• Sogar mathematisch bewiesen – Grenzen von Mathematik an Beispielen aus der Kryptografie (Vorfassung)

Katharina Klembalski, Berlin

In diesem Artikel werden Verfahren der Kryptografie unter der Perspektive angewandter Mathematik analysiert. Insbesondere wird den Fragen nachgegangen: Was leistet Mathematik im Anwendungszusammenhang und was nicht? Sowie: Welche Konsequenzen folgen daraus? Ziel ist es Reflexionsanlässe aufzuzeigen, die das Fach mit dem „größten Absolutheitscharakter relativieren“ können und eine kritische Sicht auf typische Gebrauchsweisen von Mathematik – über die Kryptografie hinaus – unterstützen können [Fischer & Malle, 1985, S. 340]. Dazu werden an verschiedenen kryptografischen Verfahren außermathematische und innermathematische Grenzen von Mathematik beschrieben sowie unterschiedliche Formen mathematischen Schließens von einander abgegrenzt.

1 Motivation – Einleitung

Kryptografie ist ein Gebiet der angewandten Mathematik, das seit längerem für die Schule interessant ist und in unterschiedlichen Funktionen in der didaktischen Literatur diskutiert wird, z.B. [Ebner & Folkers, 2006], [Zuber, 2001]. Meine Motivation, mich mit dem Thema zu befassen gründet sich auf zwei Beobachtungen:

Während meiner ersten – länger zurückliegenden – Auseinandersetzung mit bestimmten kryptografischen Verfahren musste ich zu meiner Verblüffung feststellen, dass zentrale Annahmen, auf denen diese Verfahren beruhen, nicht bewiesen sind. Das war für mich damals in höchstem Maße unbefriedigend und irritierend, besonders im Hinblick darauf, dass diese Verfahren täglich von vielen selbstverständlich verwendet werden. Im Rückblick ist eher meine ursprüngliche Erwartungshaltung infrage zu stellen.

Die andere Beobachtung ist eng mit der ersten verknüpft, dieser jedoch übergeordnet. So scheint gelegentlich der Überzeugungsgehalt einer Argumentation umso stärker zu sein, je mehr Mathematik enthalten ist. Das führt dazu, dass Mathematik auch dann eingesetzt wird, wenn sie nur eingeschränkt sinnvoll mit dem Gegenstand, den sie beschreiben (oder illustrieren oder begründen) soll, verknüpft werden kann. Dieser Umstand führte Davis und Hersh dazu, den Begriff der *rhetorischen Mathematik* in Abgrenzung zur *angewandten Mathematik* einzuführen, um den unterschiedlichen Gebrauch von Mathematik zu charakterisieren.[1]

Die hohe Akzeptanz von Mathematik, auf die beide Beobachtungen zurückgehen, gründet sich insbesondere auf die Erfahrungen vieler Menschen zur Wirksamkeit von Mathematik – in Schule, Beruf, Technik und Alltag – sowie auf die spezielle Schlussweise in der Mathematik. Im Sinne einer kritischen Sicht auf typische mathematische Denk- und Gebrauchsweisen, [Winter, 1996], [Fischer & Malle, 1985, S. 340], stellen sich die Fragen:

1. Was leistet Mathematik im Anwendungszusammenhang?
2. Was kann Mathematik nicht leisten?

sowie

3. Welche Konsequenzen folgen daraus im jeweiligen Kontext?

Diesen Fragen gehe ich im Folgenden anhand von Inhalten aus der Kryptografie nach. Ziel ist es, Reflexionsanlässe aufzuzeigen, die die Erfahrungen zur Wirksamkeit von Mathematik und zu ihren Schlussweisen nicht infrage stellen, aber relativieren können.

Dazu stelle ich im Folgenden außermathematische Grenzen von Mathematik anhand von Beispielen aus der Kryptografie vor, beschreibe innermathematische Grenzen speziell entlang des RSA-Verfahrens und grenze die beobachteten unterschiedlichen mathematischen Schlussweisen voneinander ab. Dabei unterstelle ich beim Leser eine prinzipielle Kenntnis der betrachteten Verfahren. Lediglich das RSA- und das One-Time-Pad-Verfahren sind im Anhang kurz beschrieben.[2]

2 Außermathematische Grenzen

Der Einsatz mathematischer Methoden ist in der Regel nur ein Element von vielen auf dem Weg zur Lösung praktischer (beispielsweise ingenieurstechnischer) Probleme. Andere sind: technische Realisierbarkeit, Kosten, Güte der Lösung oder die einfache Bedienbarkeit eines Produkts. Im Fall der Kryptografie lassen sich wechselseitige Abhängigkeiten zwischen diesen Elementen ganz natürlich beobachten, beispielsweise indem kryptografische Verfahren auf Sicherheit und Durchführbarkeit hin untersucht und verglichen werden. Dazu vier Beispiele:

1. *Sicherheit vs. Effizienz*: Das One-Time-Pad

[1] Danach lässt sich angewandte Mathematik letztlich auf ein Experiment zurückführen. Rhetorischer Mathematik fehlt diese Eigenschaft; ihre Akzeptanz gründet sich auf das hohe Vertrauen in die Mathematik.

[2] Eine übersichtliche Darstellung der hier benutzten Verfahren mit interessanter historischer Einbettung findet sich bei Engel [1979], ein hoher unterrichtspraktischer Bezug einschließlich einer Diskussion für unterschiedliche Schultypen sowie eine umfangreiche, kommentierte Literaturübersicht bietet Stohr [2008]. Einen mathematisch umfassenden Einstieg ermöglicht Buchmann [2010].

(vgl. S. 8) ist ein beweisbar sicheres und einfach durchzuführendes Verschlüsselungsverfahren. Es wird dennoch nicht eingesetzt. Ein Grund dafür ist der hohe Aufwand für die notwendige Schlüsselverwaltung. Im Gegensatz dazu kann die Sicherheit verbreiteter Verfahren wie RSA nicht bewiesen werden. Zwar wird die Chance eines erfolgreichen Angriffs von Experten als vernachlässigbar gering eingeschätzt, dennoch wird hier letztlich ein Verlust an Sicherheit aus praktischen Erwägungen in Kauf genommen.[3]

2. *Mathematische Korrektheit vs. technische Realisierbarkeit*: Primzahlen sind kritische Bausteine verschiedener kryptografischer Verfahren wie RSA, Diffie-Hellman-Schlüsseltausch u.a. Wegen der Anzahl der notwendigen Rechenschritte bekannter Algorithmen zur Identifikation einer Primzahl wird die Primalität der in der Praxis eingesetzten Zahlen nicht bewiesen. Stattdessen wird im in der Praxis häufig genutzten Miller-Rabin-Test die Chance, fälschlich eine zusammengesetzte Zahl ausgewählt zu haben, nach oben abgeschätzt. Hier geben also technische Gründe den Ausschlag.

3. *Technische Realisierbarkeit vs. Bedienbarkeit*: Um Passwörter gegen Erraten zu schützen, empfiehlt es sich, möglichst lange und möglichst zufällig erscheinende Zeichenkombinationen zu verwenden. In der technischen Ausführung spielt es praktisch keine Rolle, ob diese Zeichenketten 6 oder 30 Zeichen lang sind, für die Sicherheit des Passwortes hingegen schon. Dennoch verwenden Nutzer selten Passwörter, die länger sind als 10 Zeichen. Einige Gründe dafür sind die erhöhte Schwierigkeit, sich (mehrere) längere Passwörter zu merken, aber auch der erhöhte Aufwand der Eingabe und die Gefahr des Vertippens.

4. *Technische Realisierbarkeit vs. Kosten*: 1998-2010 wurden in Europa Bankkarten eingesetzt, die nachgewiesen unsicher waren, d.h. an einem Nachmittag gefälscht werden konnten. Ein Grund dafür war der verwendete RSA-Schlüssel, der mit 320 bit schlicht zu klein war. Technisch wäre es möglich gewesen, das Problem zu lösen. Wegen der damit verbundenen Kosten ist das nur sehr zögerlich geschehen.[4] Eine ähnliche Schlamperei wurde auch bei der – viel zu langen – Verwendung des Magnetstreifens bei EC-Karten an den Tag gelegt. Dieser hat sich seit mehr als einem Jahrzehnt als für Kartenfälschungen anfällig erwiesen, und seine Funktionalität wird schon lange durch die mittlerweile standardmäßig vorhandenen Chips auf den Karten erfüllt. Sein Gebrauch ist daher nicht mehr notwendig. Dennoch erfolgte der Austausch von Automaten und Terminals, die den Magnetstreifen nutzen, nur langsam und wurde ernsthaft erst in den letzten Jahren, nach immer höheren Schäden für die Banken, betrieben.

In den Beispielen konkurrieren mathematische mit technologischen und finanziellen Erwägungen, aber auch mit Bequemlichkeit oder schlicht fehlendem Sachverstand der Beteiligten. *Die* beste Lösung gibt es häufig nicht. Stattdessen ist zwischen verschiedenen Lösungen auszuwählen: einer effizienten, (beweisbar) sicheren, praktisch umsetzbaren oder anderen.

Die abschließende Gewichtung mathematischer und nicht mathematischer Faktoren erfolgt letztlich normativ, lässt sich also nicht aus rein mathematischen Erwägungen heraus begründen. Wesentliche Gesichtspunkte liegen außerhalb der mathematischen Kontrolle beziehungsweise stehen oft sogar im Widerspruch dazu.

3 Innermathematische Grenzen

Innermathematische Grenzen tun sich auf, wo ungelöste mathematische Fragen bestehen, aber auch in der Art der Fragestellungen, die mathematisch (nicht) zugänglich sind. In der Kryptografie führen diese Grenzen zu unterschiedlichen, teils überraschenden Konsequenzen, wie ich im Folgenen am Beispiel des RSA-Verfahrens beschreiben werde.[5]

Die Beurteilung der Sicherheit von RSA lässt sich auf zwei offene Fragen in der Mathematik zu-

[3] Achtung, hier handelt es sich um verschiedene Verwendungen des Begriffs *sicher*. Die Sicherheit von RSA (und fast aller anderen kryptografischen Verfahren) bezieht sich auf Wahrscheinlichkeiten. So kann durch „brutales“ Probieren aller möglichen Schlüssel (theoretisch) ein Verfahren gebrochen werden. Praktisch kann ein solches Vorgehen ausgeschlossen werden, weil der Erwartungswert für die mittlere Dauer dieses Vorgehens mit den vorhandenen technischen Möglichkeiten und den gewählten Parametern der Schlüssellänge zu hoch ist. Damit ist das Ereignis „RSA wird nicht geknackt“ kein sicheres Ereignis im mathematischen Sinn. Anders verhält es sich im Fall des One-Time-Pads. Zwar kann hier eine Nachricht mit allen möglichen Schlüsseln „entschlüsselt“ werden. Ein Angreifer hat jedoch – ressourcenunabhängig – keine Möglichkeit herauszufinden, welche der „entschlüsselten“ Nachrichten die richtige ist.

[4] Das Problem des zu kurzen RSA-Schlüssels war seit 1998 für eine in Frankreich genutzte Karte bekannt. Trotzdem wurde dasselbe System von einer weiteren Bank in der Schweiz noch bis mindestens 2006 verwendet. Die eingesetzten Karten waren sogar teils bis nach 2010 im Umlauf [Kehrer & Rütten, 2007]. Eine ausführliche Darstellung, die Angriffsmöglichkeiten und besonders auch fragwürdigen Stellungnahmen der betroffenen Bank enthält, ist zu finden unter: http://postcard-sicherheit.ch/
Die Kostenüberlegungen betreffen in erster Linie das Verhältnis der Kosten für die Erstellung neuer Karten und dem Austausch der Automaten gegenüber den Kosten des Schadenersatzes, den man „kulanterweise“ dem Kunden leisten muss. Der Aufwand des Kunden, seinen Schaden bzw. die Ursache seines Schadens der Bank und Händlern nachzuweisen, spielt für diese Kosten-Nutzen-Rechnung keine Rolle.

[5] RSA wird neben dem Verschlüsseln auch zum Signieren verwendet (vgl. S. 8). Ein Angreifer hat in beiden Fällen unterschiedliche Interessen: Geheime Nachrichten sollen entschlüsselt werden; gefälschte Signaturen erfordern Verschlüsseln. Im Interesse der Lesbarkeit sind die Ausführungen für den ersten Fall formuliert. Sie gelten in entsprechend inverser Begrifflichkeit bezüglich dem Verschlüsseln und dem Entschlüsseln auch für das Signieren mit RSA.

rückführen:

1. Ist es möglich, große zusammengesetzte Zahlen (ausreichend) schnell zu faktorisieren?

Bisher ist das nicht möglich, und das ist gut so, denn dieses Nicht-Berechnen-Können ist notwendig für die Eigenschaft der Asymmetrie von RSA. Die effizienteste bekannte Möglichkeit für einen Angreifer, RSA zu knacken, besteht darin, den benötigten geheimen Schlüssel mit Hilfe der Primfaktorzerlegung des öffentlich bekannten Moduls n zu berechnen. Tatsächlich liefert die Mathematik zwar die Existenz und Eindeutigkeit dieser Zerlegung, ja sogar einen konstruktiven Weg, diese zu bestimmen, beispielsweise durch Probedivision. Für praktische Zwecke ist diese Vorgehen wegen des damit verbundenen Aufwandes aber nutzlos. Hier liegt also eine innermathematische Grenze vor. **Die Erfahrung, dass es *nützlich* ist, etwas nicht berechnen oder nachweisen zu können, ist im Unterricht eher selten.**[6]

Wegen der Bedeutung der Faktorisierung für kryptografische Verfahren wurden in den letzten Jahrzehnten eine Reihe von Faktorisierungsalgorithmen entwickelt, die gegenüber der „klassischen“ erheblich schneller sind. In Verbindung mit der Zunahme der Rechengeschwindigkeit führt das dazu, dass heute bereits Zahlen mit ca. 200 Stellen schnell faktorisiert werden können, die noch vor 33 Jahren als praktisch unzerlegbar galten, vgl. [Engel, 1979, S. 42] vs. [Buchmann, 2010, S. 174]. Der Rechenaufwand dieser neuen Verfahren steigt mit zunehmender Stellenzahl des eingesetzten Moduls n aber in weit stärkerem Maß als der Aufwand für die Durchführung von RSA (fast exponentiell im Vergleich zu polynomial). Daher lässt sich eine – an die technischen Möglichkeiten angepasste – Erhöhung der Stellenzahl nicht ausgleichen, und der geheime Schlüssel bleibt für den Angreifer außer Reichweite.

Dieses für den Kryptografen günstig verlaufende „Wettrüsten“ ist von zwei Seiten bedroht. So lässt sich nicht ausschließen, dass nicht doch ein effizientes Verfahren zur Faktorisierung gefunden wird, auch wenn es Gründe gibt, die die Existenz eines solchen Algorithmus nicht plausibel erscheinen lassen. Diese Bedrohung ist daher eher grundsätzlicher Art und erscheint wenig akut, vgl. [Buchmann, 2010, S.143]. Die zweite Bedrohung erfolgt von einem Algorithmus, der sich von den bisher diskutierten deterministischen Algorithmen grundlegend unterscheidet. Der 1995 publizierte Shor-Algorithmus wurde für Quantencomputer formuliert [Shor, 1997]. Er ist nicht deterministisch, kann für bestimmte Probleme viele potentielle Lösungen gleichzeitig prüfen und wird das Faktorisierunsproblem lösen können. Glücklicherweise ist die Entwicklung von Quantencomputern noch nicht weit genug fortgeschritten: Für den aktuellen Rekord einer Faktorisierung – ausgeführt mit einem Quantencomputer – mit dem gleichzeitig auch ein Existenznachweis für die Ausführbarkeit vorliegt, wurde 15 in die Faktoren 3 und 5 zerlegt.

2. Gibt es vielleicht Angriffe, die ohne Kenntnis des geheimen Schlüssels auskommen?

Mit der Gefahr muss man leben. Im Detail muss zwischen Angriffen auf die Einwegfunktion, das Potenzieren modulo n, und solchen auf die Implementierung unterschieden werden. So ist es im ersten Fall denkbar, dass es gelingt $c = a^e \bmod n$ zu entschlüsseln, indem die e-te Wurzel direkt berechnet wird (anstatt durch Potenzieren mit d, vgl. S. 8). Ein Algorithmus, der das (in Polynomzeit) leistet, ist glücklicherweise nicht bekannt, seine prinzipielle Existenz lässt sich aber auch nicht ausschließen.

Weiterhin gibt es Angriffe, die Details der Implementierung ausnutzen, beispielsweise ungünstige Schlüsselparameter oder Seitenkanalangriffe, u.a. [Buchmann, 2010, S. 146ff] und [Ertel, 2007, S. 89f]. Sie sind durch entsprechende Modifikation des Protokolls, in dem RSA verwendet wird, leicht zu vermeiden. Tiefergehende Aussagen zur Sicherheit eines Verfahrens müssen daher immer das Protokoll mit einschließen, in dem das Verfahren verwendet wird. Bewiesen wird dabei der folgende Schluss: *Das eingesetzte Verfahren ist immun gegen den Angriff X, vorausgesetzt das Problem Y ist nur schwer berechenbar.* Es sei hervorgehoben, dass sich jede Sicherheit aus einem solchen Beweis nur auf bekannte Angriffe bezieht. Ganz abgesehen davon, dass auch dieses „schwer berechenbar“ nicht gesichert ist.

Letztlich begrenzen beide Fragestellungen den Einsatz von RSA. Und wieso gilt RSA dennoch als sicher? Was bedeutet das für die Praxis?

4 Abgrenzen mathematischer Schlussweisen

In der Ausführung von RSA und bei der Einschätzung der Sicherheit lassen sich unterschiedliche Formen mathematischer Argumentation beobachten.

[6] Andere mathematische Anwendungen, in denen Nichtwissen nützlich ist, finden sich in der Diffie-Hellmann-Schlüsselvereinbarung (diskreter Logarithmus) oder bei Zero-Knowledge-Protokollen (Quadratwurzelproblem). Auch in diesen Fällen ist die Einwegeigenschaft (vgl. S. 8) der zugrunde liegenden Funktion nicht nachgewiesen. Beispiele für nützliches Nichtwissen in der Mathematik, jenseits der Kryptografie, sind mir nicht bekannt. Für etwaige Hinweise wäre ich dankbar.

[7] Neben den Rechenregeln für Kongruenzen handelt es sich im Kern um das Lemma von Bézout und den erweiterten euklidischen Algorithmus (Schlüsselkonstruktion von RSA), den Algorithmus zum schnellen Potenzieren (Durchführung von RSA) sowie den Satz

Auf der einen Seite stehen Sätze und Algorithmen der Zahlentheorie.[7] Deren Beweise folgen den Regeln deduktiven Schließens, das oft synonym für mathematisches Schließen steht. Insbesondere sind die Schlüsse *dauerhaft*, *unpersönlich* und *in sich vollständig* [Pólya, 1975, S. 172].

Die Aussagen zur Sicherheit von RSA im vorangegangenen Abschnitt besitzen diese Eigenschaften nicht. So ist der Schluss auf Sicherheit *nicht vollständig*, da sich aufgrund der dargestellten offenen Fragen erfolgreiche Angriffe prinzipbedingt nicht ausschließen lassen. Insbesondere gilt die Reduktion eines erfolgreichen Angriffs auf das Faktorisierungsproblem nur für Angriffe auf den geheimen Schlüssel; und die Sicherheitsaussagen zu einer konkreten Implementierung von RSA beziehen sich nur auf bisher(!) bekannte Angriffsmöglichkeiten.[8] Auch unabhängig von diesen Unwägbarkeiten ist der Schluss auf die Sicherheit von RSA *nicht dauerhaft*. Eine Ursache liegt darin, dass die in der praktischen Umsetzung verwendeten Schlüssellängen auf Abschätzungen zur technischen Entwicklung beruhen, die wiederum auf Erfahrungswerte zurückgehen. Diese Erfahrungswerte unterliegen jedoch dauerhafter Veränderung. Die Einschätzung, inwieweit daher RSA tatsächlich „sicher“ ist, ist nicht objektiv entscheidbar, indivduell verschieden und damit insbesondere *nicht unpersönlich*.

Als Konsequenz folgt daraus die Notwendigkeit, den Einsatz der angewendeten Verfahren regelmäßig zu prüfen – beispielsweise im Hinblick auf die sinnvoll einzusetzende Schlüssellänge (vgl. auch Beispiel 4, S. 4). Darüber hinaus ist blindes Vertrauen nicht angebracht. Was nicht heißen muss, dass jeder Nutzer sich im Detail mit den verwendeten kryptografischen Verfahren auseinandersetzen muss. Aber eine erhöhte Grundaufmerksamkeit, das Aktuellhalten von Sicherheitssoftware sowie ein Infragestellen bzw. ein Vergleich verschiedener Expertenmeinungen scheinen angemessen.

5 Fazit – besondere Chancen für den Mathematikunterricht

Die vorgestellten Anwendungen und diskutierten Grenzen von Mathematik illustrieren in unterschiedlicher Weise, warum außermathematische Fragestellungen (fast) nie rein mathematische Antworten besitzen können. Dieser Fakt kann – mehr oder weniger explizit – an jeder Anwendung von Mathematik im Unterricht thematisiert werden. Einige Aspekte, die spezifisch sind für die Kryptografie oder im Zuge des Anwendens von Mathematik (auf nicht reinmathematische Probleme) nur selten eine Rolle spielen, sollen zum Abschluss hervorgehoben werden:

a. Die unter *Außermathematische Grenzen* betrachteten Beispiele relativieren die kryptografischen Verfahren in Bezug auf die Welt jenseits des Algorithmus. Besonders der Faktor Mensch, das größte Sicherheitsrisiko für jedes Verschlüsselungsverfahren, demonstriert, dass kein noch so sehr verbessertes kryptografisches Verfahren den sachgerechten und achtsamen Umgang mit der jeweiligen kryptografischen Anwendung ersetzen kann.[9]

b. Die *Innermathematischen Grenzen* gewinnen an Gewicht durch Gegenüberstellung mit einer Grenze, die im hier betrachteten Kontext der Kryptografie *nicht* auftritt. Dazu sei der Prozess des Anwendens betrachtet, wie er zum Beispiel im Modellierungskreislauf von Schupp [1988] in Abb. 1.1 [Lambert, 2007] dargestellt wird.

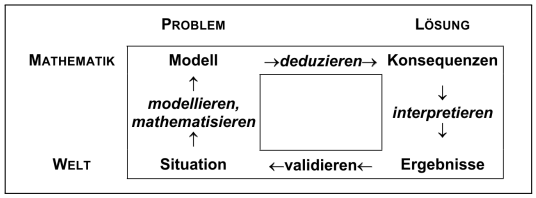

Abbildung 1.1: Anwenden von Mathematik

Bei der Diskussion mathematischer Grenzen im Anwendungsprozess liegt der unterrichtliche Fokus in der Regel auf den Übergängen Mathematik-Welt bzw. Welt-Mathematik, d.h. den Schritten *Modellieren und Mathematisieren* einserseits und *Interpretieren* andererseits. Das liegt zum einen daran, dass der Schritt des *Matematisierens und Modellierens* Schülern oft schwer fällt und daher stärker betont wird. Zum anderen beinhaltet die Mehrzahl der betrachteten Anwendungen deskriptive Modelle und macht daher Verein-

von Euler bzw. den kleinen Satz von Fermat (Nachweis der Korrektheit von RSA).

[8] Als Maßnahme, die Sicherheit dieses und anderer kryptografischer Verfahren zu erhöhen, werden die Verfahren häufig vor dem Einsatz veröffentlicht. Auf diese Weise können sie bereits im Vorfeld auf Sicherheit getestet werden, und die Gefahr erfolgreicher Angriffe wird verringert.

[9] Auch ohne vertiefte Kenntnisse der fast wöchentlich in der Tagespresse benannten Anwendungen wird deutlich, dass Schwachstellen eher selten in den eingesetzten kryptografischen Verfahren zu finden sind. Vielmehr werden fachliche Fehler in der Implementierung und Fahrlässigkeit bzw. Unwissenheit der Benutzer ausgenutzt. In jüngerer Vergangenheit betraf das diverse Kreditkartenunternehmen, Technologieunternehmen (Sony, Apple, Telekom) und Verwaltungen (verschiedene deutsche Meldeämter, Verwaltung von Patientenakten).
Dass so viele Angriffe aus Fehlern von Anbietern und Nutzern herrühren, heißt nicht, dass die eingesetzten Verfahren selbst sicher sind, sondern, dass es leichter ist, Fehler der Anwender auszunutzen, als die Verfahren selbst anzugreifen. Etwas pessimistischer wäre die Interpretation, dass erfolgreiche Angriffe auf die Verfahren selbst von Nutznießern schlicht besser geheimgehalten werden.

fachungen, Idealisierungen etc. eines realweltlichen Phänomens notwendig. Der zweite Schritt, das *Deduzieren*, verläuft – in Bezug auf Grenzen – in der Regel ereignisarm, da die Modelle gerade so gewählt sind, dass die zur Verfügung stehenden mathematischen Methoden eingesetzt werden können.[10] Daraus folgt wiederum, dass das *Interpretieren* der mathematischen Konsequenzen in erster Linie im Hinblick auf die Einschränkungen im ersten Schritt erfolgt. Zusätzlicher Interpretationsbedarf ergibt sich teilweise aufgrund mathematischer Annahmen oder Vereinfachungen während der *Deduktion*, die nun auf realweltliche Bedeutung geprüft werden müssen.

Im Fall der Kryptografie verhält es sich genau andersherum. So sind die betrachteten Objekte, die Daten, die verschlüsselt (signiert oder übermittelt) werden, bereits mathematischer Art. Vereinfachen oder Idealisieren eines realweltlichen Phänomens findet nicht statt. Die eingesetzten Algorithmen hatten vor ihrer Entwicklung kein reales Gegenstück; sie konstituieren sozusagen Realität und beschreiben diese naturgemäß vollständig – ganz ohne „störende“ Realitätselemente (wie sonst beispielsweise Reibung, abgerundete Würfelecken, inhomogene Gewichtsverteilung etc.). Die Grenze Welt-Mathematik besteht hier nicht. Die Vollständigkeit der Beschreibung suggeriert unter Umständen eine mathematische Kontrolle, die offensichtlich nicht gegeben ist. Stattdessen führt die innermathematische Auseinandersetzung mit den intendierten Eigenschaften zur (seltenen) Konfrontation mit offenen Problemen in der Wissenschaft Mathematik, d.h. innermathematischen Grenzen in der Phase des *Deduzierens*.

Diese innermathematischen Grenzen stehen im besonderen Widerspruch zur Erfahrung, dass, im schulischen Rahmen, „unlösbare“ Probleme fast immer auf Zeit bestehen (Subtraktion in $\mathbb{N}$, Nullstellen von Polynomen). Hindernisse während des *Deduzierens* (und Anpassung hinsichtlich der zugänglichen mathematischen Kenntnisse) erscheinen daher eher als Indiz für individuelle Wissenslücken und stellen nicht die Mathematik selbst infrage. Dadurch wird ein Bild von Mathematik begünstigt, das mit genug Anstrengung jedes mathematische Problem – nicht notwendig von einem selbst – gelöst werden kann, vgl. auch [Führer, 1988, S. 100]. Dass das nicht so ist, ist spätestens seit Gödel bekannt, jedoch bestehen selten Gelegenheiten, das im Unterricht zu reflektieren. Dass das Faktorisierungsproblem für die Kryptografie *nützlich* ist, ist ein zusätzliches Bonbon.

c. Die *Abgrenzung mathematischer Schlussweisen*, die Gegenüberstellung deduktiven Schließens auf der einen Seite und plausibler Schlüsse im Bereich der Anwendung auf der anderen Seite kann Gelegenheit sein, die Rolle von Mathematik in Anwendungen zu reflektieren. Von hervorgehobener Bedeutung erscheint hier eine Konnotation des deduktiven Schließens, die direkt auf die Merkmale *unpersönlich* und *dauerhaft* zurückgeht. Diese Merkmale – von Teilen des mathematischen Gehalts einer Anwendung – werden unter Umständen der Anwendung selbst zugeschrieben. Zur Verdeutlichung des resultierenden Problems soll beispielhaft Koblitz [2007, S. 977] zitiert werden (aus den Ausführungen zu *provable security* über den mathematischen Beweis)[11]:

> „The first is the notion of 100% certainty. Most people not working in a given specialty regard a “theorem” that is “proved” as something that they should accept without question. The second connotation is of an intricate, highly technical sequence of steps. From a psychological and sociological point of view, a “proof of a theorem” is an intimidating notion: it is something that no one outside an elite of narrow specialists is likely to understand in detail or raise doubts about. That is, a “proof” is something that a non-specialist does not expect to really have to read and think about.“

Diese Vorstellung von Mathematik ist im Fall des deduktiven Schließens wohl angemessen. Im Rahmen von Anwendungen von Mathematik auf außermathematische Fragestellungen ist sie das nicht. Wie das Beispiel von RSA gezeigt hat, ist die Frage der Sicherheit eben nicht vollständig deduktiv zu beantworten, sondern wird erst durch plausibles Schließen zugänglich. Der Gewinn der so gewonnenen Aussagen wird quasi dadurch „bezahlt“, dass die Eigenschaften *dauerhaft*, *unpersönlich* und *in sich vollständig* im Anwendungszusammenhang im Allgemeinen nicht gelten.[12]

Andererseits stellt diese Tatsache die Eindeutigkeit und Wahrheit mathematischer Schlüsse infrage, die für durchaus nicht wenige Schüler das

[10] Manchmal soll auch ganz pragmatisch nur der aktuelle Stoff geübt werden.

[11] Tiefergehende Überlegungen in Bezug auf die Wirkung „verborgener Mathematik“ auf und in der Gesellschaft finden sich bei Jablonka & Gellert [2007]. Unbedingt empfehlenswert ist auch [Führer, 1988].

[12] Eigentlich verhält es sich genau umgekehrt, die Eigenschaften gelten sowieso nur im Sonderfall der deduktiv geordneten (und auf Axiomen aufgebauten) Welt eigener Art, d.h. für das Produkt Mathematik, wie es beispielsweise in vielen Vorlesungen gelehrt wird. Im dominierden Teil der Begegnung mit Mathematik, d.h. beim Mathematiktreiben und Anwenden von Mathematik, treten die drei Eigenschaften fast nie gemeinsam auf.

Fach Mathematik wohltuend von anderen Fächern abheben. Im Sinne einer kritischen Sicht auf den Gebrauch von Mathematik scheint das jedoch sehr gesund zu sein.

Literatur

Buchmann, Johannes (2010): Einführung in die Kryptographie. Berlin: Springer

Ebner, Bruno & Martin Folkers (2006): Mit Mathematik unterschreiben: Ein Vorschlag für den Schulunterricht. Hildesheim: Franzbecker, 24–37

Engel, Arthur (1979): Datenschutz durch Chiffrieren: Mathematische und algorithmische Aspekte. MU, 25(6), 30–51

Ertel, Wolfgang (2007): Angewandte Kryptographie. München: Hanser

Fischer, Roland & Günther Malle (1985): Mensch und Mathematik. Mannheim: Bibliographisches Institut

Führer, Lutz (1988): Mattematik – Laterna magica der Späth-Renaissance. Staatliches Studienseminar Hameln 1978 – 1988, Festschrift

Jablonka, Eva & Uwe Gellert (2007): Mathematisation and demathematisation. In: Jablonka, Eva & Uwe Gellert (Hg.): Mathematisation – demathematisation: Social, philosophical and educational ramifications, Rotterdam: Sense Publishers, 1–18

Kehrer, Anika & Christiane Rütten (2007): Durchleuchtet – Die schwache Signatur der Schweizer Postcard. c't, (5), 210–212

Koblitz, Neal (2007): The uneasy relationship between mathematics and cryptography. Notices of the AMS, 54(8), 972–979

Lambert, Anselm (2007): Ein Einstieg in die reflektierende Modellbildung mit produktiven Aufgaben. In: Herget, Wilfried et al. (Hg.): Materialien für einen realitätsbezogenen Mathematikunterricht. Bd. 10. Mathematik im Alltag. Schriftenreihe der ISTRON-Gruppe, Hildesheim: Franzbecker, 75–89

Pólya, Georg (1975): Mathematik und plausibles Schliessen. Bd. 2. Typen und Strukturen plausibler Folgerung. Basel u.a.: Birkhaeuser

Schupp, Hans (1988): Anwendungsorientierter Mathematikunterricht in der Sekundarstufe I zwischen Tradition und neuen Impulsen. MU, 34(6), 5–16

Shor, Peter. W. (1997): Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26, 1484–1509, URL arXiv:quant-_ph/9508027v2

Stohr, Monika (2008): Unterricht in Kryptologie. Dissertation, Ludwig-Maximilians-Universität München, URL http://edoc.ub.uni-_muenchen.de/8456/1/Stohr_Monika.pdf

Winter, Heinrich (1996): Mathematikunterricht und Allgemeinbildung. Mitteilungen der Gesellschaft für Didaktik der Mathematik, 61, 37–46

Zuber, Jörn (2001): Kryptologie. Ein Wahlthema im Schuljahrgang 13. Log In, 21(3-4), 54–66

Anhang – Kurzfassung von RSA und One-Time-Pad

RSA

Das RSA-Verfahren verwendet zum Verschlüsseln eine sogenannte Einwegfunktion mit Hintertür. Konkret wird die Eigenschaft ausgenutzt, dass die Berechnung einer e-ten Potenz modulo n leicht durchzuführen ist, wohingegen sich dieser Schritt i.A. nur schwer praktisch umkehren lässt (daher Einwegfunktion). Im Gegensatz zum Wurzelziehen wie in den reellen Zahlen erfolgt die Umkehrung modulo n ebenfalls durch Potenzieren. Der hierbei verwendete Exponent d wird mit Hilfe von e und der Primfaktoren von n bestimmt. Die Kenntnis von d beziehungsweise der Primfaktoren von n entspricht der „Hintertür“. Nun kann jeder Daten verschlüsseln, indem er mit dem öffentlich bekannten Exponenten e modulo n verschlüsselt. Die Entschlüsselung erfolgt mit einem nur vom Empfänger der Nachricht bekannten geheimen Schlüssel d. Ein Angreifer muss zum Entschlüsseln d erraten beziehungsweise n faktorisieren, um d berechnen zu können. Aus diesem Grund wird n als Produkt zweier großer Primzahlen (mit ca. 300-600 Stellen) gebildet. Eine schematische Darstellung von RSA sieht somit folgendermaßen aus:

Schritt	Beispiel	mathematischer Hintergrund
Schlüsselkonstruktion		
Wahl zweier Primzahlen p und q	$p = 11, q = 7$	Miller-Rabin-Test
$n = p \cdot q$	$n = 77$	Faktorisierungsproblem
Konstruktion von e, d mit $e \cdot d = k(p-1)(q-1)+1$ für ein $k \in \mathbb{N}$	$e = 7 \quad d = 43$	Erweiterter euklidischer Algorithmus
Verschlüsseln einer Nachricht m		
$c = m^e \bmod n$ mit dem öffentlichen Schlüssel (e,n)	$c = 8^7 \bmod 77 = 57$	Schnelles Potenzieren
Entschlüsseln eines Geheimtextes c		
$m = c^d \bmod n \,(= m^{ed} \bmod n)$ mit dem geheimen Schlüssel d	$m = 57^{103} \bmod 77 = 8$	Schnelles Potenzieren & Satz von Euler (Korrektheit)

Der Einsatz von RSA zum Verschlüsseln oder Signieren ist möglich, da $(m^e)^d \equiv m^{ed} \equiv (m^d)^e \bmod n$ ist, d.h. die Reihenfolge in der mit den Exponenten e (öffentlich) und d (geheim) modulo n potenziert wird,

kann vertauscht werden.

One-Time-Pad

Gegeben sei eine Nachricht der Länge n, bestehend aus Elementen einer Menge M. Zum Verschlüsseln wird zu jedem Zeichen der Nachricht ein zufällig gewähltes Element der Menge M addiert. Liegt die Nachricht binär codiert vor ($M = \{0,1\}$, wird also zu jeder Stelle zufällig 0 oder 1 addiert (modulo 2). Diese Zufallsfolge ist der geheime Schlüssel. Zum Entschlüsseln benötigt der Empfänger diese Folge, um die Verschlüsselung rückgängig zu machen. Nachrichtentext und verschlüsselter Text sind statistisch unabhäng und bieten einem Angreifer keinerlei Angriffspunkte.

Ein Beispiel im üblichen Alphabet ist das folgende. Die Verschlüsselung erfolgt dadurch, dass jeder Buchstabe der zu übermittelnenden Nachricht (Klartext) durch den Buchstaben ersetzt wird, der soviele Stellen im Alphabet nachfolgt, wie der Position des Schlüsselbuchstaben entspricht. Die Buchstaben werden sozusagen addiert. Der entstandene Geheimtext kann übermittelt werden und wird durch „Subtraktion“ entschlüsselt.

Klartext		P	R	I	M
Schlüssel	+	A	B	M	V
Geheimtext		P	S	U	H

Verschlüsseln

Geheimtext		P	S	U	H
Schlüssel	-	Q	S	N	W
Klartext		Z	A	H	L

Entschlüsseln mit einem falschen Schlüssel

Anstatt *Zahl* kann der potentieller Angreifer jedes andere Wort (oder Buchstabenkombination) mit vier Zeichen „entschlüsseln“. Er kann nicht entscheiden, ob und welches Ergebniss das richtige ist, falls (i) der Schlüssel tatsächlich nur einmal verwendet wird, (ii) der Schlüssel aus einer zufälligen Zeichenfolge besteht und die Zeichen gleichverteilt sind und (iii) der Schlüssel geheim bleibt. Andernfalls ist es möglich mit Hilfe statistischer Analysen Rückschlüsse auf die Nachricht zu erhalten.

Der daraus resultierende Anspruch an die Schlüsselverwaltung macht das Verfahren für Alltagsanwendungen unbrauchbar.