Dr. Anita Dorfmayr, Universität Wien

Von Cäsar bis RSA

Verschlüsselung von der 1. bis zur 8. Klasse

Anwendungsorientierter Mathematikunterricht kann nicht nur Motivation und Interesse der Schüler/innen fördern, sondern auch das Verständnis für mathematische Zusammenhänge vertiefen. Und ganz nebenbei erhalten die Schüler/innen endlich eine Antwort auf die Frage „Wozu braucht man das?“.

Dieser Beitrag ist dem Thema *Verschlüsseln von Nachrichten* gewidmet. An Hand konkreter Aufgabenstellungen und Erfahrungen aus dem Unterricht wird gezeigt, dass dieses Thema im Mathematikunterricht jeder Schulstufe sinnvoll eingesetzt werden kann. Die Möglichkeiten reichen von einzelnen Aufgaben, an Hand derer z.B. das Thema Teilbarkeit geübt wird, bis hin zu umfangreichen Projekten, die als Einstieg oder Vertiefung des Rechnens mit Restklassen verwendet werden können. So können die Schüler/innen Zahlentheorie als etwas Spannendes und „Brauchbares“ erleben.

1. Einführung

1.1. Von den Anfängen der Verschlüsselung bis zur modernen Kryptografie

Die Anfänge der Verschlüsselung gehen auf die Ägypter zurück. Sie verwendeten schon um 2000 v. Chr. unübliche Hieroglyphen zum Verschlüsseln geheimer Botschaften.

Hebräische Gelehrte verwendeten ca. 500 v. Chr. unter anderem die Geheimschrift **Atbash**, bei der sie einfach ein „umgedrehtes“ Alphabet verwendeten: Das erste Zeichen des hebräischen Alphabets (**A**leph) wurde mit dem letzten Zeichen (**T**aw) verschlüsselt, das zweite (**B**eth) mit dem vorletzten (**S**in), usw. Von den ersten und letzten beiden Zeichen des hebräischen Alphabets hat diese Geheimschrift auch ihren Namen: **A**leph-**T**aw-**B**eth-**S**in.

Eines der ersten bekannten Chiffrier-Instrumente ist die **Skytale**. Sie wurde ungefähr 500 – 400 v. Chr. von den Spartanern verwendet. Zum Verschlüsseln wurde zuerst ein Pergamentstreifen spiralförmig auf einen Holzstab mit einem bestimmten Durchmesser d aufgerollt. Dann schrieb der Absender die Nachricht längs des Holzstabs auf den Pergamentstreifen (Abb. 1).

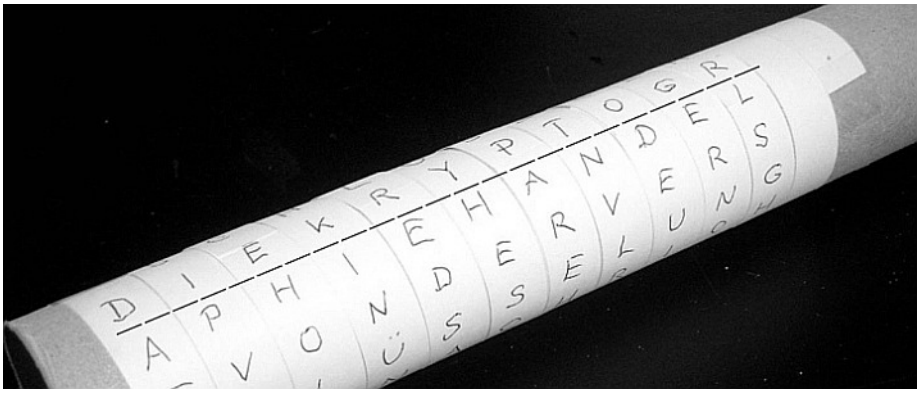


Abbildung 1: Verschlüsseln mit einer Skytale

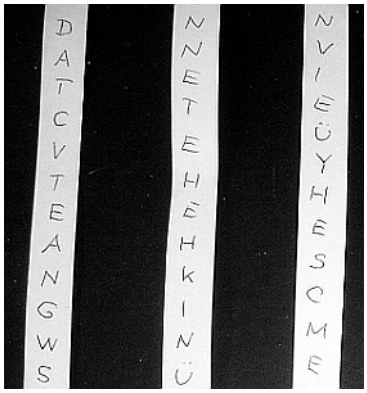


Abbildung 2: Geheimtext

Der Empfänger erhielt nur das abgewickelte Band, auf dem die Zeichen willkürlich angeordnet zu sein schienen (Abb. 2). Er konnte den Geheimtext mit Hilfe eines Stabes mit demselben Durchmesser d entschlüsseln. Dazu musste er die Pergamentstreifen auf diesen Stab aufwickeln und konnte die ursprüngliche Nachricht anschließend ablesen.

Abbildung 3: Enigma

Eine der bekanntesten Chiffriermaschinen ist die **ENIGMA**, die im 2. Weltkrieg vom deutschen Militär verwendet wurde [6]. Es handelt sich dabei um eine Chiffriermaschine (Abb. 3). Die zu verschlüsselnde Nachricht wird – ähnlich wie bei einer Schreibmaschine – über eine Tastatur eingegeben. Mehrere Rotor-Blätter im Inneren der ENIGMA (Abb. 4) sorgen dafür, dass die Nachricht Zeichen für Zeichen verschlüsselt wird.

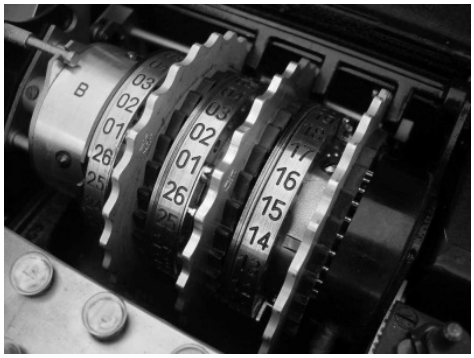


Abbildung 4: Enigma – Walzensystem

Die kryptografische Stärke der ENIGMA liegt darin, dass ein Buchstabe abhängig von seiner Position in verschiedene Zeichen chiffriert wird. Aus einem A kann einmal ein B werden, an einer anderen Stelle ein K, usw. Solche Chiffrierverfahren heißen polyalphabetisch (siehe auch Abschnitt 2.2).

Die Anfänge der **mathematischen Kryptografie** gehen auf den Mathematiker Claude Shannon zurück. Schon 1948 erkannte er, dass die Vernam Chiffre das einzige sichere Verfahren ist, das es jemals geben würde. Diese Chiffre erweist sich jedoch in der Praxis nur als wenig brauchbar (siehe dazu Abschnitt 2.2).

Die Güte eines klassischen Chiffrierverfahrens wird heute daran gemessen, wie hoch der Rechenaufwand zum „Knacken des Codes“ ist. Die Qualität eines Codes steht also in direktem Zusammenhang mit der Leistungsfähigkeit von Computern. Dies gilt nicht mehr für die neuen Verfahren der **Quantenkryptografie**, die seit den 1980er Jahren immer mehr Bedeutung gewinnen. Vielmehr wird bei diesen Verfahren ein Angreifer, der die geheime Schlüsselübertragung abzuhören versucht, fast immer sofort bemerkt. In diesem Fall wird einfach ein neuer Schlüssel generiert und übertragen.

1.2. Ziele der Kryptografie

Die Kryptografie beschäftigt sich mit dem Verschlüsseln von Nachrichten und verfolgt folgende Ziele:

- **Vertraulichkeit / Zugriffsschutz:**
  Nur dazu berechtigte Personen können die verschlüsselte Nachricht lesen.
- **Authentizität / Fälschungsschutz:**
  Der Empfänger/die Empfängerin einer Nachricht kann die Identität des Absenders zweifelsfrei feststellen.
- **Integrität / Änderungsschutz:**
  Der Empfänger/die Empfängerin einer Nachricht kann nachprüfen, ob die Nachricht nach ihrer Erzeugung verändert wurde.
- **Verbindlichkeit / Nichtabstreitbarkeit:**
  Der Absender/die Absenderin einer Nachricht kann dies nicht bestreiten und ist daher gegenüber Dritten nachweisbar.

Im Schulunterricht sollte der Schwerpunkt auf dem Ziel der Vertraulichkeit liegen. In einem Wahlpflichtfach kann auch das Thema Authentizität behandelt werden.

2. Kryptografie in der Sekundarstufe I

2.1. Kästchencode und Zahlencode

Mit Geheimschriften experimentieren Kinder schon in der Grundschule. Ein Beispiel dafür ist der Kästchencode. Die Buchstaben des Alphabetes werden dafür in ein vorher vereinbartes Raster eingetragen, für dessen Gestaltung es mehrere Möglichkeiten gibt (Abb. 5).

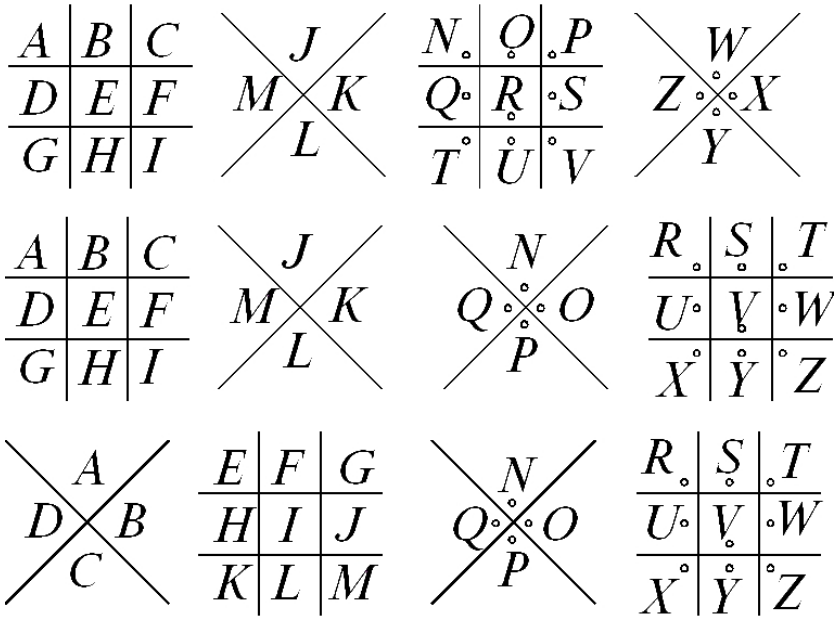


Abbildung 5: Drei mögliche Kästchencodes

Ein Text wird zeichenweise verschlüsselt. Dazu wird jeder Buchstabe in ein geheimes Zeichen verwandelt, das sich aus seiner Position in diesem Raster ergibt (Abb. 6).

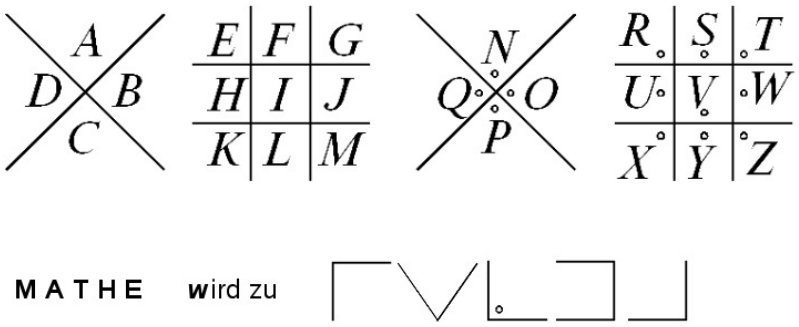


Abbildung 6: Verschlüsselung mit einem Kästchencode

Die Entschlüsselung eines Geheimtextes ist nur dann möglich, wenn der richtige Code – das richtige Raster also – verwendet wurde. Bei der Verwendung des falschen Kästchencodes entstehen sinnlose Wörter (Abb. 7).

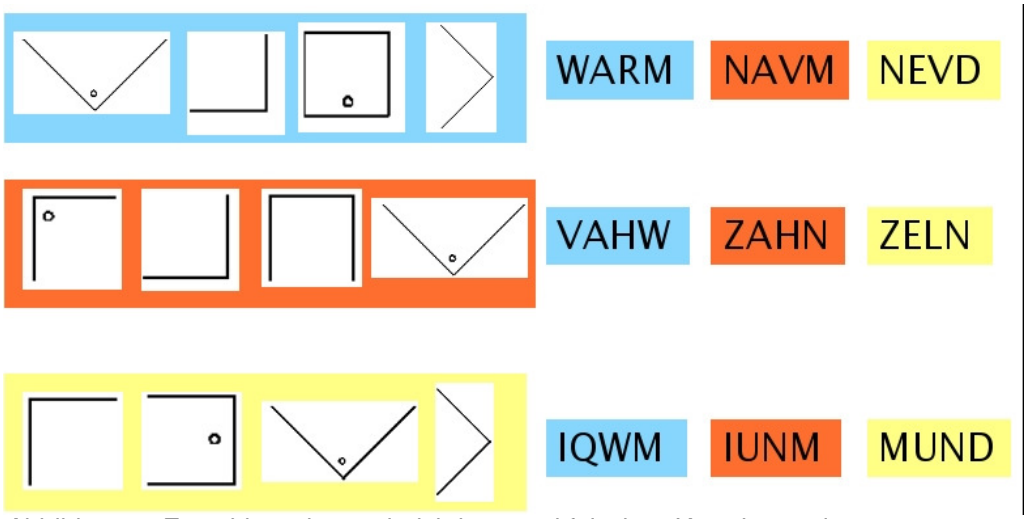


Abbildung 7: Entschlüsselung mit richtigen und falschen Kästchencodes - Nur ein Wort ist richtig!

Beim Arbeiten mit diesen sehr einfachen Kästchencodes lernen die Schülerinnen und Schüler schon die Grundmechanismen von Verfahren zur Verschlüsselung:

- Wie wird verschlüsselt und entschlüsselt?
  Als Mathematiklehrerinnen / Mathematiklehrer wissen wir, dass eine bijektive Zuordnung zwischen der Menge der Buchstaben und der Menge der Geheimzeichen bestehen muss.
- Alle Kommunikationspartner müssen mit derselben Codetafel arbeiten, da nur ein Code die richtigen Ergebnisse liefert.

Das Darstellen von Texten mit Hilfe von Zahlen übt auf Kinder ebenso eine große Faszination aus. Sie experimentieren schon früh mit dem „mathematischeren“ **Zahlencode**. Jedem Buchstaben entspricht in eindeutiger Weise eine Position im Alphabet. Entsprechend wird jeder Buchstabe durch die Nummer seiner Position im Alphabet verschlüsselt.

Das Wort „HUT“ könnte beispielsweise verschlüsselt werden als „8 21 20“. Allerdings ist das Entschlüsseln nicht immer eindeutig möglich (Abb. 8). Das Verbessern der Methode ist bereits für Schülerinnen und Schüler der 1. Klasse AHS naheliegend: Jede Position im Alphabet muss mit Hilfe von zwei Ziffern beschrieben werden.

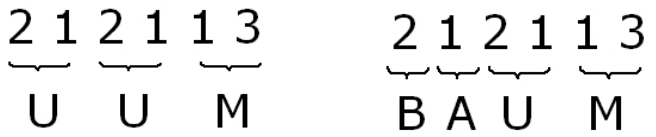


Abbildung 8: Zahlencode - Entschlüsselung nicht eindeutig

Sowohl beim Kästchencode als auch beim Zahlencode stellt sich die Frage der Sicherheit. Ein Spion kann diese Form von Zahlencode leicht knacken. Im Fall des Kästchencodes müsste der Spion irgendwie in den Besitz der Codetafel kommen oder aber den Geheimtext mit viel Geduld oder mit Hilfe des Computers durch Probieren entschlüsseln.

Die hier vorgestellten Verschlüsselungsverfahren haben also große Mängel im Bereich der Sicherheit. Wie Codes sicherer werden könnten, zeigen die folgenden Abschnitte.

2.2. Symmetrische Verfahren

Bei symmetrischen Verfahren vereinbaren Sender und Empfänger einer Nachricht einen gemeinsamen Schlüssel. Diesen verwenden sie zum Chiffrieren und Dechiffrieren.

Cäsar-Code: Verschieben „auf Mathematisch“

Wie könnten wir den Zahlencode aus dem letzten Abschnitt sicherer gegenüber Angriffen nicht befugter Personen machen? Schülerinnen und Schüler kennen den Trick: Wir verschieben das Codealphabet um ein paar Stellen, etwa um drei. Mathematisch bedeutet dies nichts anderes als eine Addition von 3. Dass für die letzten Buchstaben im Alphabet modulo 26 reduziert werden muss, stellt für Schülerinnen und Schüler der Sekundarstufe 1 keine Schwierigkeit dar, zumal dieses Verfahren auch mit Hilfe einer **Chiffrierscheibe** (Abb. 9) ausgeführt werden kann: Die innere Scheibe ist gegenüber der äußeren, größeren Scheibe drehbar. Mit Hilfe dieser Verschlüsselungsmaschine kann die Cäsar-Chiffre in Buchstaben- oder Zahlenform angewendet werden.

Abbildung 9: Chiffrierscheibe Cäsar

Der Schlüssel zu einer sinnvollen Kommunikation ist dabei die Anzahl n der Stellen, um die das Alphabet verschoben wurde.

Bei einem Cäsar-Code mit Schlüssel n = 3 (Abb. 10) wird beispielsweise das Wort „MATHEMATIK“ verschlüsselt zu „16042311081304230809 11“. Entschlüsselt wird, indem die entsprechende Codetafel von unten nach oben gelesen wird.

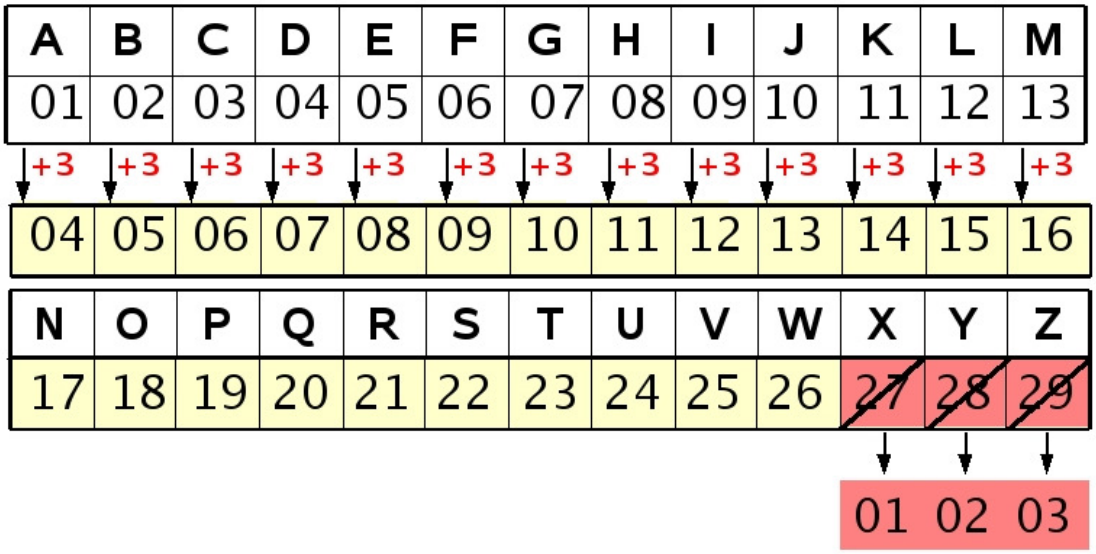


Abbildung 10: Cäsar-Chiffre mit Schlüssel n = 3

Auch beim Cäsar-Code stellt sich die Frage der Sicherheit. Auch dieser Code kann recht einfach geknackt werden, denn er ist **monoalphabetisch**. Das bedeutet, dass jeder Buchstabe des Klartextes beim Chiffrieren immer in dasselbe Geheimtextzeichen verschlüsselt wird. Bei Schlüssel n = 3 etwa (Abb. 10) wird jedes A des Klartextes zu „04“. Zum Knacken des Codes verwendet man die für jede Sprache typischen Buchstabenhäufigkeiten.

Es sei bekannt, dass der Geheimtext mit Cäsar chiffriert wurde und dass es sich um einen deutschen Text handelt. Im Deutschen ist „E“ der häufigste Buchstabe. Wenn nun im Geheimtext beispielsweise „08“ das häufigste Geheimtextzeichen ist, so kann man relativ sicher davon ausgehen, dass „08“ für „E“ steht. „E“ ist der fünfte Buchstabe im Alphabet, sodass der Schlüssel wahrscheinlich n = 3 ist. Wird also nur ein einziges Geheimtextzeichen richtig dechiffriert, so kann daraus schon der Schlüssel ermittelt und der gesamte Text dechiffriert werden. Diese Methode bewährt sich vor allem bei langen Geheimtexten, bei denen die Häufigkeiten der Geheimtextzeichen gut mit den tatsächlichen Buchstabenhäufigkeiten der zugrunde liegenden Sprache übereinstimmen.

Vigenère – der bessere Cäsar

Die Vigènere-Verschlüsselung basiert auf derselben Idee wie der Cäsar-Code. Allerdings wird hier nicht jedes Zeichen des Klartextes um dieselbe Anzahl von Stellen verschoben. Es werden mehrere Schlüssel verwendet. Je nach Position des Klartextzeichens kommt ein anderer Schlüssel zum Einsatz.

Realisiert wird diese Idee so, dass die Kommunikationspartner ein Schlüsselwort vereinbaren. Das Schlüsselwort wird wiederholt unter den Klartext geschrieben und stellenweise „addiert“. Addition von „A“ bedeutet Addition von 1, also Verschiebung um eine Stelle, Addition von „B“ Verschiebung um zwei Stellen, usw. Im Beispiel aus Abb. 12 wird das Wort „GEHEIMNIS“ mit dem Schlüsselwort „A KEY“ verschlüsselt. Das erste Zeichen des Klartextes wird um eine Stelle verschoben, das zweite Zeichen um 11 Stellen, usw.

Klartext:	G E H E I M N I S
Schlüssel:	A K E Y A K E Y A
Geheimtext:	H P M D J X S H T

Abbildung 11: Vigenère-Verschlüsselung mit einem Schlüsselwort

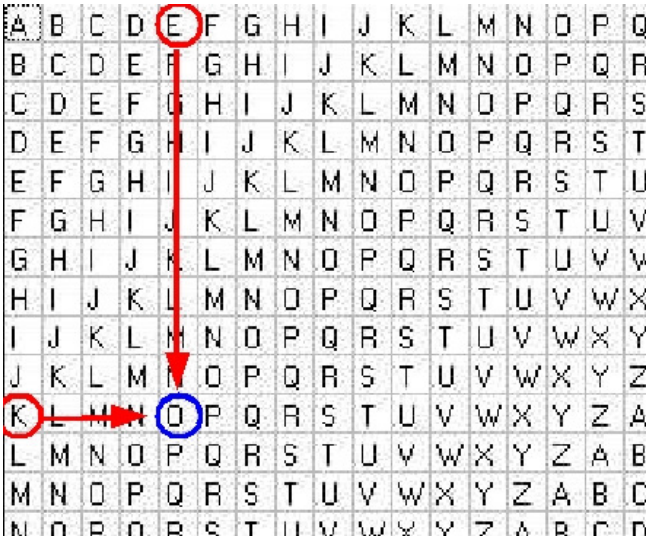


Abbildung 12: Vigenère-Quadrat

Wird beim Verschlüsseln dem „A“ die Position „00“ statt „01“ zugewiesen, kann zum Verschlüsseln mit Vigenère alternativ auch das Vigènere-Quadrat verwendet werden. Dabei wird das Alphabet wiederholt zyklisch vertauscht in Zeilen untereinander geschrieben. Der Klartextbuchstabe „E“ aus der 5. Spalte und der Schlüsselwortbuchstabe „K“ aus der entsprechenden Zeile ergeben das Geheimtextzeichen „O“, usw. (Abb. 11)

Durch diese Vorgangsweise entsteht ein **polyalphabetischer** Code. Ein Buchstabe aus dem Klartext kann – abhängig von seiner Position – in verschiedene Geheimtextzeichen chiffriert werden. So wird etwa das „E“ aus dem Beispiel in Abb. 12 einmal zu einem „P“, und einmal zu einem „D“. Das Knacken des Codes ist allein durch Vergleichen der Häufigkeiten der Geheimtextzeichen mit den Buchstabenhäufigkeiten der zugrunde liegenden Sprache nicht mehr möglich.

Doch auch dieser Code kann geknackt werden. Es gibt Verfahren, wie etwa den Kasiski-Test oder den Friedman-Test [11], mit deren Hilfe die Länge des Schlüsselwortes bestimmt werden kann. Im Beispiel aus Abb. 12 ist dieses n = 4 Stellen lang. Den Geheimtext schreibt man dann in n = 4 Spalten an. In der ersten Spalte stehen dann alle Zeichen, die mit dem ersten Schlüsselwortbuchstaben verschlüsselt wurden, in der zweiten Spalte wurden alle Zeichen mit dem zweiten Schlüsselwortbuchstaben verschlüsselt, usw. Pro Spalte liegt daher eine Cäsar-Verschlüsselung vor. Diese n Cäsar-Codes können wie oben beschrieben geknackt werden. Fügt man die Spalten anschließend wieder zusammen, so erhält man den Klartext.

Vernam-System oder One-Time-Pad

Kann wirklich jeder Code geknackt werden? Nein, denn durch einen einfachen Trick wird aus dem Vigènere Verfahren ein absolut sicherer Code. Dazu muss „nur“ ein theoretisch unendlich langes Schlüsselwort verwendet werden. Jedes Zeichen des Schlüsselwortes darf dann nur ein einziges Mal zum Verschlüsseln verwendet werden. In der Praxis werden (theoretisch) unendlich lange Folgen von Zufallszahlen als Schlüsselwort verwendet. Jene Stellen, die einmal zum Verschlüsseln verwendet wurden, werden vernichtet. Der Empfänger verwendet dieselben Stellen zum Entschlüsseln der Nachricht und vernichtet diesen Teil der Folge dann ebenso.

Dieses Verfahren ist – abgesehen von dem Fall, dass jemand in den Besitz der Zufallsfolge kommt – zu 100% sicher. Allerdings stellt sich das Problem des Schlüsseltausches. Die Kommunikationspartner müssten sich regelmäßig in absolut

vertrauter Umgebung treffen, um ihre Schlüssel auszutauschen. Weiters müssten regelmäßig neue Stellen des Schlüsselwortes generiert werden.

Dieses Verfahren wurde etwa im Kalten Krieg für das Rote Telefon [7] verwendet. Die Schlüssel wurden per Kampfjet zwischen den USA und er damaligen UdSSR hin- und hergeschickt.

3. Kryptografie in der Sekundarstufe II

3.1. Asymmetrische Verfahren

Die bisher betrachteten symmetrischen Verfahren sind für viele Bereiche unseres täglichen Lebens (z.B. Bankgeschäfte) nicht sicher genug. Sie bergen aber noch einen wesentlichen anderen Nachteil: Jede Person muss mit jedem potentiellen Kommunikationspartner einen Schlüssel vereinbaren. Dazu ist eine große Anzahl an Schlüsseln erforderlich. Jeder Kommunikation muss ein Treffen vorangehen, in dem die Schlüssel sicher ausgetauscht werden.

Bei einem asymmetrischen Verfahren verfügen Sender und Empfänger einer Nachricht nicht mehr über identische Schlüssel. Zum Verschlüsseln und Entschlüsseln werden unterschiedliche Informationen benötigt. Bei Public-Key-Verfahren, wie wir sie im Folgenden betrachten wollen, kann jener Teil des Schlüssels, der zum Verschlüsseln benötigt wird, sogar öffentlich gemacht werden – und das, ohne die Sicherheit der Kommunikation zu gefährden.

Nehmen wir an, Bob möchte Alice eine Nachricht schicken. Beide haben je einen öffentlichen und einen privaten (geheimen) Schlüssel (Abb. 13). Die öffentlichen Schlüssel werden – wie heute Telefonnummern – etwa in einer Datenbank im Internet veröffentlicht.

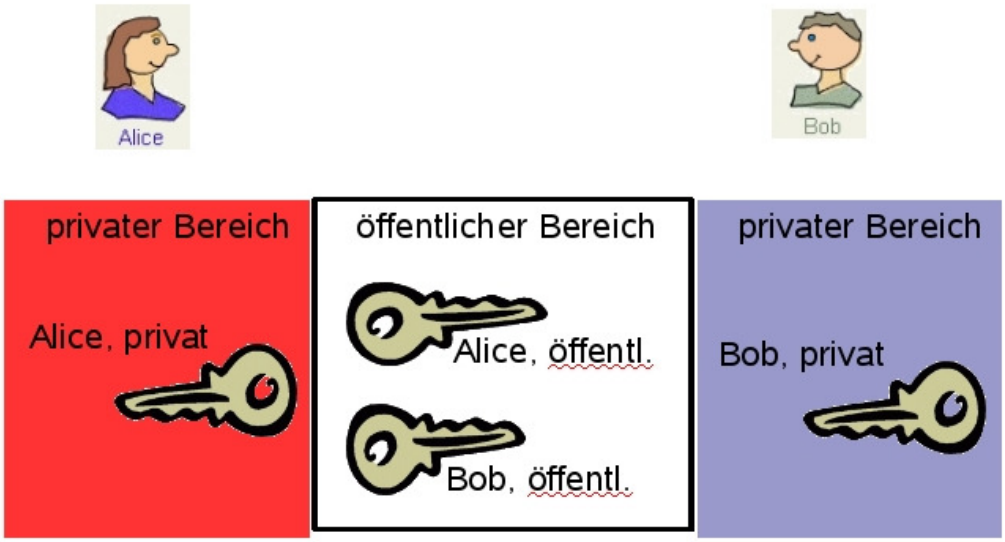


Abbildung 13: Alice und Bob haben je einen öffentlichen und einen privaten Schlüssel

- **Verschlüsselung:** Bob findet Alices öffentlichen Schlüssel in einer öffentlichen Datenbank. Er verschlüsselt seine Nachricht mit Hilfe von Alices öffentlichem Schlüssel und sendet die verschlüsselte Nachricht an Alice. (Abb. 14)
  Verschlüsselt wird mit einem öffentlichen Schlüssel.
- **Entschlüsselung:** Alice erhält die Nachricht von Bob. Sie entschlüsselt sie unter Verwendung ihres eigenen privaten Schlüssels.
  Entschlüsselt wird mit dem privaten Schlüssel. (Abb. 14)

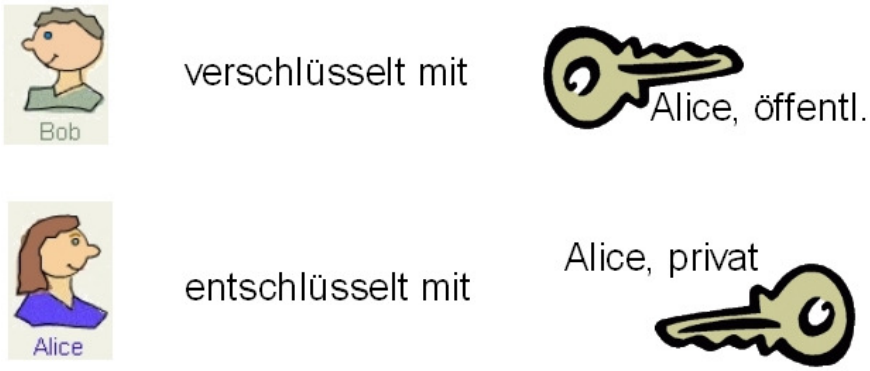


Abbildung 14: Bob sendet Alice eine Nachricht, Alice entschlüsselt sie

Jeder Kommunikationspartner besitzt also ein Schlüsselpaar – bestehend aus einem öffentlichen und einem privaten Teil. Die beiden Schlüsselteile sind so konzipiert, dass der Empfänger einer Nachricht mit seinem privaten Schlüssel nur jene Texte entschlüsseln kann, die mit seinem öffentlichen Schlüssel chiffriert wurden.

Problem der Authentikation[1]

Alice kann sich nicht sicher sein, dass die Nachricht von Bob stammt. Da für die Verschlüsselung der Nachricht nur sein öffentlicher Code nötig war.

Dieses Problem löst Bob, indem er seine Nachricht zweimal verschlüsselt:

1. Er verschlüsselt ihre Nachricht zuerst mit seinem eigenen privaten Schlüssel.
2. Dann verschlüsselt er diesen neuen Text mit Alices öffentlichem Schlüssel.

Alice kann diese Nachricht in zwei Schritten entschlüsseln:

1. Zuerst verwendet sie ihren privaten Schlüssel. Sie erkennt, dass noch nicht der Klartext vorliegt.
2. In einem zweiten Schritt kontrolliert Alice, ob die Nachricht tatsächlich von Bob stammt. Dazu wendet sie Bobs öffentlichen Schlüssel auf den Text an. Nur, wenn die Nachricht tatsächlich von Bob stammt, erhält Alice auf diese Weise den Klartext.

1 Der Begriff *Authentikation* kommt vom Englischen *authentication* und wurde unverändert ins Deutsch übernommen.

3.2. RSA – ein Beispiel für ein asymmetrisches Verfahren

Whitfield Diffie und Martin Hellman gaben in ihrem Artikel „New Directions in Cryptography“ Anstoß für Public Key Systeme, indem sie die Idee des Schlüsseltausches beschrieben. Erst Ronald C. Rivest, Adi Shamir, Leonard Adleman gelang es, dazu auch eine Methode zu entwickeln – den nach ihnen benannten RSA – Algorithmus, der heute beispielsweise häufig zur Verschlüsselung bei verschiedenen Transaktionen im Internet verwendet wird.

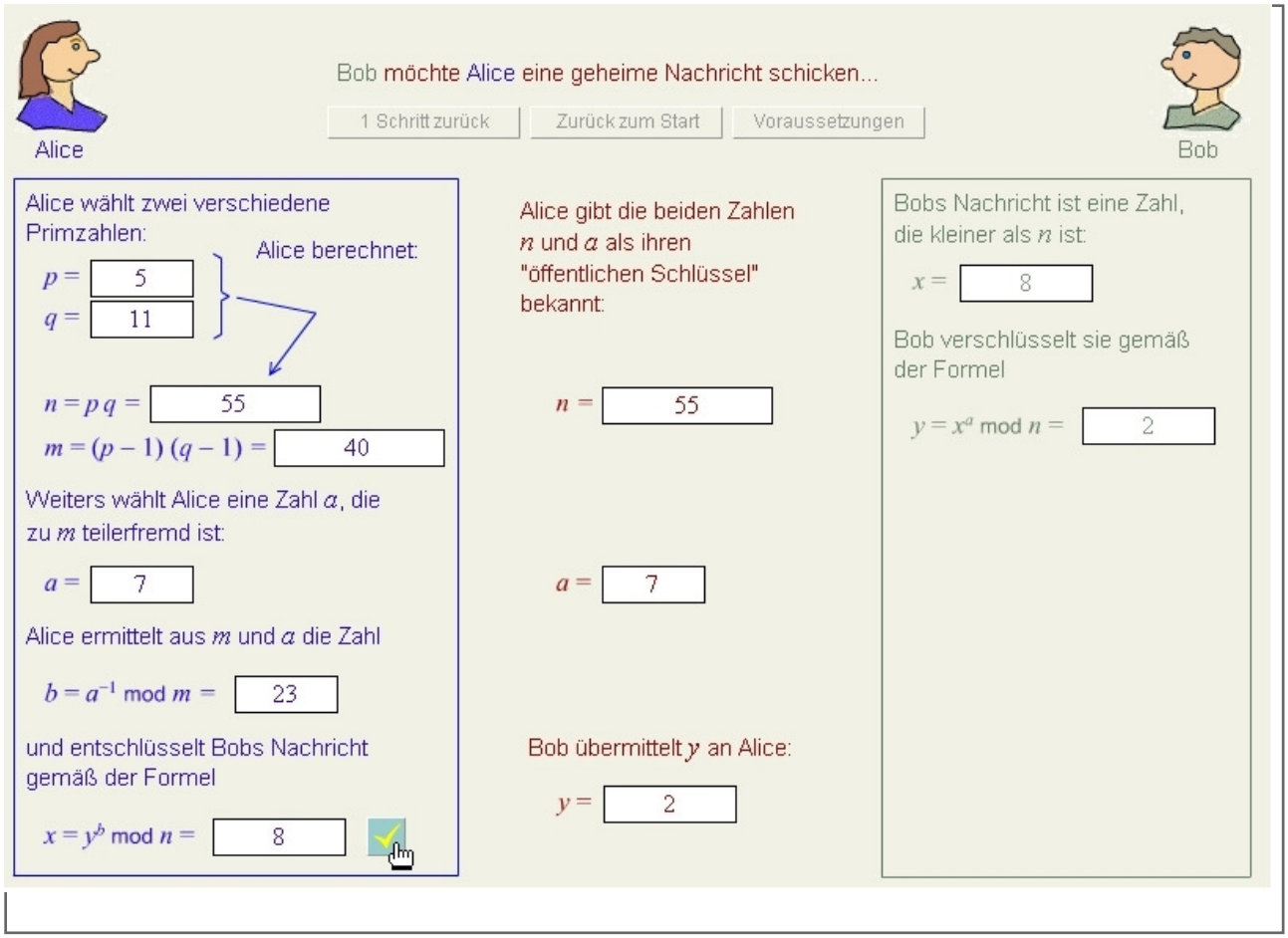
Die Funktionsweise und Sicherheit des RSA-Verfahrens beruht auf der Tatsache, dass

- es für die Faktorisierung großer natürlicher Zahlen nach wie vor keinen brauchbaren Algorithmus gibt.
- die Verfahren zur Chiffrierung und Dechiffrierung bei Kenntnis dieser Primfaktoren einen sehr geringen Rechenaufwand haben und daher schnell sind.

Die mathematische Basis für die Funktionsweise sind

- der Satz von Euler-Fermat und
- der erweiterte euklidische Algorithmus.

Wie das RSA-Verfahren funktioniert, zeigt Abb. 15.



4. Materialien für den Schulunterricht

Im Rahmen des Projektes Medienvielfalt im Mathematikunterricht entstand ein Lernpfad mit dem Titel „**RSA-Algorithmus: Asymmetrische Verschlüsselung**“ [3]. Es handelt sich dabei um einen online-Kurs, der von Schülerinnen und Schülern in selbstständiger projektorientierter Weise bearbeitet werden soll. Neben anschaulichen Applets, Informationen über die Funktionsweise symmetrischer und asymmetrischer Verschlüsselungsverfahren, einer ausführlichen Darstellung des theoretischen Hintergrundes werden auch Links zu kostenlosen Tools und weiteren online-Kursen zum Thema Kryptografie geboten.

Der Kurs eignet sich hervorragend für eine Wahlpflichtfachgruppe. Einzelne Teile daraus sind allerdings auch im Regelfach einsetzbar.

5. Literatur

[1.] C. Ableitinger, A. Dorfmayr, P. Hauer-Typpelt: Steckt da wirklich Mathe drin? Unterlagen zur Kinderuni Wien 2006.

[2.] D. Hachenberger: Mathematik für Informatiker, Pearson Studium, München 2005.

[3.] http://www.austromath.at/medienvielfalt/ [12.04.2007]

[4.] http://www.linuxfocus.org/Deutsch/May2002/article243.shtml#243lfindex0 [12.04.2007]

[5.] http://de.wikipedia.org/wiki/Atbash [12.04.2007]

[6.] http://de.wikipedia.org/wiki/Enigma_%28Maschine%29 [12.04.2007]

[7.] http://de.wikipedia.org/wiki/Heiß_Draht [12.04.2007]

[8.] http://de.wikipedia.org/wiki/Kryptografie [12.04.2007]

[9.] http://de.wikipedia.org/wiki/Quantenkryptografie [12.04.2007]

[10.] http://de.wikipedia.org/wiki/Skytale [12.04.2007]

[11.] D. Dorninger: Anwendungen der Mathematik (für LAK) – Modelle, Verfahren, Beispiele. TU Wien, 2004.

[12.] A. Beutelspacher, Christian und die Zahlenkünstler – Ein Mathe-Krimi. Dtv, 2007.