DHBW
Duale Hochschule
Baden-Württemberg
Karlsruhe

Grundlagen der Kryptographie und Steganographie

Studienarbeit

für die Prüfung zum

Bachelor of Science

des Studiengangs Informatik / Angewande Informatik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

Jens Döllmann

Abgabedatum 17. Mai 2021

Bearbeitungszeitraum	2 Semester
Matrikelnummer	8876462
Kurs	TINF18B4
Gutachter der Studienakademie	Ralf Brune

Inhaltsverzeichnis

1 Einleitung **2**

1.1 Symmetrische Verschlüsselung 4

1.2 Modulare Arithmetik 5

Kapitel 1

Einleitung

Redet man heutzutage über das Thema Kryptographie, sind im Gespräch wahrscheinlich Themen wie E-Mail-Verschlüsselung, Internetprotokolle oder Anwendungen im Bankenwesen. Auch bekannt sind die Angriffe auf kryptographische Systeme, wie zum Beispiel die Entzifferung der durch die Enigma-Chiffriermaschine verschlüsselten deutschen Funksprüche während des Zweiten Weltkrieges. Es scheint als wäre Kryptographie stark mit den modernen elektronischen Kommunikationstechniken verbunden. Dies ist allerdings nicht so: Frühe Formen der Kryptographie gehen zurück bis etwa 2000 v. Chr., als bereits im antiken Ägypten neben den Standard-Hieroglyphen zusätzlich auch „geheime“ Zeichen verwendet wurden (Paar und Pelzl 2010, S. 2). Es werden prinzipiell zwei unterschiedliche kryptographische Verfahren unterschieden, diese sind Symmetrische- und Asymmetrische Algorithmen. Die symmetrische Verschlüsselung ist seit langer Zeit ein fester Bestandteil der Kryptographie, mit bekannten historischen Verfahren wie die Cäsar-Chiffre welche bereits im antiken Rom für das Verschlüsseln von Nachrichten verwendet wurde. Asymmetrische Verschlüsselung hingegen ist eine gänzlich neue Form der Kryptographie, Whitfield Diffie, Martin Hellman und Ralph Merkle haben die Idee im Jahr 1976 erstmalig öffentlich eingeführt (ebd., S. 3). Eine Übersicht über das Gebiet der Kryptographie ist in Abbildung 1.1 zu sehen (ebd., S. 3). Es ist zu bemerken, dass an oberster Stelle nicht die Kryptographie, sondern der Oberbegriff Kryptologie zu finden ist, welche sich in die zwei großen Bereiche unterteilt:

Kryptographie Die Wissenschaft eine Nachricht so zu verändern, dass ihr Sinn nur von dem Empfänger verstanden werden kann, für den sie bestimmt ist.

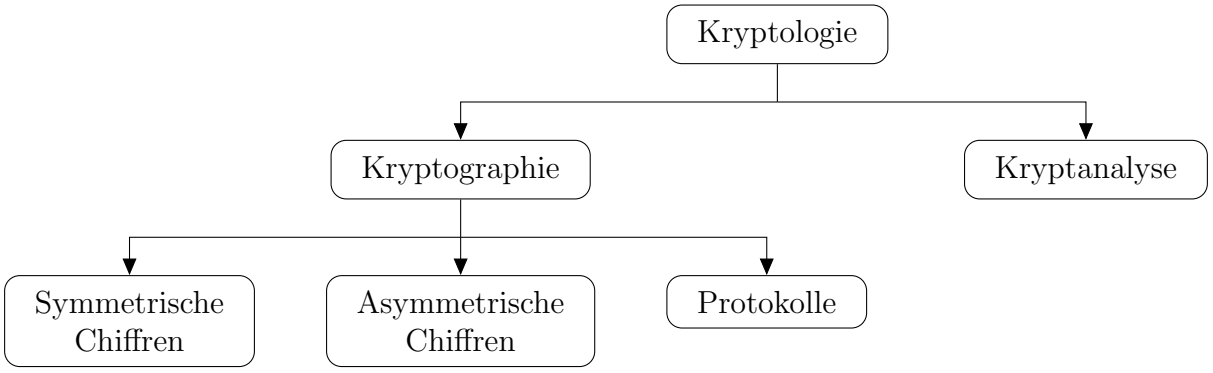

Abbildung 1.1: Die Kryptologie und ihre Untergebiete

Kryptanalyse Die Wissenschaft ein kryptographisches System zu analysieren mit dem Ziel mögliche Schwachstellen aufzudecken. Die Kryptanalyse ist ein äußerst wichtiger Teil der Kryptologie. Ohne Personen welche versuchen ein kryptographisches System zu brechen, wird man nie herausfinden können ob das System wirklich sicher ist. Ein starkes Kryptoverfahren sollte dem *Kerckhoffs's principle* unterliegen, welches im Jahr 1883 von Auguste Kerckhoffs postuliert wurde und von Paar und Pelzl durch folgende Definition beschrieben ist (2010, S. 11):

Definition 1.0.1 (*Kerckhoffs's principle*)**.** *„A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.“*

Auf den ersten Blick scheint das *Kerckhoffs's principle* nicht sonderlich intuitiv. Es sei einfach zu glauben, dass ein System sicherer sein muss, wenn die Details der Implementierung geheim gehalten werden. In der Regel ist dies aber nicht so. Ein Kryptoverfahren bleibt nicht für immer geheim und die Vergangenheit hat gezeigt, dass ein System dessen geheimes Design an die Öffentlichkeit gelangt, fast immer unsicher ist. Ein hierfür gutes Beispiel ist das Content Scrambling System (CSS) für das Verschlüsseln von DVD-Videoinhalten. Trotz großer Bemühungen der Industrie die Funktionsweise von CSS geheim zu halten, gelang das Design durch Reverse Code Engineering dennoch schnell an die Öffentlichkeit. Es zeigten sich Mängel in der Implementierung, welche das Brechen der Verschlüsselung mit sehr geringen Aufwand ermöglichten (Barry 2004).

1.1 Symmetrische Verschlüsselung

Denkt man an die Teilbereiche der Kryptographie, ist die Symmetrische Verschlüsselung das wohl klassischste Beispiel. Zwei Parteien kommunizieren mit einem Algorithmus zum Ver- und Entschlüsseln von Nachrichten und haben sich auf einen gemeinsamen geheimen Schlüssel geeinigt. Wie es in der Literatur sehr beliebt ist, wird die Idee der symmetrischen Verschlüsselung mit einem einfachen Beispiel eingeführt (Paar und Pelzl 2010, S. 4–6): Zwei Parteien Alice und Bob möchten über einen unsicheren Kanal Nachrichten untereinander austauschen. Ein unsicherer Kanal ist hierbei lediglich die Kommunikationsstrecke, z.B. das Internet, die Luftschnittstelle bei WLAN und Mobilfunk oder jedes andere Medium, über das sich digitale Daten übertragen lassen.

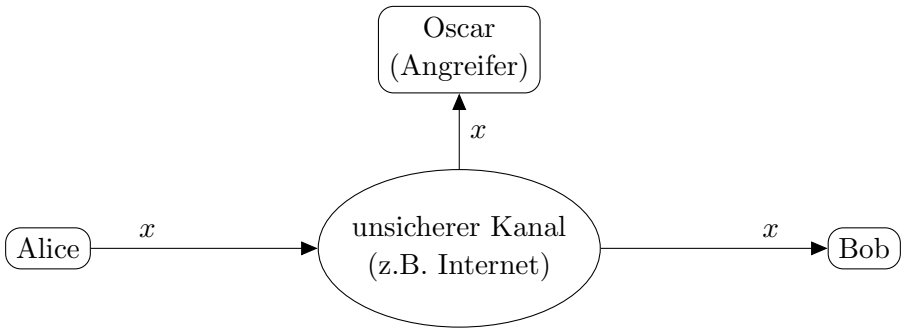

Abbildung 1.2: Kommunikation über einen unsicheren Kanal

Es ist klar warum Alice und Bob gerne geheime Nachrichten austauschen würden. Alice möchte sich an ihrem Bankkonto anmelden und sendet ihr Passwort zu Bob. Ein potenzieller Angreifer Oscar soll die Passwörter von Alice nicht in Klartext mitlesen können. In einer solchen Situation bietet die Symmetrische Verschlüsselung eine gute Lösung: Bevor Alice ihr Passwort sendet, verschlüsselt sie es mit einem symmetrischen Algorithmus. Bob invertiert die Verschlüsselung und erhält die unverschlüsselte Nachricht. Wurde für die Verschlüsselung ein sicherer Algorithmus gewählt, erscheint die Nachricht für Oscar nur wie eine zufällige Folge von Bits.

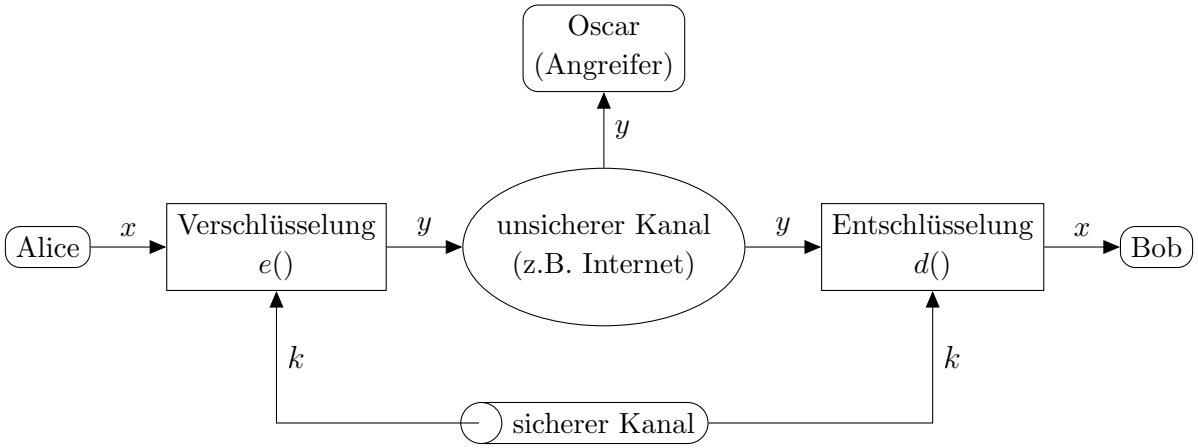

Abbildung 1.3: Kommunikation mit symmetrischer Verschlüsselung

Die Variablen x, y und k aus Abbildung 1.3 haben in der Kryptographie eine besondere Bedeutung:

- x ist der Klartext (engl. *plaintext*).
- y ist das Chiffrat oder der Geheimtext (engl. *ciphertext*).
- k ist der Schlüssel (engl. *key*).
- $e(\cdot)$ ist die Verschlüsselung (engl. *encryption*).
- $d(\cdot)$ ist die Entschlüsselung (engl. *decryption*), d.h. die Umkehrfunktion von e.

Für die Symmetrische Verschlüsselung wird der geheime Schlüssel k benötigt. Dieser muss vor der Kommunikation auf einem sicheren Weg zwischen Alice und Bob verteilt werden.

1.2 Modulare Arithmetik

Fast alle kryptographischen Algorithmen, sowohl Symmetrische als auch Asymmetrische Chiffren, basieren auf Arithmetik in einer endlichen Menge von ganzen Zahlen (Paar und Pelzl 2010, S. 13). Dies steht im Gegensatz zu der Mathematik (und dem Alltagsleben) in der wir es gewöhnt sind in unendlichen Mengen zu rechnen, z.B. die natürlichen Zahlen oder die reellen Zahlen. Die modulare Arithmetik, d.h. die Division mit Rest, bietet eine gute Möglichkeit um in diesen begrenzten Mengen rechnen zu können.

Lemma 1.2.1 (Remmert und Ullrich 2008, S. 179–180)**.** *Folgende Aussagen über drei ganze Zahlen a, b, m, wobei $m > 0$, sind äquivalent:*

i) a und b lassen bei Division mit Rest durch m denselben Rest.

ii) Die Differenz $a - b$ ist durch m teilbar.

Beweis. $\exists\, q_1, q_2, r_1, r_2 \in \mathbb{Z}$
Es seien $a = q_1 m + r_1$ und $b = q_2 m + r_2$ mit $0 \leq r_1, r_2 < m$, die Gleichungen, die bei Division mit Rest entstehen.
i) $\Rightarrow$ ii):
Es gilt $r_1 = r_2$ zu zeigen: $m|(a - b)$.

$$\begin{aligned} a - b &= q_1 m + r_1 - q_2 m + r_2 \\ a - b &= (q_1 - q_2)m + r_1 - r_2 \\ \Rightarrow a - b &= (q_1 - q_2)m \\ \frac{a-b}{m} &= q_1 - q_2 \end{aligned}$$

Aus den letzten beiden Gleichungen folgt: $m|(a - b)$.
ii) $\Rightarrow$ i):
Es gilt $m|(a - b)$ zu zeigen: $r_1 = r_2$.

$$\begin{aligned} & m|(a - b) \\ \Rightarrow\ & m|(q_1 m + r_1) - (q_2 m + r_2) \\ \Rightarrow\ & m|(q_1 - q_2)m + (r_1 - r_2) \end{aligned}$$

m teilt das Ganze und $m|(q_1 - q_2)m$ weshalb folgen muss: $m|(r_1 - r_2)$. [1]
$r_1 - r_2$ muss ein Vielfaches von m sein oder 0. Wegen des Bereiches in dem r_1 und r_2 sich befinden ist die einzige Lösung $r_1 - r_2 = 0$. Es folgt: $r_1 = r_2$. □

[1] Nach der Regel wenn $a|x$ und $a|y \Rightarrow a|x - y$. Also mit konkreten Werten $m|(q_1 - q_2)m + (r_1 - r_2) - (q_1 - q_2)m \Rightarrow m|(r_1 - r_2)$.

Nach Gauß nennt nennt man zwei Zahlen $a, b \in \mathbb{Z}$, die bei der Division durch m denselben Rest ergeben, *kongruent modulo m*. Anstelle der schwerfälligen Teilbarkeitsschreibweise $m|(a-b)$ führte Gauß folgende Schreibweise ein (Remmert und Ullrich 2008, S. 180):

$$a \equiv b \mod m \quad \text{oder kürzer:} \quad a \equiv b \quad (m)$$

Literaturverzeichnis

Barry, Mark (Juni 2004). *Cryptography in Home Entertainment*. Einsichtsname: 03.01.2021. URL: http://www.math.ucsd.edu/~crypto/Projects/MarkBarry/index.htm.

Paar, Christof und Jan Pelzl (2010). *Understanding Cryptography*. Springer. ISBN: 978-3-642-04100-6.

Remmert, Reinhold und Peter Ullrich (2008). *Elementare Zahlentheorie*. 3. Aufl. Birkhäuser. ISBN: 978-3-7643-7730-4.