# 1 Einleitung

*Ich weiß nicht, was soll es bedeuten [...]* – H. Heine

In der Vergangenheit galt die Kryptographie als die Lehre der Methoden, den Inhalt vertraulicher Botschaften durch Verschlüsseln zu verbergen.[1] Begrifflich unterschied man davon die Kryptoanalyse, d.h. den Versuch, die Verschlüsselung zu brechen, und die Kryptologie als Sammelbegriff für Kryptoanalyse und Kryptographie.

Schon in der Antike entwickelten die Menschen Verfahren, um ihre Botschaften vor unbefugter Einsichtnahme, einem sogenannten „Angriff", zu schützen. Bis in die frühe Neuzeit hinein dominierten steganographische Methoden, mit denen man versuchte, sogar die Existenz einer geheimen Botschaft zu verbergen. Beispiele dafür sind die Verwendung von Geheimtinte und die Absprache unverdächtiger Formulierungen als Stichworte für bestimmte Geheimnisse. Daneben verwendete man aber auch Permutations- und Substitutionschiffren und entwickelte Methoden, diese Chiffren zu brechen.

Erst im 19. Jahrhundert wurde die Kryptologie systematisiert und formalisiert. Im 20. Jahrhundert beschleunigte die maschinelle Datenverarbeitung und -übermittlung die Entwicklung der Kryptologie. So gelang es den Briten während des zweiten Weltkrieges, die Chiffre der deutschen Enigma, einer Familie elektromechanischer Verschlüsselungsmaschinen, zu brechen. Der britische Geheimdienst verwendete Spezialrechner, die eigens für diesen einen Zweck konstruiert worden waren.

## 1.1 Die moderne Kryptographie

*Cryptography is about communication in the presence of adversaries.* – R. Rivest

Früher war die Kryptographie vor allem für Militärs, Geheimdienste und Diplomaten wichtig. Das hat sich in jüngster Zeit drastisch geändert! Ausschlaggebend dafür sind die zunehmende Bedeutung von Computern und deren Vernetzung, besonders aber der Aufbau eines weltweiten Computernetzwerkes, des Internet.

Viele Internet-Nutzer „ahnen nicht, welche Spur sie mit jedem Mausklick hinterlassen und wie einfach es ist, Computer anzuzapfen" [30]. Nationale Datenschutzmaßnahmen sind in einem weltweiten Computernetzwerk wirkungslos. Mit juristischen oder organisatorischen Mitteln allein kann man keine Abhilfe schaffen, zumal das Internet dezentral

[1] Auf griechisch bedeutet „krýptein" soviel wie „verbergen".

organisiert ist, niemandem gehört und in keinem Staat ansässig ist. Nutzer und Anbieter sind trotzdem nicht völlig hilflos den „Räubern im Netz“ [30] ausgeliefert. Oft ist es möglich, sich in Eigeninitiative zu schützen, z.B. indem sich die Kommunikationsteilnehmer auf den Einsatz kryptographischer Verfahren verständigen. Die Kryptographie bietet hier zwar kein Allheilmittel, ist aber eine Schlüsseltechnologie für die Realisierung sicherer Kommunikation – auch in anderen Medien als dem Internet.

In der Vergangenheit dienten, wie bereits erwähnt, kryptographische Methoden der Geheimhaltung des Inhaltes vertraulicher Botschaften. Dagegen ist heute die Kryptographie als weit umfassendere Wissenschaft anzusehen. Der Einsatz kryptographischer Verfahren dient heute meist einem oder mehreren der folgenden Ziele:

- Der Geheimhaltung von Daten.
- Der Sicherstellung der Authentizität von Daten.
- Der Authentifizierung von Kommunikationsteilnehmern.
- Der Ermöglichung anonymer Kommunikation.

Alle Algorithmen und Protokolle, die der Erreichung dieser Ziele dienen, bezeichnen wir als *Kryptosysteme*. Zunehmend bürgert es sich heute ein, die Kryptoanalyse als Teilgebiet der Kryptographie zu sehen, also nicht mehr zwischen Kryptographie und Kryptologie zu unterscheiden. Entsprechend verfahren wir auch in der vorliegenden Arbeit.

## 1.2 Der Entwurf von Kryptosystemen: Drei methodische Ansätze

*Cryptography [...] is finally, slowly, and painfully becoming a science.* – J. Leichter

In der modernen Kryptographie kennt man drei Ansätze, die *Sicherheit* eines Kryptosystems zu beschreiben: Den informationstheoretischen, den komplexitätstheoretischen und den systembasierten Ansatz.

Der **informationstheoretische Ansatz** bietet unbedingte Sicherheit. Das heißt, nicht einmal Angreifer mit unbeschränkter Rechenkapazität können ein informationstheoretisch sicheres Kryptosystem brechen. Die Vernam-Chiffre, siehe Abschnitt 2.2, ist informationstheoretisch sicher, jedoch fast immer unpraktikabel. Überhaupt führt der informationstheoretische Ansatz nur selten zu praktikablen Kryptosystemen.[2]

Probleme, die ein Angreifer mit unbeschränkter Rechenkapazität theoretisch lösen kann, können für reale Angreifer praktisch unlösbar sein. Auf dieser Überlegung basiert der

[2] Auf einzelnen Teilgebieten der Kryptographie hat der informationstheoretische Ansatz sehr wohl zu unbedingt sicheren *und* praktikablen Kryptosystemen geführt. Dies gilt insbesondere für *Secret Sharing* Systeme und *Authentication Codes* (siehe Kapitel 10 und 11 in [67]).

**komplexitätstheoretische Ansatz.** Die Komplexitätstheorie betrachtet Probleme und versucht, die inhärente Schwierigkeit dieser Probleme zu bestimmen. Bezüglich eines Rechenmodells bezeichnet man die mindestens erforderlichen Ressourcen zum Lösen eines Problems als die *Komplexität* (also die *‚Schwierigkeit'*) des Problems. Übliche Berechnungsmodelle sind z.B. Turingmaschinen und Boolesche Schaltkreise. Das Ziel des komplexitätstheoretischen Ansatzes in der Kryptographie besteht darin, Angriffe auf Kryptosysteme zu formalisieren und Kryptosysteme zu finden, die anzugreifen beweisbar *praktisch unmöglich* ist. Üblicherweise betrachtet man in der Komplexitätstheorie Kryptosysteme in Abhängigkeit von einem Sicherheitsparameter. Ein Kryptosystem gilt als *sicher*, wenn es nur mit überpolynomiellem Ressourceneinsatz gebrochen werden kann. Eine Wahrscheinlichkeit gilt als *signifikant*, wenn es ein Polynom gibt, dessen Kehrwert schneller gegen Null geht als die Wahrscheinlichkeit. Wir sprechen in diesem Zusammenhang von der *asymptotischen Sichtweise.*

Der **systembasierte Ansatz** ist eher pragmatischer Natur. Beruhend auf „Versuch und Irrtum" (Preneel [50], Abschnitt 1.4.3) haben sich bestimmte kryptanalytische Prinzipien herausgebildet, die zu erfolgreichen Angriffen auf ältere Kryptosysteme geführt haben. Beim Entwurf neuer Kryptosysteme versucht man, geeignete Lehren aus dem Scheitern der älteren Systeme zu ziehen. Kryptanalytische Prinzipien, die in den letzten Jahren zu erfolgreichen Angriffen geführt haben, sind z.B. die differentielle und die lineare Kryptanalyse, siehe dazu den Übersichtsartikel von Schneier [59].

Wenn der **informationstheoretische Ansatz** zu praktikablen Kryptosystemen führt, ist er den konkurrierenden Ansätzen vorzuziehen. Dieser Fall ist jedoch eine seltene Ausnahme. Sehr oft sind die praktischen Anforderungen an ein Kryptosystem so, daß man sogar beweisen kann, daß es kein informationstheoretisch sicheres Kryptosystem gibt, welches die gestellten Anforderungen erfüllt. Ein einfaches Beispiel, das schon auf Shannon [64] zurückgeht, ist die Forderung, *‚viel Information'* verschlüsselt mit Hilfe eines *‚kleinen Schlüssels'* über einen unsicheren Kanal zu übermitteln. Im folgenden behandeln wir den informationstheoretischen Ansatz nicht weiter. Allerdings werden bei den Beweisen in Abschnitt 4 teilweise Methoden aus der Informationstheorie angewendet.

Wegen seiner pragmatischen Vorgehensweise, die auf Versuch und Irrtum basiert, kann man von dem **systembasierten Ansatz** kaum sagen, er führe zu systematischen Entwurfsmethoden für Kryptosysteme. Allerdings wird auch bei Anwendung des systembasierten Ansatzes oft versucht, die Frage nach der Sicherheit des entworfenen Kryptosystems mit formalen Methoden zu behandeln. So beweist Lai [27], daß die von ihm entworfene IDEA-Blockchiffre nicht durch differentielle Kryptanalyse gebrochen werden kann. Der prinzipielle Nachteil des systembasierten Ansatzes besteht darin, daß man beim Entwurf neuer Kryptosysteme stets nur auf bekanntgewordene kryptanalytische Prinzipien *reagiert*, während der informationstheoretische und der komplexitätstheoretische Ansatz geeignet sind, auch neue kryptanalytische Methden *vorwegzunehmen.* Trotzdem ist der systembasierte Ansatz in der Praxis sehr erfolgreich. Manche Autoren bezweifeln sogar generell den Nutzen des komplexitätstheoretischen Ansatzes für den

Entwurf praktikabler Kryptosysteme.[3]

Traditionell sucht die **Komplexitätstheorie** meist nach asymptotischen Aussagen. Ihr Ansatz in der Kryptographie beschränkt sich meistens sogar auf die folgende Sichtweise, die wir in dieser Arbeit etwas vereinfachend als *asymptotische Sichtweise* bezeichnen: Ein Kryptosystem ist *effizient*, wenn es in Polynomialzeit berechnet werden kann, und es ist *sicher*, wenn alle Angriffe superpolynomielle Zeit benötigen. Als *Theorie* versucht die Komplexitätstheorie primär einen abstrakten Erkenntnisgewinn zu erreichen. Asymptotische Aussagen sind in der Kryptographie wertvoll, weil sie von vielen Details abstrahieren. Der wichtigste Beitrag, den die Komplexitätstheorie bisher in der Kryptographie geleistet hat, besteht in der genauen Definition und Überprüfung von Konzepten, die ohne die Komplexitätstheorie vage geblieben wären. Aber für den Entwurf praktikabler Kryptosysteme sind asymptotische Aussagen wenig hilfreich. Eine asymptotische Aussage über den Aufwand, ein Kryptosystem zu brechen, liefert keinen Hinweis darauf, wie groß der Sicherheitsparameter bei einer praktischen Realisierung des Kryptosystems gewählt werden muß, um gegebenen Sicherheitsanforderungen zu entsprechen. Glücklicherweise sind die Beweistechniken aus der Komplexitätstheorie oft stark genug, um Aussagen treffen zu können, die genau genug für den Entwurf praktikabler Kryptosysteme sind.

## 1.3 Quantifizierte Reduktionen

*One key technique, however, is [...] the 'reduction'.* – D.S. Johnson

Eine Standardmethode bei der Programmierung ist die Verwendung von Unterprogrammen. Das komplexitätstheoretische Gegenstück zum Unterprogramm ist das *Orakel*. Ein Algorithmus $A$ mit einem $P$-Orakel verhält sich wie jeder andere Algorithmus, nur kann er ein Orakel aufrufen wie ein Unterprogramm, das bei Eingabe einer Instanz des Problems $P$ eine entsprechende Lösung liefert. Bei der Laufzeit von $A$ zählt jeder Orakel-Aufruf als ein Elementarschritt. Wenn $A$ effizient das Problem $P_A$ löst, ist $A$ eine *Reduktion* von $P_A$ auf $P$, und das Problem $P_A$ ist auf das Problem $P$ *reduzierbar*. Die Reduktion $A$ erlaubt es uns, die Komplexitäten der Probleme $P$ und $P_A$ zu vergleichen: Wenn das Problem $P$ effizient lösbar ist, dann auch das Problem $P_A$. Umgekehrt gilt genauso: Wenn $P_A$ nicht effizient lösbar ist, dann erst recht nicht $P$.

Der folgende Satz ist die Grundlage für den Sicherheitsbeweis der public-key Chiffre von Rabin [51]. Für uns liefert dieser Beweis ein erstes Beispiel für eine Reduktion.

**Satz 1.1**
*Sei $n$ das Produkt zweier Primzahlen. Wenn es einen effizienten probabilistischen Algorithmus gibt, der mit signifikanter Wahrscheinlichkeit zu einem zufälligen quadratischen*

[3] Besonders deutlich wird Daemen [11]: "*Complexity theory is a powerful tool in an important part of cryptography. However, in the case of practical conventional cryptography, we believe that its relevance is marginal. By practical conventional cryptography we mean symmetric block ciphers, stream ciphers and cryptographic hash functions that actually have to be implemented and used. In our opinion the complexity theoretical way of thinking encourages poor design.*" (Hervorhebung im Original!)

*Rest $y(\mathrm{mod} n)$ eine Wurzel $x$ mit $x^2 \equiv y(\mathrm{mod} n)$ findet, dann gibt es einen effizienten Algorithmus, $n$ zu faktorisieren.*

**Beweis:** Wir betrachten den folgenden Algorithmus:

1. Wähle gemäß Gleichverteilung eine zufällige Zahl $r \in \mathbb{Z}_n$.
2. Berechne $y := r^2 \bmod n$.
3. Berechne $t := \mathrm{ggT}(y, n)$.
4. Ist $t > 1$, dann ist $t$ ein nichttrivialer Teiler von $n$; beende den Algorithmus.
5. Berechne mit Hilfe eines Orakels einen Wert $x$ mit $x^2 \equiv y \pmod n$.
6. Wenn $x \equiv \pm r \pmod n$, dann gib 1 aus. Sonst gib $\mathrm{ggT}(x + r, n)$ aus.

Ist $\mathrm{ggT}(y, n) = 1$, dann hat der quadratische Rest $y$ vier Quadratwurzeln modulo $n$, unter anderem $r$ und $-r$. Mit der Wahrscheinlichkeit 0,5 ist $x \notin \{r, -r\}$, und in diesem Fall ist $\mathrm{ggT}(x + r, n)$ ein nichttrivialer Teiler von $n$. □

Im Sinne der asymptotischen Betrachtungsweise ist Satz 1.1 eine durchaus befriedigende Aussage. Wenn wir aber die Rabin public-key Chiffre konkret realisieren wollen und davon ausgehen, daß es praktisch unmöglich ist, eine geeignet gewählte Zahl $n$ zu faktorisieren, müssen wir uns mit der folgenden Frage beschäftigen: *Mit wieviel* Verlust *ist die Reduktion im Beweis von Satz 1.1 behaftet?*

Der Verlust bei einer Reduktion bezieht sich auf die Rechenzeit, die Anzahl der erforderlichen Orakel-Aufrufe und die Erfolgswahrscheinlichkeit. Bei Betrachtung einer Reduktion $A$ von dem Problem $P_A$ auf das Problem $P$ wollen wir das folgende wissen:

(a) Wie komplex ist der Algorithmus $A$?

(b) Wieviele Aufrufe des $P$-Orakels sind im Durchschnitt notwendig?

(c) Wenn das $P$-Orakel bei Eingabe einer Instanz des Problems $P$ mit der Wahrscheinlichkeit $p$ eine entsprechende Lösung liefert, wie groß ist die Wahrscheinlichkeit $p_A$, daß der Algorithmus $A$ eine Lösung einer Instanz des Problems $P_A$ liefert?

Der Verlust der vorliegenden Reduktion ist wie folgt zu *quantifizieren*:

(a) Algorithmus $A$ erfordert die zufällige Wahl eines Elements aus $\mathbb{Z}_n$, eine Quadratbildung modulo $n$ und die Berechnung eines ggT.

(b) Das Orakel wird genau einmal aufgerufen.

(c) Wenn das Orakel mit der Wahrscheinlichkeit $p$ eine Quadratwurzel $\bmod n$ liefert, dann liefert Algorithmus $A$ mit der Wahrscheinlichkeit $p/2$ einen nichttrivialen Teiler von $n$.