Kurfürst Maximilian Kulturgymnasium

KURFÜRST-MAXIMILIAN-GYMNASIUM BURGHAUSEN

S E M I N A R A R B E I T

Rahmenthema des Wissenschaftspropädeutischen Seminars:

……

……

Leitfach: ……

Thema der Arbeit:

……

……

……

Verfasser/in:

……

Kursleiter/in:

……

Abgabetermin: 10. November 2020 *(2. Unterrichtstag im November)*

Bewertung	Note	Notenstufe in Worten	Punkte		Punkte
schriftliche Arbeit				x 3	
Abschlusspräsentation				x 1	
				Summe:	
				Gesamtleistung nach § 29 (7) GSO = Summe:2 (gerundet)	

Datum und Unterschrift der Kursleiterin bzw. des Kursleiters

Datum und Unterschrift des Oberstufenkoordinators

Seminararbeit

Quirin Möller

8. November 2020

Inhaltsverzeichnis

1 Einleitung

Bei der Betrachtung der Benennung der Epochen in der menschlichen Geschichte ist bemerkbar, dass hier mehrmals die bedeutendste technische Errungenschaft aus diesem Zeitraum zur Namensgebung verwendet wird. Das ist natürlich sinnvoll da diese Entwicklungen im großen Ausmaß das Leben der Menschen beeinflussten und auch für den weiteren Verlauf der Geschichte ausschlaggebend sind. Diese Namen sind wie »Bronzezeit« recht selbsterklärend, hier wurde die Metallverarbeitung, vor allem mit Bronze erfunden und revolutionierte die Waffentechnik und ermöglichte auch viele andere neuartige Gegenstände.[1] Schwieriger wird es dann schon bei dem Titel des aktuellen Zeitabschnittes: »Digitales Informationszeitalter«. Nach Jörn Lengsfeld sind hierbei die »Informations- und Kommunikationstechnologien« die prägenden Technologien.[2] Diese Technik hat deshalb eine so große Bedeutung in unserem Leben, da sie uns durch das nicht mehr wegzudenkende Internet jederzeit Zugriff auf eine unfassbare Menge an Informationen verschafft. Allerdings werden auch diese Erfindungen leider nicht immer fortschrittsbringend eingesetzt, sondern sie haben genau wie die Erfindungen des Atomzeitalters ihre Schattenseiten, welche meist zwar um einiges unauffälliger sind, aber nicht immer auch ungefährlicher. Denn gerade diese riesige Reichweite macht das Internet so attraktiv für Angreifer und deshalb mussten Verfahren entwickelt werden um sich gegen Verbrecher, die im Hintergrund mitlesen oder schädliche Informationen verbreiten zu schützen. Aus diesem Grund wurden Verschlüsselungsverfahren entwickelt. Bei »Verschlüsselung« denkt man zwar schnell an Geheimnachrichten und ›top-secret‹ Dokumente, allerdings begegnen wir digitalen Verschlüsselungen inzwischen tagtäglich.

[1] *Bronzezeit in Europa.*
[2] Jörn Lengsfeld, *Digitales Informationszeitalter.*

2 Verschlüsselung im Allgemeinen

2.1 Definition

Bei der Verschlüsselung handelt es sich um eine Form der Codierung, hierzu gehört zum Beispiel auch der *Morsecode* oder die allgegenwärtigen *Borcodes*, allerdings liegt die Zielsetzung bei der Verschlüsselung nicht nur einfach darin die Information in ein anderes Format zu übertragen, sondern hier will man »die Informationen systematisch so verfälschen, dass sie nicht rekonstruiert werden können, es sei denn, durch ausdrücklich hierzu Berechtigte.«[3] Die Verschlüsselung gehört zum Bereich der *Kryptographie*, womit die »Wissenschaft vom geheimen Schreiben«[4] gemeint ist.

2.1.1 Terminologie

Aus diesem Wissenschaftsbereich stammen noch mehrere Begriffe ab, die im folgenden von Bedeutung sein werden:

Chiffre Geheime Methode des Schreibens, also eine Form des Verschlüsselns

Klartext Der unverschlüsselte Text

Chiffretext Der verschlüsselte Text, bzw. Ausgangstext

Chiffrieren Das verschlüsseln des *Klartextes* zum *Chiffretext*

Dechiffrieren Das entschlüsseln des *Chiffretextes* um wieder den *Klartext* zu erhalten

[3] Dankmeier, *Grundkurs Codierung*, S. 263.
[4] Wätjen, *Kryptographie*, S. 1.

2.2 Ziele der Kryptographie

2.2.1 Geheimhaltung

Der wohl bekannteste und offensichtlichste Verwendungszweck der Verschlüsselung ist eine Nachricht geheim zu halten. Hierbei wird die zu übertragende Nachricht so entstellt, dass sie für jeden völlig unsinnig erscheint, außer für den beabsichtigten Empfänger, welcher den geeigneten Schlüssel besitzt, er ihm das Dechiffrieren ermöglicht.[5]

2.2.2 Authentikation

Bei der Authentikation liegt das Ziel darin, die Echtheit einer Identität oder Nachricht zu überprüfen, da wir uns in der digitalen Welt nicht einfach durch unser Aussehen oder unsere Stimme ausweisen können und auch bei Nachrichten ist nicht zweifelsfrei Festzustellen von wem sie versendet hat und ob sie auf ihrem Weg verändert wurden. Zur *Teilnehmerauthentikation* gehört unter anderem das eingeben der Geheimzahl am Geldautomaten, da nur der Besitzer der EC-Karte auch die dazu gehörige Nummer kennt und so seine Identität dem Geldautomaten nachweisen kann. Hier gilt das Prinzip:

> Ich weise meine Identität dadurch nach, dass ich nachweise, etwas zu haben, was kein anderer hat.[6]

Ähnlich funktioniert es bei der *Nachrichtenauthentikation*: hier verknüpft der Ersteller sein »Geheimnis« mit dem Dokument um es authentisch zu machen. Im Falle des Bankautomaten, muss allerdings zusätzlich zum Kontoinhaber logischerweise auch der Bankautomat die Geheimnummer kennen. Es gibt aber auch sogenannte *Signaturverfahren*, bei denen dies nicht notwendig ist.

[5] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*.
[6] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*.

2.2.3 weitere Ziele

Neben den beiden oben genannten Zielen für die die RSA-Verschlüsselung am häufigsten eingesetzt wird, gibt es auch noch weitere Ziele, die zwar weniger prominent sind, jedoch ähnliche Techniken nutzen. Bei dem Zeil der *Anonymität* wird die Identität verborgen, was bei einer digitalen Geschäftsabwicklung mit dem Zahlen mit Bargeld verglichen werden kann, aber auch oft zum Schutz der Privatsphäre eingesetzt wird. Wie die RSA-Verschlüsselung basieren *kryptographische Protokolle* größtenteils auf dem *Public-Key-Verfahren*. Mit einem Protokoll wird hierbei die zum Datenaustausch nötige Abfolge von auszuführenden Schritten bezeichnet. Somit ist es durch vorher festgelegte Protokolle möglich, dass sich eine große Anzahl von Teilnehmern miteinander verschlüsselt verständigen können. Ein *kryptografisches Protokoll* muss sich aber nicht auf den digitalen Nachrichtenaustausch beschränken, sondern auch schon das Bedienen eines Bankautomaten wird als solches bezeichnet.

2.3 Klassische Chiffren

Die Verschlüsselung kann auf eine lange Entwicklungsgeschichte zurückblicken, und laut Ertel (*Angewandte Kryptographie*, S. 28) werden alle Verfahren, die bis etwa 1950 entwickelt und verwendet wurden als *klassische Chiffren* bezeichnet. Diese Chiffren können in *Transpositionschiffre* und *Substitutionschiffre* unterteilt werden. Bei einer *Transpositionschiffre* wird die Anordnung der Zeichen im Chiffretext gegenüber dem Klartext verändert, die Zeichen an sich aber bleiben dabei gleich. Im Chiffretext einer *Substitutionschiffre* dagegen bleibt die Position des Zeichens erhalten, jedoch wird das Zeichen an sich ersetzt. Diese lässt sich noch weiter *monoalphabetische*, bei der ein Klartext-Zeichen im Chiffretext immer durch das gleiche Zeichen repräsentiert wird und *polyalphabetische*, bei der sich das zugehörige Chiffretext-Zeichen abhängig vom Kontext verändert.

2.3.1 Caesar-Verschlüsselung

Die nach ihrem berühmtesten Benutzer JULIUS CAESAR benannte Chiffre ist zwar keine besonders sichere, aber zur Veranschaulichung gut geeignet. Diese Chiffre ist eine *monoalphabetische Substitutionschiffre* und kann noch genauer den *Verschiebechiffren* zugeordnet werden. Wie es durch den Namen bereits suggeriert wird, wird der Klartext durch Verschiebung seiner Zeichen chiffriert. Bei der Caesar-Verschlüsselung wird dies erreicht, indem jedes Zeichen mit dem Zeichen ersetzt wird, das an der Stelle im verwendeten Alphabet steht, die sich aus der Position des Klartext-Zeichens im Alphabet, summiert mit dem Schlüssel ergibt. Allgemein kann dies mit folgender Formel beschrieben werden:

$$z \mapsto (z + k) \bmod n \tag{1}$$

Hierbei steht z für das Klartextzeichen und k für den Schlüssel. Zusätzlich wird durch das Modulo verhindert, dass des Chiffre-Zeichen außerhalb des Alphabets liegt, wobei n die Länge des Alphabets angibt. Bei $k = 3$, wie JULIUS es verwendete, ergibt sich dann folgende Klartext-Alphabet zu Chiffre-Alphabet Zuordnung:

Klartext:	**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**
Chiffretext:	**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**

Wenn dieses Vorgehen jetzt auf einen Text angewendet wird, entstehen Ergebnisse, die in etwa so aussehen:

seminararbeit	hallo welt	schule
↓	↓	↓
VHPLQDUDUEHLW	KDOOR ZHOW	VFKXOH

Die Entschlüsselung erfolgt hier mit dem selben Schlüssel, der auch bei der Verschlüsselung verwendet wurde, indem die Buchstaben in entgegengesetzte Richtung verschoben werden. Diese Art der Verschlüsselung ist allerdings sehr unsicher, da sie mehrere Problemstellen aufweist:

Die Schlüsselübertragung Verschlüsselung wird häufig benutzt, wenn damit gerechnet

wird, dass die Kommunikation abgehört wird. Da aber um die verschlüsselte Kommunikation herzustellen zuerst der Schlüssel ausgetauscht werden muss, stellt sich hier die Frage, wie das erreicht werden kann, ohne dass der ungewollte Dritte davon Kenntnis nimmt.

Schlüsselmöglichkeiten Es gibt hier nur eine sehr begrenzte Anzahl von Zahlen, die für k eingesetzt werden können, und zwar $n-1$. Theoretisch können auch größere Zahlen eingesetzt werden, allerdings erzeugen sie aufgrund des Modulo keine neuen Chiffretexte. Durch diese begrenzten Variationen ist es möglich den Klartext zu ermitteln, indem alle möglichen Schlüssel durchprobiert werden.

Monoalphabetisch Da es sich um eine *monoalphabetische* Verschlüsselung handelt, kann der Schlüssel ermittelt werden, indem die statistische Verteilung der Buchstaben im Chiffretext mit dem durchschnittlichen Auftreten in der jeweiligen Sprache verglichen wird.

2.4 Symmetrie

Eine weitere wichtige Unterteilung der Verschlüsselungsformen ist die *Symmetrie*. (vgl. Ertel, *Angewandte Kryptographie*[18]) Hier wird unterschieden, ob die Entschlüsselung mit dem gleichen Schlüssel wie die Verschlüsselung erfolgt, dies wird als *symmetrisch* bezeichnet, oder ob für die Entschlüsselung ein separater Schlüssel verwendet werden muss (*asymmetrisch*). Wenn nun E die Verschlüsselung (encryption), D die Entschlüsselung (decryption), M den Klartext, C den Chiffretext (ciphertext) und K den Schlüssel (key) bezeichnet, gilt für einen *symmetrischen Algorithmus*:

$$E_K(M) = C \tag{2}$$

$$D_K(C) = M \tag{3}$$

$$D_K\left(E_K(M)\right) = M \tag{4}$$

Für einen *asymmetrischen Algorithmus* gilt nahezu identisches, mit dem Unterschied, dass für die Verschlüsselung der Schlüssel K_1 und für die Entschlüsselung K_2 verwendet

wird:

$$E_{K_1}(M) = C \tag{5}$$

$$D_{K_2}(C) = M \tag{6}$$

$$D_{K_2}\left(E_{K_1}(M)\right) = M \tag{7}$$

3 RSA-Verschlüsselung

3.1 Das Public-Key-Verfahren

Die Grundlage der RSA-Verschlüsselung bildet die Idee der *Public-Key-Kryptosysteme*.

> [Diese] wurden 1976 von von *W. Diffie* und *M. Hellman* eingeführt. Jeder Benutzer eines solchen Systems hat einen öffentlichen und einen privaten Schlüssel. Damit besitzt jeder Benutzer A eine *öffentliche* Chiffriertransformation E_A und eine *private* Dechiffriertransformation D_A.[7]

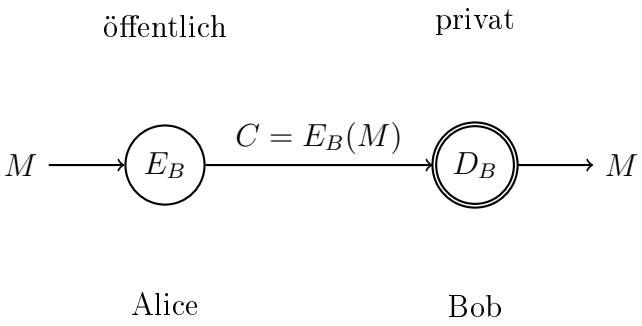
Durch diese Form der *asymmetrischen* Verschlüsselung wird das Problem der Schlüsselübertragung behoben, da der zur Verschlüsselung der Nachricht notwendige Schlüssel öffentlich zugänglich ist, die Nachricht jedoch nur mit dem geheimen privaten Schlüssel wieder lesbar gemacht werden kann. Zusätzlich ermöglicht sie durch das Wegfallen des gegenseitigen Schlüsselaustausches auch die verschlüsselte Kommunikation mit jedem beliebigen Partner, ohne die moderner Nachrichtenaustausch durch »E-Mails« oder »Instant-Messenger« undenkbar wären.[8] Ähnlich zum *asymmetrischen Algorithmus* gilt hier:

[7] Wätjen, *Kryptographie*, S. 67.
[8] Vgl. Ertel, *Angewandte Kryptographie*, S. 21.

$$E_{P_A}(M) = C \tag{8}$$
$$D_{S_A}(C) = M \tag{9}$$
$$D_{S_A}\left(E_{P_A}(M)\right) = M \tag{10}$$

Wobei P_A für den öffentlichen Schlüssel (public key) des Teilnehmers A und S_A für den privaten (secret key) steht.[9]
Beispielhaft wäre damit der Ablauf einer Nachrichtenübertrag folgender:

> Alice (A) möchte an Bob (B) eine private Nachricht M schicken. Alice kennt Bobs[[10]] öffentlichen Schlüssel und damit E_B. Alice bildet den Chiffretext $C = E_B(M)$ und sendet ihn Bob. Nur Bob kennt die Dechiffriertransformation D_B, und nur er kann damit den Text durch
>
> $$D_B(C) = D_B(E_B(M)) = M$$
>
> entschlüsseln.[11]



Veranschaulichung des Public-Key-Verfahrens[12]

Um die Geheimhaltung zu gewährleisten muss das eingesetzte Verfahren so konzipiert

[9] Vgl. Ertel, *Angewandte Kryptographie*, 21f.
[10] »›Alice‹ und ›Bob‹ als Kommunikationspartner sind Bestandteil der kryptographischen Fachsprache.« Ertel, *Angewandte Kryptographie*, S. 21
[11] Wätjen, *Kryptographie*, S. 68.
[12] Wätjen, *Kryptographie*, S. 67.

sein, dass von dem öffentlichen Schlüssel P keine Rückschlüsse auf den privaten Schlüssel S gezogen werden können.[13]

3.2 Entwicklung des RSA-Algorithmus

Das bis heute wichtigste Public-Key-Kryptosystem[14] »wurde 1978 von *R. **R**ivest*, *A. **S**hamir* und *L. **A**dleman* erfunden, als sie zu zeigen versuchten, dass Public-Key-Kryptographie unmöglich sei.«[15] Dabei war *Rivest* für die Entwicklung des Algorithmus und *Shamir* für die Überprüfung auf Schwachstellen zuständig, während *Adelman* auf beiden Seiten mitwirkte.[16] Sie waren jedoch nicht die ersten, denn »Ende 1997 [wurde bekannt], dass *Clifford Cocks* von den britischen Government Communications Headquarters (GCHQ) bereits 1975 dieselbe Idee hatte, sie aber strenger Geheimhaltung unterlag.«[17]

3.3 Schlüsselerzeugung

Um die bei einem *asymmetrischen Verschlüsselungsverfahren* nötigen beiden Schlüssel zu erzeugen müssen zuerst zwei unterschiedliche Primzahlen p und q erzeugt werden.(Vgl. Dankmeier, *Grundkurs Codierung*, S. 278) Aus diesen wird dann das Produkt $n = p \cdot q$, den *Modul*, gebildet. Für die Funktionalität des Verfahrens spielt die größe der verwendeten Primzahlen keine Rolle, allerdings sinkt mit steigender Größe die Gefahr des »Aufbrechens« durch einen Unbefugten, da die Sicherheit der RSA-Verschlüsselung auf dem *Faktorisierungsproblem* beruht. Dies ist »das bisher ungelöste Problem der schnellen Zerlegung großer Zahlen in ihre Primfaktoren, die Aufgabe hat eine exponentielle Komplexität.«[18] Dadurch ist es bei den heute verwendten 100- bis 350-stelligen mit aktuellen Methoden und Rechenleistung nicht möglich aus n die zugrundeliegenden Primzahlen p

[13] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*, S. 49.
[14] Vgl. Pieprzyk, *Topics in Cryptology - CT-RSA 2010: The 10th Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, S. 26.
[15] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*, S. 77.
[16] Ertel, *Angewandte Kryptographie*, S. 77.
[17] Wätjen, *Kryptographie*, S. 71.
[18] Dankmeier, *Grundkurs Codierung*, S. 279.

und q zu berechnen. Zusätzlich zu n muss auch noch die *Eulersche Phi-Funktion* von n gebildet werden.

3.3.1 Eulersche Phi-Funktion

Die Eulersche Φ-Funktion $\Phi(n)$ bezeichnet die Menge der zu n *teilerfremden* Zahlen a von 1 bis $n-1$.[19]

$$\Phi(n) = |\{a \in [1, n-1] \,|\, \mathrm{ggT}(n, a) = 1\}| \tag{11}$$

»Da alle Primzahlen p nur durch 1 und sich selbst teilbar sind, sind sie sicher zu den Zahlen 1 bis $p-1$ teilerfremd, daher ist $\Phi(p) = p-1$.«[20] Da n das Produkt zweier verschiedener Primzahlen und somit teilerfremder natürlicher Zahlen ist, gilt die *Multiplikativität*[21]:

$$\Phi(n) = \Phi(pq) = \Phi(p) \cdot \Phi(q) \tag{12}$$

Für $\Phi(p) = p-1$ und $\Phi(q) = q-1$ ergibt sich also[22]:

$$\Phi(n) = (p-1) \cdot (q-1) \tag{13}$$

3.3.2 Das modulare Inverse

»Des weiteren [wird] eine zu $\Phi(n)$ teilerfremde Zufallszahl e $[(1 < e < \Phi(n))]$[23] [gewählt] und [...] hierzu die *modulare inverse* Zahl d bezüglich $\Phi(n)$ [berechnet]. Für d gilt:«[24]

$$d \cdot e \mod \Phi(n) = 1 \tag{14}$$

[19] Vgl. Swoboda, Pramateftakis und Spitz, *Kryptographie Und IT-Sicherheit: Grundlagen Und Anwendungen*, S. 111.
[20] Steinfeld, *Eulersche Phi-Funktion - Mathepedia*.
[21] Vgl. Steinfeld, *Eulersche Phi-Funktion - Mathepedia*.
[22] Vgl. Dankmeier, *Grundkurs Codierung*, S. 279.
[23] Wätjen, *Kryptographie*, S. 71.
[24] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*, S. 279.

Da e und $\Phi(n)$ teilerfremd sind, gibt es hierfür eine eindeutige Lösung[25]. Dieses »d kann berechnet werden mit dem *erweiterten Euklidischen Algorithmus.*«[26]

Der erweiterte Euklidische Algorithmus Lorem ipsum

3.3.3 Die Schlüssel

Mit diesen berechneten Zahlen können nun die Schlüssel erstellt werden(Vgl. Ertel, *Angewandte Kryptographie*, S. 77):

Der öffentliche Schlüssel (P) besteht aus dem Paar $P = (e, n)$ und wird allen Personen, von denen der Besitzer Informationen erhalten will, zugänglich gemacht. Hier wird auch erkenntlich, weshalb es so wichtig ist, dass n nicht leicht in seine Primfaktoren zerlegt werden kann, denn wenn es einem Angreifer gelingen sollte diese ausfindig zu machen könnte er damit den *privaten Schlüssel* berechnen und alle (abgefangenen) Nachrichten zu entschlüsseln.

Der geheime Schlüssel (S) wetzt sich aus $S = (d, n)$ zusammen und sollte nur dem Besitzer bekannt sein.

Da die Schlüsselerzeugung meist von einer Schlüsselvergabestelle, wie z.B. dem Anbieter Sofortnachrichtendienstes, sollte dieser nach Berechnung der Schlüssel die Primzahlen p und q, sowie das Ergebnis der zugehörigen Eulerfunktion $\Phi(n)$ löschen, damit auch im Falle einer Kompromittierung der Server dessen die Privatsphäre der Nutzer geschützt ist.[27]

[25] Vgl. Ertel, *Angewandte Kryptographie*, S. 77, 164.
[26] Ertel, *Angewandte Kryptographie*, S. 77.
[27] Dankmeier, *Grundkurs Codierung*, S. 279.

3.4 Ver- und Entschlüsselungs Algorithmus

Möchte Bob nun eine chiffrierte Nachricht an Alice verschicken, muss er folgendermaßen vorgehen (Vgl. Wätjen, *Kryptographie*, S. 71):

1. Bob beschafft sich den öffentlichen Schlüssel P von Alice

2. Da die Buchstaben seiner Nachricht nicht direkt verschlüsselt werden, muss er sie in Zahlen übersetzen, die in $\mathbb{Z}_n$ enthalten sein müssen.

3. Mit der Chiffrierfunktion 15^{28} verschlüsselt Bob alle Buchstaben und übermittelt den ermittelten Geheimtext an Alice.

$$C = E(M) = M^e \mod n \tag{15}$$

In Abbildung 1 wurde der Ablauf einer Verschlüsselung mit dem Programm **Cryptool 2** veranschaulicht. Aus Gründen der Übersichtlichkeit wurde hier anstelle der einzelnen Buchstaben der gesamte Text in eine Zahl umgewandelt und die Schlüsselgenerierung wurde dem Programm überlassen.

Um Bobs Nachricht lesen zu können, muss sie den Chiffretext mit der Dechiffrierfunktion 16 entschlüsseln und wieder zurück in Buchstaben konvertieren.[30]

$$M = D(C) = C^d \mod n \tag{16}$$

[28] Ertel, *Angewandte Kryptographie*, S. 77.
[29] erstellt vom Verfasser
[30] Ertel, *Angewandte Kryptographie*, S. 77.
[31] erstellt vom Verfasser

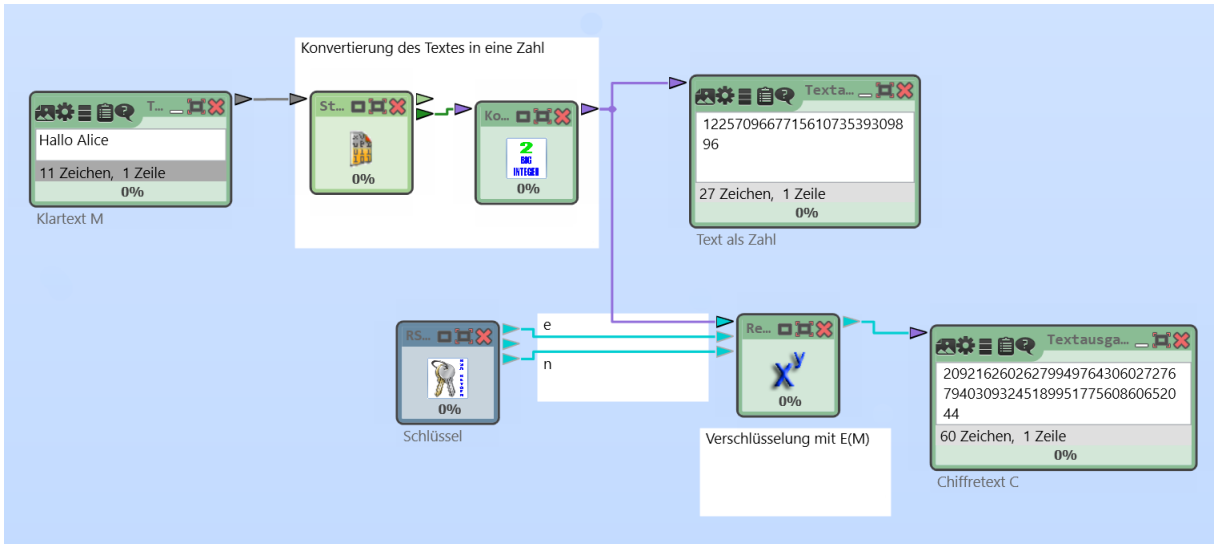


Abbildung 1: Veranschaulichung des Verschlüsselungprozesses[29]

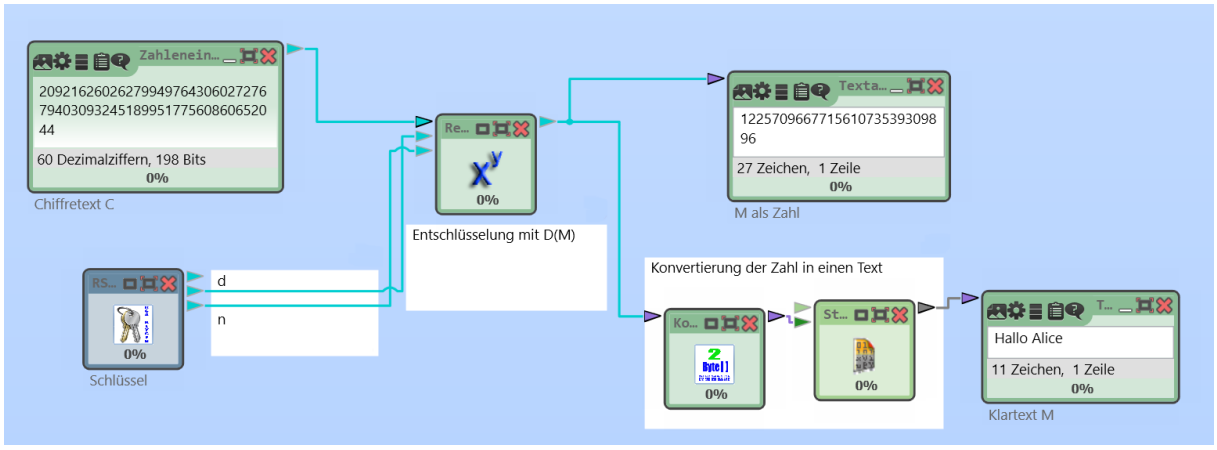


Abbildung 2: Veranschaulichung des Entschlüsselungprozesses[31]

3.5 Digitale Signatur

Neben dem Verschlüsseln von Nachrichten wird das RSA-Verfahren auch häufig dazu verwendet um digitale Nachrichten zu signieren. Bei einer *digitalen Signatur*, oft auch *elektronische Unterschrift* »unterschreibt« ein Teilnehmer A seine Nachricht oder Datei indem er eine nur ihm bekannten *Signaturfunktion* s_A auf diese anwendet (Vgl. Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*, S. 40–43). Neben der geheimen Signaturfunktion besitzt jeder Teilnehmer auch noch eine *Verifikationsfunktion* v_A, welche er öffentlich zugänglich macht oder zusätzlich mit einer signierten und einer unsignierten Version der Nachricht mitversendet. Mit dieser kann der Empfänger die signierte Nachricht entschlüsseln und falls sich der dechiffrierte Text mit dem unsignierten deckt, ist die Identität des Absenders bewiesen, da nur der Besitzer des privaten Schlüssel den Text so verschlüsseln konnte, dass der Chiffretext sich nach Anwendung der öffentlichen Verifikationsfunktion dem Klartext entspricht[32].

$$SIG = s_A(M) \tag{17}$$

$$v_A(SIG) = M \tag{18}$$

Bei der Verwendung des RSA-Verfahrens wird als *Signaturfunktion* die Funktion verwendet, welche bei der Verschlüsselung die Dechiffrierfunktion 16 darstellt:

$$SIG = s_A(M) = M^d \mod n \tag{19}$$

Und als *Verifikationsfunktion* die Chiffrierfunktion 15

$$M = v_A(SIG) = SIG^e \mod n \tag{20}$$

Da es aber unpraktikabel ist immer gesamte Dateien zu signieren, da es zu lange dauert und in zu großen Signaturdateien resultiert, wird in der realen Anwendung meist eine *Hashfunktion* verwendet, welche einen kleinen »Fingerabdruck« der Datei erstellt und nur dieser wird signiert. Beim Verifizieren wird ebenfalls nur das Ergebnis der auf die Datei angewendeten Hashfunktion mit der Signatur durch die Verifikationsfunktion verglichen.

[32] Vgl. Wätjen, *Kryptographie*, S. 68.

3.6 Mathematischer Beweis des Verfahrens

Um den RSA-Algorithmus mathematisch zu beweisen, muss bestätigt werden, dass die Funktionen E 15 und D 16 invers zueinander sind und für alle $M \in \mathbb{Z}_n$ gilt:[33]

$$D(E(M)) = E(D(M)) = M \tag{21}$$

»Nunächst gilt nach Rechenregeln für die MOD-Funktion:«[34]

$$(M^e \mod n)^d \mod n = K^{ed} \mod n \tag{22}$$

(Eine kurze Erklärung der verwendten Rechenregeln lässt sich hier finden: *Modulares Potenzieren*) Da das modulare Inverse d in 14 als $ed \mod \Phi(n) = 1$ bestimmt wurde, gilt nach Einführung des ganzzahligen Faktors k:[35]

$$e \cdot d = k \cdot \Phi(n) + 1 \tag{23}$$

Zusammen mit 22 resultiert das in folgender Gleichung, die es zu beweisen gilt:[36]

$$M = M^{k\Phi(n)+1} \mod n = M \cdot M^{k\Phi(n)} \mod n \tag{24}$$

Sind nun M und n teilerfremd, kann der *Satz von Fermat-Euler* benutzt werden, um den Beweis zu erbringen. Nach Bronštejn u. a., *Taschenbuch der Mathematik*, S. 390 lautet dieser auf den vorliegenden Fall bezogen:

$$M^{\Phi(n)} \mod n = 1 \tag{25}$$

Mit

$$M^{k\cdot\Phi(n)} \mod n = \left(M^{\Phi(n)} \mod n\right)^k \mod n = 1^k \mod n = 1 \tag{26}$$

[33] Vgl. Ertel, *Angewandte Kryptographie*, S. 78.
[34] Dankmeier, *Grundkurs Codierung*, S. 282.
[35] Vgl. Wätjen, *Kryptographie*, S. 72.
[36] Vgl. Dankmeier, *Grundkurs Codierung*, S. 282.

und

$$M \cdot M^{k\Phi(n)} \mod n = \left(M \mod n \cdot M^{k\Phi(n)} \mod n\right) \mod n \tag{27}$$
$$= M \mod n \mod n = M$$

da $M < n$ und somit $M \mod n$ wieder M ergibt, ist $M = M^{k\Phi(n)+1} \mod n$, was zu beweisen war, bewiesen.
Für den Randfall, dass M nicht teilerfremd zu n ist, sondern ein Vielfaches von q oder p ist, ist ebenfalls ein Beweis vorhanden, diesen hier aufzuführen würde jedoch den Rahmen sprengen, es soll jedoch gesagt werden, dass er teilweise auf dem eben beschriebenen Vorgehen basiert.

3.7 Bewertung

Die größte Vorteil des RSA-Verfahrens ist wie bei Public-Key-Kryptosystemen allgemein die Einfachheit der Schlüsselverteilung, welche es für viele Anwendungen überhaupt erst brauchbar macht (Vgl.Dankmeier, *Grundkurs Codierung*, S. 285). Ein weiterer positiver Punkt im Bezug auf die Schlüssel ist, dass hier im Gegensatz zu manch anderen Verfahren diese für jeden Teilnehmer nur einmalig generiert werden müssen, was insbesondere in Anbetracht der relativ hohen Rechenintensität der Primzahlgenerierung wichtig ist. Auch die Möglichkeit der Signatur mit den gleichen wie zur Verschlüsselung genutzten Schlüsseln und Funktionen trägt zur großen Anerkennung bei. Wie bereits erwähnt basiert die Sicherheit auf dem *Faktorisierungsproblem*. Da dieses Problem jedoch mit neuen Algorithmen und schnelleren Rechnern immer schneller zu lösen ist, sinkt die Sicherheit. Dieses Problem kann jedoch einfach mit längeren Schlüsseln gelöst werden, was allerdings zu höheren Ansprüchen von Rechenleistung bei der Benutzung mit sich bringt.[37] So veröffentlichte *Rivest* 1977 einen mit einer 129 Dezimalstellen langen Zahl n verschlüsselte Text, für den er annahm, dass es 40 Quadrillionen Jahre benötige um diesen zu entschlüsseln. Bereits 1994 wurde er innerhalb von 8 Monaten geknackt.[38] Zur Sicherheit durch dass *Faktorisierungsproblem* gilt auch noch anzumerken, dass »Experten *glauben*, dass es kein

[37] Vgl. *Der RSA - Algorithmus*.
[38] Vgl. Wätjen, *Kryptographie*, S. 73.

effizientes [...] Ver- fahren zur Faktorisierung gibt. Bewiesen ist dies jedoch *nicht.*«[39]

3.8 praktische Anwendungen

4 Schluss/Ausblick

[39] Ertel, *Angewandte Kryptographie*, S. 80.

Literatur

[1] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie: von RSA zu Zero-Knowledge*. 8., überarbeitete Auflage. Wiesbaden: Springer Spektrum, 2015. ISBN: 978-3-8348-1927-7.

[2] Il'ja N. Bronštejn u. a. *Taschenbuch der Mathematik*. 10., überarbeitete Auflage. Edition Harri Deutsch. Haan-Gruiten: Verlag Europa-Lehrmittel - Nourney, Vollmer GmbH & Co. KG, 2016. 1233 S. ISBN: 978-3-8085-5789-1.

[3] *Bronzezeit in Europa*. URL: `https://www.lernhelfer.de/schuelerlexikon/geschichte/artikel/bronzezeit-europa-deutschland` (besucht am 03. 08. 2020).

[4] Wilfried Dankmeier. *Grundkurs Codierung: Verschlüsselung, Kompression, Fehlerbeseitigung*. 3., überarb. und erw. Aufl. Wiesbaden: Vieweg, 2006. ISBN: 978-3-528-25399-8.

[5] *Der RSA - Algorithmus*. URL: `https://www.zum.de/Faecher/Inf/RP/infschul/kr_rsa.html` (besucht am 08. 11. 2020).

[6] Wolfgang Ertel. *Angewandte Kryptographie: mit 51 Bildern und 30 Aufgaben*. 2., bearb. Aufl. München: Fachbuchverl. Leipzig im Carl Hanser Verl, 2003. ISBN: 978-3-446-22304-2.

[7] Jörn Lengsfeld. *Digitales Informationszeitalter*. URL: `https://joernlengsfeld.com/de/definition/digitales-informationszeitalter/` (besucht am 03. 08. 2020).

[8] *Modulares Potenzieren*. URL: `https://medienwissenschaft.uni-bayreuth.de/inik/material/email_nur_fuer_dich/3_verschluesseln/3.3_asymmetrisch_verschluesseln/Modulares%20Potenzieren%20-%20AB.pdf` (besucht am 07. 11. 2020).

[9] J. Pieprzyk. *Topics in Cryptology - CT-RSA 2010: The 10th Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010. ISBN: 9783642119255. URL: `https://books.google.de/books?id=crqoCAAAQBAJ`.

[10] Thomas Steinfeld. *Eulersche Phi-Funktion - Mathepedia*. URL: `https://mathepedia.de/Eulersche_Phi-Funktion.html` (besucht am 03. 11. 2020).

[11] J. Swoboda, M. Pramateftakis und S. Spitz. *Kryptographie Und IT-Sicherheit: Grundlagen Und Anwendungen*. Studium : IT-Sicherheit Und Datenschutz. Vieweg+Teubner Verlag, 2008. ISBN: 978-3-8348-9473-1. URL: `https://books.google.de/books?id=2oQkBAAAQBAJ`.

[12] Dietmar Wätjen. *Kryptographie: Grundlagen, Algorithmen, Protokolle*. 2. Aufl. Heidelberg: Spektrum, Akad. Verl, 2008. ISBN: 978-3-8274-1916-3.

Erklärung

Ich versichere, dass ich die Seminararbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benützt habe.

....

Ort und Datum Unterschrift