche bieten eine höhere Sicherheit als andere und werden aufgrund dessen häufiger als andere verwendet. Da sich die Menschen bereits seit mehr als 2000 Jahren mit unterschiedlichen Möglichkeiten der Verschlüsselung beschäftigen, haben sich sehr viele unterschiedliche Systeme entwickelt. Kryptografie kann in den unterschiedlichsten Lebensbereichen verwendet werden. Die Enigma beispielsweise war eine Maschine im zweiten Weltkrieg, welche zur Geheimhaltung von Nachrichten verwendet wurde und erst spät durch die Engländer decodiert werden konnte. Diese Arbeit beschreibt nur ein Beispiel aus dem breit gefächerten Rahmen der asymmetrischen Kryptografie und veranschaulicht, welche mathematischen Rechenschritte zur Durchführung des RSA-Verfahrens von Nöten sind.

Rückbeziehend auf das zu Beginn genannte Zitat von Uwe Saint Mont ist weiterhin dessen Wahrheitsgehalt zu erkennen. Es gibt keine (oder kaum) Möglichkeiten, eine 100%ige Sicherheit von Daten zu gewähren. Die derzeit entwickelten Verfahren ermöglichen nur ein gewisses Grad an Sicherheit. Vielleicht wird in Zukunft jedoch ein Verfahren entwickelt, welches eine näherungsweise vollständige Sicherheit garantieren kann. Bis dahin jedoch gilt weiterhin: „[Man] schützt Daten am besten dadurch, dass man sie erst gar nicht erhebt.“[28]

[27] Vgl. Klaus Schmeh: Kryptografie Verfahren-Protokolle-Infrastrukturen. Heidelberg 2016. Seite 214.
[28] Uwe Saint-Mont: Die Macht der Daten. Nordhausen 2010. Seite 92.

9. Anhang

Variable	Erklärung	Berechnung
M	Der zu verschlüsselnde Text, Klartext	$\boldsymbol{M = C^e \bmod n}$
C	Der verschlüsselte Text, Geheimtext	$\boldsymbol{C = M^d \bmod n}$
k	Schlüssel der symmetrischen Verschlüsselung	Frei wählbar
x	Privater Schlüssel der asymmetrischen Verschlüsselung	Aus d, p und q
a	Öffentlicher Schlüssel der asymmetrischen Verschlüsselung	Aus e und n
e	Der Exponent der Verschlüsselung	$\boldsymbol{1 < e < \varphi(n)}$
d	Der Exponent der Entschlüsselung	Rest von $\frac{g}{\varphi(n)}$
p	Eine große Primzahl	Frei wählbar
q	Eine große Primzahl $\neq \boldsymbol{p}$	Frei wählbar
n	Teil des öffentlichen Schlüssels	$\boldsymbol{n = p \times q}$
$\boldsymbol{\varphi(n)}$	Eine Phi-Funktion	$\boldsymbol{\varphi(n) = (p-1) \times (q-1)}$

10. Literaturverzeichnis

Primärliteratur/-quellen:

- Andreas Kirchner: Euler Phi Funktion. (o. A.). https://www.mathe-lerntipps.de/euler-phi-funktion/ (Stand 29.03.2019).
- Dr. Michael Welter: Primzahlen. Bonn 2007. http://www.math.uni-bonn.de/people/welter/primzahlen.pdf (Stand 21.03.2019).
- Georg Krause: Quantenkryptographie. Heidelberg 2014/15. https://www.thphys.uni-heidelberg.de/~wolschin/qms14_3.pdf (Stand 17.03.19).
- Hans Werner Lang: Kryptografie für dummies. Weinheim 2018.
- H.W. Lang: Sätze von Fermat und Euler. Flensburg 2018. http://www.inf.fh-flensburg.de/lang/krypto/grund/fermat-euler.htm (Stand 17.03.19).
- Klaus Schmeh: Kryptografie Verfahren-Protokolle-Infrastrukturen. Heidelberg 2016 (6., aktualisierte Auflage).
- O.V.: (o.A.) https://www.studienkreis.de/mathematik/primfaktorzerlegung-erklaerung/ (Stand 01.04.2019)
- o.V.: RSA-Verschlüsselungsverfahren. Berlin (o.A.). http://didaktik.mathematik.hu-berlin.de/files/krytographie.pdf (Stand 29.03.2019).
- o. V.: Modulo rechnen EINFACH erklärt, inkl. BEISPIEL. (o. A.). https://www.youtube.com/watch?v=zWcegz6rwxg (Stand 29.03.2019).
- o. V.: Modulo-Teilen mit Rest?-Grundlagen: (o. A.) 2015. https://www.youtube.com/watch?v=rVGrds7AbPw (Stand 29.03.2019).
- R.L. Rivest, A. Shamir, L.Adelman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Cambridge (o.A.). https://people.csail.mit.edu/rivest/Rsapaper.pdf (Stand 16.03.2019).
- Uwe Saint-Mont : Die Macht der Daten. Nordhausen 2010.

Sekundärliteratur/-quellen:

- Carsten Eilers: Verfahren der Kryptographie, Teil 8:RSA. (o. A.) 2016. https://www.ceilers-news.de/serendipity/784-Verfahren-der-Kryptographie,-Teil-8-RSA.html (Stand 29.03.2019).
- Cengiz Ay: Bit und Byte. (o. A.) https://www.sps-lehrgang.de/bit-und-byte/ (Stand 29.03.2019).
- Christian Stobitzer: Caeser Verschlüsselung/ Chaeser Chiffre. (o. A.) 2015. https://www.kryptowissen.de/caesar-chiffre.html (Stand 29.03.2019)
- Christian Stobitzer: Symmetrische Verschlüsselung. (o. A.). https://www.kryptowissen.de/symmetrische-verschluesselung.html (Stand 29.03.2019).
- Cornelius Diekmann: Mathematik der Kryptographie. (o. A.). https://www.schuelerkonferenz.edu.tum.de/fileadmin/w00brm/www/Facharbeiten_2008/diekmann_cornelius_2008_www.pdf (Stand 29.03.2019).
- Dennis Keil: Euklidiktischer Algorythmus. (o. A.). http://www.abi-mathe.de/buch/diskrete-algebra-uni/euklidischer-algorithmus/ (Stand 29.03.2019)
- H. Haertel: RSA-Verfahren (Rechenbeispiel). (o. A.) 2006. https://www.oszhandel.de/gymnasium/faecher/informatik/krypto/rsa.htm (Stand 29.03.2019).
- Julian von Mendel: RSA-Verschlüsselung. (o. A.) 2009. https://derjulian.net/resources/facharbeit.pdf (Stand 29.03.2019)
- Klaus Schmeh: Die Grundlagen der Kryptografie-Teil 1. (o. A.) 2014. http://scienceblogs.de/klausis-krypto-kolumne/2014/08/21/die-grundlagenkrise-der-kryptografie-teil-1/ (Stand 29.03.2019)
- Niels Boeing: Kampf um Leben und Code. (o. A.) 2013. https://www.zeit.de/zeit-wissen/2013/06/datenverschluesselung-kryptografen (Stand 29.03.2019).
- Niel Hagen Kirschke: Kryptologie: Hinleitung zum RSA-Verfahren. (o. A.) 2014/15. https://www.huma-gym.de/wp-content/uploads/Kryptologie-Hinleitung-zum-RSA-Verfahren.pdf (Stand 29.03.2019).
- o. V.: Kerckhoffs-Prinzip. (o. A.). http://deacademic.com/dic.nsf/dewiki/761637 (Stand 29.03.2019)
- o. V.: RSA-Verschlüsselung. Bayreuth (o. A). http://geonext.uni-bayreuth.de/fileadmin/did_inf/krypto/RSA.pdf (Stand 29.03.2019).

- Patrick Beuth: Verschlüsselung für den Tag X. (o. A.) 2015. https://www.zeit.de/digital/datenschutz/2015-09/post-quanten-kryptografie-tanja-lange-pqcrypto (Stand 29.03.2019).
- Prof. Dr. Klaus Lagally: Verschlüsselung- Grundrecht oder Delikt?. Stuttgart 1997. http://www2.informatik.uni-stuttgart.de/ifi/bs/lehre/inf+ges/cryptogr/vortrag.html (Stand 29.03.2019).
- Stefan Edelkamp: Beispiel RSA. (o. A.) 2016. https://nms.kcl.ac.uk/stefan.edelkamp/lectures/itsec/slides/rsa.pdf (Stand 29.03.2019).
- Thorsten Ferres: Facharbeit Mathematik- Kryptologie. (o. A.) https://docplayer.org/8276989-Facharbeit-mathematik-kryptologie-thorsten-ferres-mss94.html (Stand 29.03.2019).

Bildquellen:

- Aghababaeetafreshi, Mona: A Security Architecture for a Wireless Memory. Tampere 2013. https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/21783/AghababaeeTafreshi.pdf (Stand 29.03.2019).
- Jonas Hellmann: SSL-Zertifikate Verschlüsselte Kommunikation im Internet. (o.A.) 2017. https://blog.jonas-hellmann.de/ssl-zertifikate-verschluesselte-kommunikation-im-internet/ (Stand 24.03.2019).
- Walter Wegscheider: Kryptographie-RSA. (o. A.) 2011. http://www.austromath.at/medienvielfalt/materialien/krypto/lernpfad/ (Stand 29.03.2019).

Abbildungsverzeichnis

11. Selbstständigkeitserklärung

Ich versichere, dass ich die Arbeit selbstständig verfasst, keine anderen Quellen und Hilfsmittel als die angegebenen benutzt und die Stellen der Arbeit, die anderen Werken dem Wortlaut oder Sinn nach entnommen sind, in jedem Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe. Das Gleiche gilt auch für beigegebene Zeichnungen, Kartenskizzen und Darstellungen.