RSA – Primzahlen zur Verschlüsselung von Nachrichten

Anton Schüller[1]
Ulrich Trottenberg[1,2]
Roman Wienands[2]
Michael Koziol[2]
Rebekka Schneider[2]

[1]**Fraunhofer-Institut**
Algorithmen und Wissenschaftliches Rechnen SCAI

[2] **Mathematisches Institut**
der Universität zu Köln

Version 1.2
24.02.2017

Inhaltsverzeichnis

1 Vorbemerkung: Kryptographie und RSA-Verfahren im Schulunterricht

Methoden, um geheime Botschaften *sicher* zu übertragen, d.h. so, dass niemand außer dem Absender und dem Empfänger sie lesen kann, sind schon seit Tausenden von Jahren von hohem Interesse, z.B. in der Politik und bei militärischen Plänen. In der heutigen Zeit ist die Bedeutung der Verschlüsselung für die Allgemeinheit noch einmal erheblich gestiegen. Gelingt es Kriminellen beispielsweise, Kontodaten abzufangen, können sie versuchen, unberechtigt Abbuchungen von Konten vorzunehmen. Um dies zu verhindern, ist eine sichere Verschlüsselung von Daten von allgemeinem Interesse.

Im Jahre 1977 wurde mit dem RSA-Verfahren (benannt nach seinen Erfindern Ron Rivest, Adi Shamir und Leonard Adleman) eine Methode entdeckt, mit der man Daten sehr sicher verschlüsseln kann und die darüberhinaus auch für den allgemeinen Gebrauch geeignet ist. Die Idee und die Sicherheit des RSA-Verfahrens beruhen darauf, dass es zwar sehr leicht ist, zwei sehr große Primzahlen miteinander zu multiplizieren, andererseits jedoch ein riesiger Zeitaufwand erforderlich ist, um aus dem Produkt dieser beiden Primzahlen die Primzahlen selbst wieder zu berechnen. Man beachte dabei, dass in der Praxis eingesetzte Primzahlen aus mehreren Hundert Stellen bestehen.

Obwohl das RSA-Verfahren sehr sicher und noch relativ jung ist, sind seine Funktionsweise und die mathematischen Prinzipien, auf denen es basiert, bereits für Schüler/-innen der Mittelstufe verständlich. RSA ist zugleich ein ausgezeichnetes Beispiel für die Bedeutung der Mathematik für die moderne Gesellschaft.

Das vorliegende Unterrichtsmodul zu den Themen Kryptographie und RSA-Verfahren enthält auch eine Vielzahl von Arbeitsblättern samt Lösungen sowie eine kurzen Beschreibung einiger beigefügter Programme. In Abschnitt 2 gehen wir auf Verschlüsselung mit dem Caesar-Code ein. Diese Inhalte und die zugehörigen Arbeitsblätter können bereits ab der Jahrgangsstufe 5 im Unterricht eingesetzt werden. Kinder in diesem Alter sind in der Regel sehr motiviert, Geheimschriften und Verschlüsselungen kennenzulernen.

Auf die RSA-Verschlüsselung gehen wir in Abschnitt 3 ausführlich ein. Abschnitt 4 enthält einige Details und effiziente Algorithmen, mit deren Hilfe man das RSA-Verfahren auch per Hand nachvollziehen kann. In der Anwendungspraxis wenden jedoch Computerprogramme das RSA-Verfahren an. Entsprechende Demo-Programme, die ebenfalls zum Unterrichtsmodul gehören, werden in Abschnitt 5.1 beschrieben. Abschnitt 5.2 enthält eine ganze Reihe von Arbeitsblättern mit den Lösungen der zugehörigen Aufgaben.

Die das RSA-Verfahren betreffenden Teile des Unterrichtsmoduls eignen sich für eine Unterrichtsreihe im Fach Mathematik, im Differenzierungsbereich Mathematik/Naturwissenschaft der Mittelstufe (ab Klasse 9) oder im Rahmen einer Projektwoche ab Klasse 9.

Die Entwicklung dieses Unterrichtsmoduls wurde unterstützt durch eine Projektförderung durch die WestLB-Stiftung Zukunft NRW, für die wir uns ganz herzlich bedanken.

2 Verschlüsselung in der Antike – der Caesar-Code

Schon um 500 v. Chr. sollen hebräische Gelehrte als Verschlüsselung ein umgekehrtes Alphabet benutzt haben. Auf das deutsche Alphabet übertragen bedeutet dies: Will man einen "geheime" Botschaft verschicken, so ersetzt man in der Botschaft den Buchstaben A immer durch Z, den Buchstaben B immer durch Y usw. Der Empfänger der Nachricht geht genauso vor und erhält wieder die ursprüngliche Nachricht.

Auf Caesar geht ein anderes Verschlüsselungsverfahren zurück, bei dem man die Buchstaben des zu versendenden Textes ersetzt durch Buchstaben, die im Alphabet um eine gewisse Anzahl von Buchstaben verschoben sind: Bei einer Verschiebung um zwei Buchstaben wird A ersetzt durch C, B durch D, C durch E usw. bis zu X durch Z. Bei den letzten – in unserem Beispiel zwei – Buchstaben, fängt man wieder von vorne an, also: Y wird ersetzt durch A und Z durch B.

Mit dem Caesar-Rad ist es leicht möglich, Texte nach dieser Methode zu verschlüsseln und wieder zu entschlüsseln (vgl. Arbeitsblatt *Caesar-Code und Restklassen*, Aufgabe 1).

2.1 Was hat der Caesar-Code mit Mathematik zu tun? – Restklassen

Mit dem Caesar-Rad ersetzt man Buchstaben durch Buchstaben. Ebenso kann man auch Buchstaben durch Zahlen ersetzen, z.B. durch die Zahlen 1 bis 26. Ähnlich wie beim Caesar-Code ist man auch hier frei in der Wahl einer Verschiebung. Man kann also A durch 3 ersetzen, B durch 4 usw. bis zu X durch 26; Y entspräche dann eigentlich der 27, wird aber wieder durch die 1 ersetzt, und Z (entspräche 28) durch die 2 (vgl. Arbeitsblatt *Caesar-Code und Restklassen*, Aufgabe 2).

Bei diesem Vorgehen wird also als Zahl jeweils der Rest genommen, den man erhält, wenn man die eigentliche Zahl durch 26 dividiert (die Buchstaben 27 und 28 existieren ja nicht). Dies entspricht der Betrachtung der Restklasse modulo 26 (vgl. Arbeitsblatt *Modulo-Rechnen*, Aufgabe 1).

Bemerkung 2.1 *Beim Ersetzen der Buchstaben durch Zahlen muss man beachten, dass die Entschlüsselung nicht eindeutig ist, wenn man unterschiedliche Anzahlen von Ziffern für unterschiedliche Buchstaben verwendet: Ersetzt man beispielsweise A durch 1, B durch 2 usw., so kann 123415 sowohl ABCDAE als auch LCDO bedeuten (12 kann als AB oder als L interpretiert werden, 15 als AE oder als O). Man sollte also immer die gleiche Anzahl von Ziffern für einen Buchstaben verwenden, also etwa 01 für A, 02 für B usw., oder die Eindeutigkeit anderweitig garantieren.*

Für das Verständnis des RSA-Algorithmus benötigen wir insbesondere den Begriff der Modulo-Funktion und die Regeln für das Modulo-Rechnen.

Definition 2.1 *Will man eine natürlichen Zahl a durch eine natürliche Zahl m teilen, so erhält man einen Rest r. Für diesen Rest gilt $0 \leq r \leq m-1$. Die Modulo-Funktion liefert zu gegebenen Zahlen a und m gerade diesen Rest r. Man schreibt auch*

$$a \bmod m = r \ .$$

Man kann diese Definition auch direkt auf ganzen Zahlen a verallgemeinern. So ist beispielsweise $-7 \bmod 3 = 2$, denn es gilt $-7 : 3 = -3$ Rest 2 wegen $-7 = -3 \cdot 3 + 2$.

Beispiel 2.1

$$\textit{Es ist } 19 : 4 = 4 \textit{ Rest } 3 \ , \ \textit{also gilt } 19 \bmod 4 = 3 \ .$$

Analog gilt:

$$\begin{aligned} 5 \bmod 3 &= 2 \quad && \textit{denn } 5 : 3 = 1 \textit{ Rest 2,} \\ 7 \bmod 4 &= 3 \quad && \textit{denn } 7 : 4 = 1 \textit{ Rest 3,} \\ 17 \bmod 6 &= 5 \quad && \textit{denn } 17 : 6 = 2 \textit{ Rest 5.} \end{aligned}$$

Man kann leicht zeigen, dass folgende Rechenregeln gelten:

$$\begin{aligned} (a \pm b) \bmod m &= (a \bmod m \pm b \bmod m) \bmod m \\ (a \cdot b) \bmod m &= (a \bmod m) \cdot (b \bmod m) \bmod m \\ (a^b) \bmod m &= (a \bmod m)^b \bmod m \end{aligned}$$

Im täglichen Leben rechnet man recht häufig modulo 10, zum Beispiel bei der schriftlichen Addition. Eine normale Uhr mit Stundenzeiger funktioniert analog zu modulo 12; digitale Tageszeitangaben (24h) analog zu modulo 24.

Zum Einüben und Vertiefen des Verständnisses der Modulofunktion dient das Arbeitsblatt *Modulo-Rechnen.*

Definition 2.2 *Die Restklasse einer Zahl a modulo einer Zahl m ist die Menge aller ganzen Zahlen, die bei Division durch m denselben (positiven) Rest lassen wie a. Man schreibt:* $[a]_m = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b = k \cdot m + a\} = \{b \mid b \equiv a \bmod m\}$ *. Jedes Element einer Restklasse bezeichnet man auch als Repräsentant der Restklasse. Die Menge aller Restklassen modulo m schreibt man häufig auch als* $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$ *.*

Beispiel 2.2 (Restklassen modulo 2)
Die Restklasse von 0 modulo 2 ($[0]_2$*) ist die Menge der geraden Zahlen.*
Die Restklasse von 1 modulo 2 ($[1]_2$*) ist die Menge der ungeraden Zahlen.*

Beispiel 2.3 (Restklassen modulo 3) *Es gibt drei Restklassen modulo 3: Eine Zahl ist durch drei teilbar, oder sie hat Rest 1, oder sie hat Rest 2. Das heißt:*

$$\begin{aligned} [0]_3 &= \{\cdots, -6, -3, 0, 3, 6, \cdots\} \\ [1]_3 &= \{\cdots, -5, -2, 1, 4, 7, \cdots\} \\ [2]_3 &= \{\cdots, -4, -1, 2, 5, 8, \cdots\} \ . \end{aligned}$$

Man beachte dabei, dass ein Rest von -2 einem Rest von 1 entspricht:
$(-5) : 3 = -1$ *Rest* -2
$(-5) : 3 = (-6 + 1) : 3 = -2$ *Rest* 1 .
Also haben wir $[-5]_3 = [-2]_3 = [1]_3$

Man kann für Restklassen eine Addition einführen. So ist z.B.

$$[1]_3 + [2]_3 = [3]_3 = [0]_3 \ .$$

Denn: Dividiert man zwei Zahlen a und b durch 3 und $a \bmod 3 = 1$, $b \bmod 3 = 2$, so gibt es Zahlen $k_1, k_2 \in \mathbb{Z}$ mit $a = 3 \cdot k_1 + 1$ und $b = 3 \cdot k_2 + 2$. Damit ist

$$a + b = k_1 \cdot 3 + 1 + k_2 \cdot 3 + 2 = (k_1 + k_2) \cdot 3 + 3 = (k_1 + k_2 + 1) \cdot 3$$

und somit $(a + b) \bmod 3 = 0$.

Entsprechend gilt für die Multiplikation von Restklassen z.B.

$$[2]_3 \cdot [2]_3 = [4]_3 = [1]_3 \ .$$

Dies sieht man folgendermaßen: Seien a und b zwei ganze Zahlen mit $a \bmod 3 = 2$ und $b \bmod 3 = 2$. Dann gibt es Zahlen $k_1, k_2 \in \mathbb{Z}$ mit $a = 3 \cdot k_1 + 2$ und $b = 3 \cdot k_2 + 2$. Damit ist

$$\begin{aligned} a \cdot b &= (k_1 \cdot 3 + 2) \cdot (k_2 \cdot 3 + 2) \\ &= (k_1 \cdot k_2 \cdot 3 + 2 \cdot k_2 + 2 \cdot k_1) \cdot 3 + 2 \cdot 2 \\ &= (k_1 \cdot k_2 \cdot 3 + 2 \cdot k_2 + 2 \cdot k_1 + 1) \cdot 3 + 1 \end{aligned}$$

und $a \cdot b$ hat bei Division durch 3 den Rest 1, also $(a \cdot b) \bmod 3 = 1$.

Addition und Multiplikation von Restklassen lässt sich einfach mit Hilfe entsprechender Tabellen darstellen. Die Additions- und die Multiplikationstabelle für das Rechnen mit Restklassen modulo 3 sehen folgendermaßen aus:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Für die Restklassen modulo 4 erhalten wir folgende Tabellen:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Zum Einüben und Vertiefen des Verständnisses von Restklassen dient das Arbeitsblatt *Restklassen.*

2.2 Nachteile des Caesar-Codes und Verallgemeinerungen

Insgesamt gibt es beim Caesar-Code nur 25 verschiedene Möglichkeiten, eine Nachricht zu verschlüsseln. (Die Einstellung des Caesar-Rads, bei jedem Buchstaben derselbe Buchstabe wieder zugeordnet wird, kann nicht als Verschlüsselung bezeichnet werden.) Wenn also jemand eine Nachricht abfängt und den Verdacht hat, sie könnte mit dem Caesar-Code verschlüsselt sein, so ist es sogar per Hand relativ leicht möglich, alle Möglichkeiten auszuprobieren und so die Nachricht zu entschlüsseln.

Man kann den Caesar-Code leicht verallgemeinern, wenn man beliebige eindeutige Zuordnungen von Buchstaben zulässt, also gegenüber dem Caesar-Code darauf verzichtet, die Reihenfolge der Buchstaben beizubehalten (monoalphabetische Verschlüsselung).

Man ordnet also dem Buchstaben A irgendeinen der vorhandenen 26 Buchstaben zu, dem Buchstaben B einen der verbleibenden 25 Buchstaben, dem Buchstaben C einen der restlichen 24 Buchstaben usw. Offensichtlich gibt es hierfür $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 2 \cdot 1 = 26!$ verschiedene Möglichkeiten. Die Zahl 26! ist so groß ($\approx 4 \cdot 10^{26}$), dass man selbst mit Hilfe moderner Computer Jahrzehnte bräuchte, um alle Möglichkeiten auszuprobieren.

Trotzdem gilt diese Art der Verschlüsselung aus gleich zwei Gründen nicht als sicher:

1. Um auf diese Art verschlüsselte Nachrichten auszutauschen, müssen Sender und Empfänger im Besitz ein- und desselben Schlüssels sein (symmetrische Verschlüsselung), d.h. die Information über die Art und Weise, wie die Nachrichten verschlüsselt sind, muss schon vorher zwischen Sender und Empfänger der Nachricht ausgetauscht worden sein. Jemand, der diesen Austausch des Schlüssels belauscht hat, ist danach jedoch in der Lage, jede verschlüsselte Nachricht zwischen dem Sender und dem Empfänger zu entschlüsseln und ihren Inhalt zu erfahren. Dies ist ein genereller Nachteil der symmetrischen Verschlüsselung.

2. Buchstaben kommen nicht gleich häufig vor. In typischen deutschen Texten kommt beispielsweise der Buchstabe E mit etwa 17 % am häufigsten vor. Es folgen N mit etwa 10 %, sowie I, R, S und A mit Werten zwischen 7,5 und 6,5 %. Auch für die anderen Buchstaben gibt es entsprechende Werte.

   Wird also ein längerer verschlüsselter Text abgefangen, so kann man aufgrund der Häufigkeitsverteilung sehr leicht auf die Buchstaben E und N schließen. Auch die Buchstaben I, R, S und A sind relativ leicht zu ermitteln. Mit diesen Informationen kann man in aller Regel leicht den gesamten Text entschlüsseln. Dies ist ein genereller Nachteil einer monoalphabetischen Verschlüsselung.

Gute Verschlüsselungsverfahren dürfen also weder monoalphabetisch noch symmetrisch sein.

Die Prinzipien der symmetrischen Verschlüsselung und der Verschlüsselung ohne Schlüsselaustausch können anhand des Arbeitsblatts *Symmetrische und asymmetrische Verschlüsselung* veranschaulicht werden:

- Bei der klassischen symmetrischen Verschlüsselung verschlüsselt der Sender die geheime Nachricht mit seinem Schlüssel. Er muss aber den Schlüssel und die versendete verschlüsselte Nachricht an den Empfänger senden. Will er den Schlüssel selbst sicher übermitteln, müsste er diesen selbst wieder sicher verschlüsseln usw. Also: Um eine geheime Nachricht sicher auszutauschen, muss man vorher schon eine geheime Nachricht (den Schlüssel) sicher ausgetauscht haben.

- Die Verschlüsselung ohne Schlüsselaustausch geht davon aus, dass Sender und Empfänger jeweils über einen geheimen Schlüssel verfügen, der keinem anderen bekannt ist. Eine sichere Übersendung einer geheimen Botschaft kann dann folgendermaßen ablaufen:

  1. Der Sender verschlüsselt seine Nachricht mit seinem Schlüssel und sendet sie an den Empfänger.

2. Der Empfänger verschlüsselt die Nachricht zusätzlich mit seinem Schlüssel und sendet sie zurück an den Sender.
3. Der Sender entschlüsselt mit seinem Schlüssel und sendet die jetzt nur noch mit dem Schlüssel des Empfängers verschlüsselte Nachricht wieder zurück an den Empfänger.
4. Jetzt kann der Empfänger mit seinem Schlüssel die Nachricht entschlüsseln.

Wichtig hierbei ist, dass sich die beiden Ver- und Entschlüsselungsvorschriften kommutativ verhalten.

3 Die RSA-Verschlüsselung

3.1 Prinzipien von RSA

RSA ist ein nahezu ideales Verfahren zur Verschlüsselung. Es verfügt über folgende Eigenschaften:

- RSA ist nicht monoalphabetisch, d.h. es gibt keine feste Zuordnung von Buchstaben im Originaltext und Zeichen im verschlüsselten Text.
- RSA ist nicht symmetrisch.
- Der Schlüssel besteht aus zwei Teilen, einem öffentlichen Teil, der jedem bekannt sein kann, der einer bestimmten Person eine Nachricht sendet, sowie einem privaten Teil, der nur dieser Person bekannt ist.

  RSA eignet sich demnach auch für Kommunikation zwischen sehr vielen Sendern und einem Empfänger, da der für alle Sender erforderliche Teil des Schlüssels öffentlich ist.
- Der öffentliche Teil des Schlüssels reicht nicht aus, um eine verschlüsselte Nachricht wieder zu entschlüsseln.
- Eine Entschlüsselung ist mit Hilfe des privaten Teils des Schlüssels trotzdem *einfach* möglich.
- Das RSA-Verfahren ist sehr sicher, denn man kann die Vorschrift, wie man die Nachricht wieder entschlüsseln kann, nicht oder nur mit einem riesigem Zeitaufwand (in der Größenordnung von Jahren, selbst wenn man moderne Hochleistungsrechner zu Hilfe nimmt) herausbekommen.

Diese letzte Bedingung lässt sich mit dem Begriff der *Einwegfunktion* beschreiben:

Definition 3.1 *Eine Einwegfunktion ist eine Abbildung f einer Menge X in eine Menge Y, so dass $f(x)$ für jedes Element von X leicht zu berechnen ist, während es für (fast) jedes y aus Y extrem schwer ist, ein Urbild x (d.h. ein x mit $f(x) = y$) zu finden.*

Beispiele für Einwegfunktionen sind das Telefonbuch und der Briefkasten:

- Das Telefonbuch ordnet jedem Namen eine Telefonnummer zu. Um aus der Telefonnummer aber auf den Namen zurückschließen zu können, müsste man die Einträge einzeln durchlesen (solange man sich nicht eines elektronischen Telefonbuchs mit Suchfunktion bedient).
- Man kann leicht eine Nachricht in einen Briefkasten einwerfen. Den Briefkasten öffnen und damit die Nachricht lesen kann jedoch nur, wer den privaten Schlüssel für seinen Briefkasten besitzt.

Zum Verständnis des Begriffs dient das Arbeitsblatt *Einwegfunktionen*.

3.2 Das multiplikative Inverse modulo einer Zahl m

Um Ver- und Entschlüsselung des RSA-Verfahrens verstehen zu können, benötigen wir neben dem Begriff der Primzahl und elementarem Rechnen mit Restklassen lediglich noch den Begriff des multiplikativen Inversen modulo einer Zahl m.

Definition 3.2 *Sind a und m zwei teilerfremde positive ganze Zahlen, so ist die multiplikative Inverse von a modulo m diejenige (eindeutig bestimmte) positive Zahl $b < m$, welche die Gleichung*

$$1 \equiv a \cdot b \bmod m$$

erfüllt. Man schreibt auch $b = a^{-1} \bmod m$.

Beispiel 3.1 *Ein erstes Beispiel: Sei $a = 7$ und $m = 3$. Gesucht sei das multiplikative Inverse von 7 modulo 3, also $b = 7^{-1} \bmod 3$. Mit anderen Worten, wir suchen die ganze Zahl $b < 3$, für die*

$$1 \equiv 7 \cdot b \bmod 3$$

ist. Dies ist ganz einfach, wenn wir eine Multiplikationstabelle für die Restklassen modulo 3 haben; denn dann können wir die gesuchte Zahl b ganz einfach hieraus ablesen. Zunächst ist $7 \bmod 3 \equiv 1$. Aus der Multiplikationstabelle modulo 3 (vgl. Abschnitt 2.1) lesen wir ab: $1 \cdot 1 = 1$. Also ist hier $b = 1$.

Beispiel 3.2 *Ein zweites Beispiel: Sei $a = 7$ und $m = 4$. Gesucht sei jetzt das multiplikative Inverse von 7 modulo 4, also $b = 7^{-1} \bmod 4$. Mit anderen Worten, wir suchen die ganze Zahl $b < 4$, für die*

$$1 \equiv 7 \cdot b \bmod 4$$

ist. Es ist $7 \bmod 4 \equiv 3$. Aus der Multiplikationstabelle modulo 4 (vgl. Abschnitt 2.1) lesen wir ab: $3 \cdot 3 = 1$. Also ist hier $b = 3$.

Bemerkung 3.1 *Die multiplikative Inverse von a modulo m existiert nur, wenn a und m teilerfremd sind. Man kann dies exemplarisch aus den entsprechenden Multiplikationstabellen ablesen.*

Es gibt einfache mathematische Methoden, um das multiplikative Inverse modulo einer Zahl m zu bestimmen (vgl. Abschnitt 4.2). In der Praxis führt man die RSA-Verschlüsselung und die RSA-Entschlüsselung mit Hilfe von Computern durch, auf denen man diese Methoden einfach programmieren kann.

3.3 Wie funktioniert Verschlüsselung mit RSA?

Wir nehmen an, ein Sender namens Bob will einer Empfängerin namens Alice eine geheime Nachricht zusenden. Dazu verwandelt Bob seine Nachricht zunächst in eine Zahl, etwa indem er die Buchstaben eindeutig durch Zahlen ersetzt.

RSA verläuft dann folgendermaßen:

Alice	**Kommunikation zwischen Alice und Bob**	**Bob**

Alice wählt zwei verschiedene Primzahlen p und q, z.B. $p = 5$ und $q = 11$. Alice berechnet

$$n = pq = 55$$

sowie

$$m = (q-1)(p-1) = 40 \ .$$

Alice wählt eine Zahl a, die zu m teilerfremd ist, z.B.

$$a = 7 \ .$$

Alice gibt die Zahlen n und a als ihren öffentlichen Schlüssel bekannt:

$$\begin{aligned} n &= 55 \\ a &= 7 \end{aligned}$$

Bobs Nachricht ist eine Zahl x, die kleiner als n ist, z.B. $x = 8$. Bob verschlüsselt sie gemäß

$$\begin{aligned} y &= x^a \bmod n \\ &= 8^7 \bmod 55 = 2 \end{aligned}$$

Bob sendet y an Alice:

$$y = 2 \ .$$

Alice berechnet aus a und m das multiplikative Inverse von a modulo m:

$$\begin{aligned} b &= a^{-1} \bmod m \\ &= 7^{-1} \bmod 40 = 23 \ . \end{aligned}$$

Sie kann Bobs Nachricht mit der Formel

$$x = y^b \bmod n = 2^{23} \bmod 55 = 8$$

wieder entschlüsseln.

Bemerkung 3.2 *Details zu den in diesem Schaubild enthaltenen Rechnungen:*

$$\begin{aligned} 8^7 \bmod 55 &= 8^2 \cdot 8^2 \cdot 8^2 \cdot 8 \bmod 55 \\ &= 9 \cdot 9 \cdot 9 \cdot 8 \bmod 55 \\ &= 81 \cdot 72 \bmod 55 \\ &= 26 \cdot 17 \bmod 55 \\ &= 442 \bmod 55 \\ &= 8 \cdot 55 + 2 \bmod 55 \\ &= 2 \end{aligned}$$

Ferner gilt

$$7^{-1} \bmod 40 = 23$$

wegen

$$7 \cdot 23 \bmod 40 = 161 \bmod 40 = 4 \cdot 40 + 1 \bmod 40 = 1 \ .$$

Die multiplikative Inverse modulo 40 zur Zahl 7 ist also die Zahl 23.

Bemerkung 3.3 (RSA in der Praxis:) *In der Praxis wählt man die Primzahlen p und q sehr groß. In der Regel haben beide mehrere Hundert Stellen. Die zugehörigen Berechnungen werden mit Hilfe von Computerprogrammen erledigt.*

Ist die zu verschlüsselnde Nachricht größer als n, so teilt man die Nachricht in mehrere kleinere Nachrichten und verschlüsselt und sendet diese unabhängig voneinander.

3.4 Warum ist die RSA-Verschlüsselung sicher?

Der öffentliche Schlüssel von Alice besteht aus den beiden Zahlen n und a und ist allgemein bekannt. Zum Entschlüsseln benötigt Alice lediglich die Zahl m. Hiermit kann sie b (das Inverse von a modulo m) bestimmen und so durch modulares Potenzieren die Nachricht entschlüsseln.

Wenn es also gelingen würde, aus der Kenntnis von n die Zahl m zu ermitteln, wäre RSA nicht sicher. Wegen

$$n = pq$$

und

$$m = (p-1)(q-1)$$

wäre dies leicht möglich, wenn es gelänge, n in seine beiden Primfaktoren p und q zu zerlegen. Bisher ist jedoch kein Verfahren bekannt, mit dem dies für große Primzahlen p und q in weniger als vielen Monaten gelingt. Daher kann RSA für hinreichend große Primzahlen als eine sehr sichere Art der Verschlüsselung betrachtet werden.

Sollte jedoch eine Methode entdeckt werden, mit der man aus n seine beiden Primfaktoren p und q oder $m = (p-1)(q-1)$ relativ einfach berechnen könnte, wäre RSA kein sicheres Verschlüsselungsverfahren mehr.

3.5 Warum funktioniert die RSA-Verschlüsselung? – Die Mathematik hinter RSA

In Abschnitt 3.3 haben wir die Funktionsweise von RSA beschrieben. Wir fassen dies noch einmal kurz zusammen:

- Alice wählt zwei verschiedene Primzahlen p und q und berechnet

  $$n = pq$$

  sowie

  $$m = (q-1)(p-1) \ .$$

  Ferner wählt Alice eine Zahl a, die zu m teilerfremd ist.

- a und n bilden den öffentlichen Schlüssel von Alice.

- Bobs Nachricht ist eine Zahl x, die kleiner als n ist. Er verschlüsselt sie nach der Formel

  $$y = x^a \bmod n \ .$$

- Zur Entschlüsselung berechnet Alice aus a und m zunächst das multiplikative Inverse von a modulo m:

  $$b = a^{-1} \bmod m$$

  und entschlüsselt dann Bobs Nachricht mittels

  $$x = y^b \bmod n \ . \tag{1}$$

Zu verstehen, warum RSA funktioniert, bedeutet mathematisch nichts anderes als die Gültigkeit der Gleichung (1) zu beweisen, also zu zeigen, dass $y^b \bmod n$ gerade wieder x ergibt.

Für diesen Beweis benötigen wir den Satz von Euler-Fermat:

Satz 3.1 (Euler-Fermat) *Sind a und n teilerfremde Zahlen mit $1 < a < n$, so gilt*

$$a^{\varphi(n)} \equiv 1 \bmod n \ . \tag{2}$$

Hierbei ist $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen[1]*.*

Diesen Satz wollen wir hier nicht beweisen. Wir werden ihn aber gleich benutzen, um Gleichung (1) für $x \neq p$ und $x \neq q$ zu beweisen. (Für $x = q$ und $x = p$ kann Gleichung (1) mit Hilfe des Chinesischen Restsatzes weitgehend analog bewiesen werden. Hierzu verweisen wir auf [5].)

Bevor wir den Beweis durchführen, vermerken wir noch, dass für Primzahlen p, q und $n = pq$ gilt

$$\varphi(p) = p-1 \qquad \varphi(q) = q-1 \qquad \text{sowie} \qquad \varphi(n) = \varphi(pq) = (p-1)(q-1) \ . \tag{3}$$

[1] Zur Erinnerung: Zwei Zahlen sind teilerfremd, wenn ihr größter gemeinsamer Teiler 1 ist.

Hiermit folgt:

$$
\begin{aligned}
y^b \bmod n &= (x^a \bmod n)^b \bmod n \\
&= (x^a)^b \bmod n \\
&= x^{ab} \bmod n && b \text{ ist das multiplikative Inverse zu } a, \text{ also } a \cdot b \bmod m \equiv 1 \ . \\
& && \text{D.h. es gibt } k \in \mathbb{Z} \text{ so dass } a \cdot b = k \cdot m + 1 \\
&= x^{k \cdot m + 1} \bmod n \\
&= x^{k \cdot m} \cdot x \bmod n \\
&= (x^m)^k \cdot x \bmod n \\
&= ((x^m)^k \bmod n) \cdot (x \bmod n) \bmod n \\
&= ((x^m) \bmod n)^k \cdot (x \bmod n) \bmod n \\
&= (1^k \bmod n) \cdot (x \bmod n) \bmod n && \text{wegen des Satzes von Euler-Fermat (sofern } x \text{ und } n \text{ teilerfremd sind), da } m = (p-1)(q-1) = \varphi(n) \text{ gesetzt wurde} \\
&= 1 \cdot x \bmod n \\
&= x && \text{wegen } x < n
\end{aligned}
$$

Damit ist Gleichung (1) bewiesen für $x \neq q$ und $x \neq p$ (um den Satz von Fermat-Euler anwenden zu können, müssen x und $n = pq$ als teilerfremd vorausgesetzt werden). Die RSA-Entschlüsselung liefert also wieder die Ausgangszahl.

4 Details zu Berechnungen beim RSA-Verfahren

Wollen Schüler/-innen den RSA-Algorithmus per Hand durchführen, ist es sinnvoll, dass sie zunächst entdecken, wie man das modulare Potenzieren möglichst einfach durchführen kann (vgl. hierzu Abschnitt 4.1).

Greift man hingegen auf Rechner zurück, muss man lediglich beachten, dass ganze Zahlen auf dem Rechner in manchen Programmiersprachen nur bis zu einer maximal darstellbaren Zahl unterstützt werden. Da beim Potenzieren recht schnell sehr große Zahlen auftauchen, sollte man die Modulo-Funktion daher auch mit unter den Exponenten ziehen.

Ferner ist in beiden Fällen noch die Bestimmung des multiplikativen Inversen modulo m erforderlich (vgl. Abschnitt 4.2).

4.1 Modulares Potenzieren

Anhand des Arbeitsblatts *Modulares Potenzieren* sollen die Schüler/-innen selbständig Methoden erlernen und anwenden, um das modulare Potenzieren per Hand möglichst einfach durchzuführen. Vorausgesetzt wird dabei allerdings, dass die Rechenregeln für Potenzen den Schüler/-innen gut bekannt sind.

4.2 Bestimmung des multiplikativen Inversen

Grundlage für die Bestimmung des multiplikativen Inversen einer Zahl a modulo einer Zahl m, wobei a und m teilerfremd sind, ist der Euklidische Algorithmus, mit dem man sehr einfach den größten gemeinsamen Teiler zweier Zahlen berechnen kann.

4.2.1 Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen

Es gibt verschiedene Möglichkeiten, um den größten gemeinsamen Teiler (ggT) zweier Zahlen a und b (kurz: $\mathrm{ggT}(a, b)$) zu bestimmen. Man kann dies beispielsweise über eine Primfaktorzerlegung der beiden Zahlen und anschließenden Abgleich der gemeinsamen Primfaktoren vornehmen oder auch mit dem Euklidischen Algorithmus. Dabei erfordert der Euklidische Algorithmus in vielen Fällen weniger Rechenaufwand als die Primfaktorzerlegung.

Nehmen wir beispielsweise an, wir wollen $\mathrm{ggT}(8, 5)$ bestimmen. Es gilt

$$8 : 5 = 1 \text{ Rest } 3 \ .$$

Basis des Euklidischen Algorithmus ist jetzt, dass $\mathrm{ggT}(8,5)=\mathrm{ggT}(5,3)$ gilt, d.h. anstatt den ggT der beiden ursprünglichen Zahlen zu ermitteln, reicht es aus, den ggT aus der kleineren dieser beiden Zahlen und dem Rest, der entsteht, wenn wir die gegebenen beiden Zahlen durcheinander dividieren, zu bestimmen. Dies gilt allgemein; wir verzichten hier jedoch auf einen Beweis. Dieser Ansatz kann rekursiv angewendet werden:

$$5 : 3 = 1 \text{ Rest } 2 \qquad \Longrightarrow \qquad \mathrm{ggT}(5, 3) = \mathrm{ggT}(3, 2)$$

sowie

$$3 : 2 = 1 \text{ Rest } 1 \qquad \Longrightarrow \qquad \mathrm{ggT}(3, 2) = \mathrm{ggT}(2, 1)$$

und schließlich

$$2 : 1 = 2 \text{ Rest } 0 \ .$$

Der letzte von 0 verschiedene Rest ist dann der ggT der beiden ursprünglichen Zahlen. Also: $\mathrm{ggT}(8, 5) = \mathrm{ggT}(5, 3) = \mathrm{ggT}(3, 2) = \mathrm{ggT}(2, 1) = 1$.

Beispiel 4.1 *Ein weiteres Beispiel für den Euklidischen Algorithmus: Zu bestimmen sei ggT(120,72). Es gilt*

$$\begin{aligned} 120 : 72 = 1 \ \textit{Rest}\ 48 \qquad &\Longrightarrow \qquad ggT(120, 72) = ggT(72, 48) \\ 72 : 48 = 1 \ \textit{Rest}\ 24 \qquad &\Longrightarrow \qquad ggT(72, 48) = ggT(48, 24) \\ 48 : 24 = 2 \ \textit{Rest}\ 0 \qquad &\Longrightarrow \qquad ggT(48, 24) = 24 \ . \end{aligned}$$

Wir haben also

$$ggT(120, 72) = ggT(72, 48) = ggT(48, 24) = 24 \ .$$

Das Arbeitsblatt *Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen* unterstützt die Schüler/-innen bei der Erarbeitung des Euklidischen Algorithmus zur Bestimmung des ggT zweier gegebener Zahlen.

4.2.2 Bestimmung des multiplikativen Inversen zweier Zahlen mit dem Euklidischen Algorithmus

Sind a und m zwei teilerfremde positive ganze Zahlen, so ist die multiplikative Inverse b zu a modulo m die eindeutig bestimmte positive Zahl $b < m$, welche die Gleichung

$$(b \cdot a) \bmod m = 1$$

erfüllt. Diese Gleichung können wir auch schreiben als

$$1 = b \cdot a + k \cdot m \tag{4}$$

mit $k \in \mathbb{Z}$. Wir wollen in diesem Abschnitt beschreiben, wie man die multiplikative Inverse berechnen kann. Das Ziel unseres Vorgehens wird dabei sein, die Zahl 1 als Linearkombination der Zahlen a und m zu schreiben.

Um diese multiplikative Inverse zu bestimmen, können wir den Euklidischen Algorithmus verwenden. Es sei $a = 5$ und $m = 8$. Wir führen jetzt in der linken Spalte den Euklidischen Algorithmus durch, bis der Rest 1 auftaucht, in der rechten Spalte schreiben wir dies in einer multiplikativen Form:

$$8 : 5 = 1 \text{ Rest } 3 \iff 8 = 1 \cdot 5 + 3 \tag{5}$$
$$5 : 3 = 1 \text{ Rest } 2 \iff 5 = 1 \cdot 3 + 2 \tag{6}$$
$$3 : 2 = 1 \text{ Rest } 1 \iff 3 = 1 \cdot 2 + \boxed{\mathbf{1}} \tag{7}$$

Idee des weiteren Vorgehens: Die Grundlage für das weitere Vorgehen ist, dass bei teilerfremden Zahlen im Euklidischen Algorithmus als Rest irgendwann die Zahl $\boxed{1}$ auftaucht. Die Idee ist jetzt, die letzte Gleichung in der Form $\boxed{\mathbf{1}} = 3 - 1 \cdot 2$ zu schreiben und hier die Zahlen 2 und 3, die als Reste in vorherigen Schritten des Euklidischen Algorithmus entstanden sind (vgl. die Gleichungen (5) und (6), mit Hilfe dieser Gleichungen zu eliminieren, so dass man auf der rechten Seite nur noch Vielfache der ursprünglichen Zahlen 8 und 5 erhält, also

$$1 = k_1 \cdot 5 + k_2 \cdot 8 \tag{8}$$

mit ganzen Zahlen k_1 und k_2. (Man mache sich klar, dass diese Gleichung der Gleichung (4) entspricht.) Betrachten wir Gleichung (8) modulo 8, so erhalten wir

$$1 = (k_1 \cdot 5) \bmod 8$$

und das multiplikative Inverse zu 5 modulo 8 ist die Zahl k_1 mod 8.

Durchführung dieser Idee: Wie gerade beschrieben, verwenden wir die einzelnen Schritte des Euklidischen Algorithmus (in der multiplikativen Form) in umgekehrter Reihenfolge. Die letzte Gleichung in der multiplikativen Form (7) können wir auch schreiben als

$$1 = 3 - 1 \cdot 2 \ . \tag{9}$$

Die 2 in dieser Gleichung wollen wir mit Hilfe von (6) ersetzen und lösen daher (6) nach dem Rest (d.h. nach der Zahl 2) auf

$$2 = 5 - 1 \cdot 3 \ .$$

Einsetzen in Gleichung (9) liefert

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 \ . \tag{10}$$

Analog ersetzen wir jetzt die Zahl 3 in dieser Gleichung mit Hilfe des ersten Schritts des Euklidischen Algorithmus. Dazu lösen wir Gleichung (5) nach dem Rest (d.h. der Zahl 3) auf

$$3 = 8 - 1 \cdot 5$$

und setzen dies in Gleichung (10) ein:

$$1 = 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5 \ .$$

Betrachten wir diese Gleichung jetzt modulo 8, so erhalten wir

$$1 = (-3 \cdot 5) \bmod 8 = (5 \cdot 5) \bmod 8 \qquad \text{wegen} \qquad -3 \bmod 8 = 5 \bmod 8 \ .$$

Offenbar gilt also $1 = (5 \cdot 5) \bmod 8$ und wir haben die multiplikative Inverse zu 5 modulo 8 gefunden. Es ist die Zahl 5 selber. Wir können dies leicht überprüfen:

$$(5 \cdot 5) \bmod 8 = 25 \bmod 8 = 1 \ .$$

Ein zweites Beispiel: Wir suchen die modulare Inverse zu 13 mod 160. Euklidischer Algorithmus:

$$160 : 13 = 12 \text{ Rest } 4 \implies 160 = 12 \cdot 13 + 4 \tag{11}$$

$$13 : 4 = 3 \text{ Rest } 1 \implies 13 = 3 \cdot 4 + 1 \tag{12}$$

Wir gehen wieder rückwärts vor und erhalten aus (12)

$$1 = 13 - 3 \cdot 4 \ . \tag{13}$$

Ersetzen wir hierin die Zahl 4 gemäß Gleichung (11) durch

$$4 = 160 - 12 \cdot 13 \ ,$$

so erhalten wir aus (13)

$$1 = 13 - 3 \cdot (160 - 12 \cdot 13) = 13 - 3 \cdot 160 + 3 \cdot 12 \cdot 13 = 37 \cdot 13 - 3 \cdot 160 \ .$$

Betrachten wir diese Gleichung modulo 160, so erhalten wir

$$1 = (37 \cdot 13) \bmod 160 \ .$$

Das multiplikative Inverse zur Zahl 13 modulo 160 ist die Zahl 37. Probe:

$$13 \cdot 37 = 481 = 3 \cdot 160 + 1$$

Leichter geht die Berechnung (sowohl von Hand als auch in Hinblick auf die Programmierung), wenn man folgende Variante des Algorithmus verwendet:

Einfachere Variante:
Wir suchen wieder eine positive Zahl $b < 160$, so dass $(13 \cdot b) \bmod 160 = 1$ gilt.

Zeile	Verfahren			Erläuterung
(I)	160	1	0	Dies steht für $\boxed{160} = \boxed{1} \cdot 160 + \boxed{0} \cdot 13$
(II)	13	0	1	Dies steht für $\boxed{13} = \boxed{0} \cdot 160 + \boxed{1} \cdot 13$
				Wie oft geht 13 in 160? 12 mal; also (III) = (I) $-12\cdot$ (II)
(III)	4	1	-12	Dies steht für $\boxed{4} = \boxed{1} \cdot 160\boxed{-12} \cdot 13$
				Wie oft geht 4 in 13? 3 mal; also (IV) = (II) $-3\cdot$ (III)
(IV)	$\boxed{1}$	-3	$\boxed{37}$	Dies steht für $\boxed{1} = \boxed{-3} \cdot 160 + \boxed{37} \cdot 13$

Das Verfahren hat jetzt in der ersten Spalte eine 1 erzeugt. Damit haben wir die multiplikative Inverse zu 13 mod 160 gefunden. Sie steht in der letzten Spalte des Verfahrens und lautet 37.

Analog können wir das alternative Verfahren auch auf unser erstes Beispiel $a = 5$ und $m = 8$ anwenden:

(I)	8	1	0	
(II)	5	0	1	Wie oft geht 5 in 8? 1 mal; also (III)=(I)$-1\cdot$(II)
(III)	3	1	-1	Wie oft geht 3 in 5? 1 mal; also (IV)=(II)$-1\cdot$(III)
(IV)	2	-1	2	Wie oft geht 2 in 3? 1 mal; also (V)=(III)$-1\cdot$(IV)
(V)	1	2	-3	In erster Spalte taucht 1 auf; multiplikative Inverse gefunden!

In diesem (und anderen Beispielen) taucht als multiplikative Inverse eine negative Zahl (hier: -3) auf. Wir sind jedoch an einer positiven Zahl b interessiert. Diese erhalten wir leicht durch $-3 \bmod 8 = 5$. Dies kann man auch sehen, wenn man Gleichung (V) ausgeschrieben betrachtet:

$$1 = 2 \cdot 8 - 3 \cdot 5 = (-3 \cdot 5) \bmod 8 = (5 \cdot 5) \bmod 8$$

und $b = 5$ ist tatsächlich die multiplikative Inverse modulo 8 zu 5.

Das Arbeitsblatt *Multiplikatives Inverses modulo einer Zahl m* beschränkt sich auf die einfachere Variante des Algorithmus. Damit können sich leistungsstarke Schüler/-innen die Bestimmung des multiplikativen Inversen mit dem Euklidischen Algorithmus selbständig erarbeiten.

In einer normalen Klasse empfiehlt sich hierzu Gruppenarbeit, damit sich die Schüler/-innen bei Verständnisproblemen gegenseitig unterstützen können.

Es ist jedoch ratsam, das Vorgehen bei der auf dem Arbeitsblatt beschriebenen Variante noch einmal detailliert an der Tafel zu erläutern oder von leistungsstarken Schüler/-innen erläutern zu lassen, bevor die Schüler/-innen sich mit Aufgabe 2 beschäftigen.

5 Unterrichtsmaterialien

Neben einem Memo, aus dem die Schüler/-innen den Ablauf von RSA auf einen Blick ersehen können, und einer Vielzahl von Arbeitsblättern, sind diesem Unterrichtsmodul auch einige Computerprogramme beigefügt, die von der Lehrkraft zu Demozwecken oder von den Schüler/-innen zum Ausprobieren verwendet werden können. Die vorliegende Unterrichtseinheit kommt jedoch auch völlig ohne diese Computerprogramme aus und ist in keiner Weise hiervon abhängig.

Beginnend mit den Computerprogrammen, werden die Materialien im Folgenden dargestellt und erläutert.

5.1 Computerprogramme

Alle beigefügten Computerprogramme sind in der Programmiersprache Python geschrieben (Version 2.6.x oder 2.7.x). Python ist frei verfügbar und kann über die Web-Seite www.python.org frei heruntergeladen werden. Dort finden sich auch entsprechende Tutorials etc.

Python wurde mit dem Ziel entwickelt, das Programmieren für den Programmierer möglichst einfach zu machen. Daher kann man Python mit relativ wenig Aufwand so weit lernen, dass man alle in der Schule vorkommenden Algorithmen problemlos programmieren kann. Wir haben dies mehrfach mit (heterogenen) Gruppen von Schülerpraktikanten der Klassen 9 - 13 erprobt und sehr gute Erfahrungen mit einer zwei- bis dreitägigen Einführung in Python gemacht.

Auf Wunsch können wir auch entsprechendes Material zur Verfügung stellen.

Python ist nicht die schnellste Programmiersprache und nach unseren Erfahrungen in der Ausführung etwa einen Faktor 30 langsamer als entsprechende optimierte C-Programme. Der Aufwand, C oder eine vergleichbare Programmiersprache zu lernen oder einen komplizierten Algorithmus in C zu programmieren, ist dafür aber wesentlich höher als bei Python.

5.1.1 Computerprogramm: Bestimmung des größten gemeinsamen Teilers zweier Zahlen

Das Python-Programm ggt_euklid.py berechnet zu zwei einzugebenden natürlichen Zahlen deren größten gemeinsamen Teiler mit dem Euklidischen Algorithmus.

5.1.2 Computerprogramm zur Bestimmung des multiplikativen Inversen modulo einer Zahl m

Das Python-Programm multiplikatives_inverses.py berechnet zu zwei einzugebenden Zahlen m und a die multiplikative Inverse von a mod m mit dem Euklidischen Algorithmus.

5.1.3 Computerprogramme zur Durchführung des RSA-Verfahrens

Das Python-Programm rsa_keys_and_decoding.py ermittelt zu zwei einzugebenden Primzahlen p und q und zu einer zu $m = (p-1)(q-1)$ teilerfremden einzugebenden Zahl a den aus $n = pq$ und a bestehenden öffentlichen Schlüssel des RSA-Verfahrens und gibt ihn aus. (Dabei wird die Teilerfremdheit überprüft und ggf. eine erneute Eingabe verlangt.) Dann bietet das Programm die Option, Nachrichten zu entschlüsseln, die mit diesem öffentlichen Schlüssel verschlüsselt wurden.

Das Gegenstück zu diesem Programm ist das Python-Programm rsa_encoding.py, das einzugebende Nachrichten mit dem ebenfalls einzugebenden öffentlichen Schlüssel verschlüsselt.

Mit den beiden Programmen können jeweils Paare von Schüler/-innen Nachrichten (in Form von Ziffernfolgen) verschlüsseln, austauschen und wieder entschlüsseln.

5.2 Arbeitsblätter und Memo

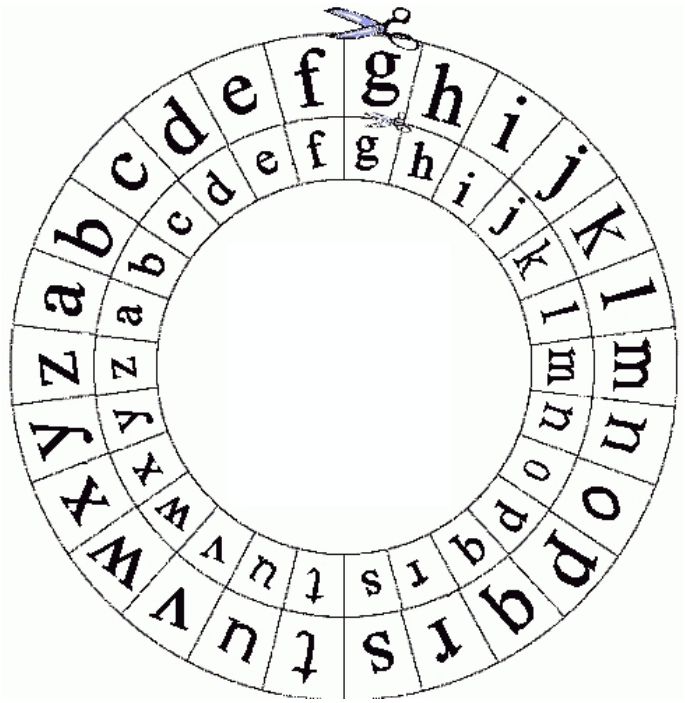
Die Arbeitsblätter werden in der Reihenfolge vorgestellt, in der sie auch im Unterricht zum Einsatz kommen können. Das Memo ist in diese Reihenfolge eingebettet. Diese Reihenfolge ist jedoch nicht zwingend. So können verschiedene Arbeitsblätter auch vorgezogen, andere weggelassen werden.

Zu jedem Arbeitsblatt gibt es ein Erläuterungsblatt mit den Lösungen der Aufgaben und ggf. zusätzlichen Infos für Lehrkräfte.

Die ersten beiden Arbeitsblätter *Caesar-Code und Restklassen* sowie *Modulo-Rechnen* können bereits in den Klassenstufen 5 oder 6 eingesetzt werden.

Arbeitsblatt: Caesar-Code und Restklassen

Der Caesar-Code ist eine Verschlüsselung, die jedem Buchstaben im Alphabet einen anderen Buchstaben zuordnet. Dabei behält man die Reihenfolge des Alphabets ein, verschiebt es aber um eine bestimmte Anzahl von Stellen. Das hier abgebildete Caesar-Rad hilft bei der Verwendung des Caesar-Codes. Die beiden Scheiben sind drehbar, sodass jede Einstellung eine andere Verschlüsselungsvorschrift ergibt.



Aufgaben:

1. Wie viele verschiedene Einstellungen des Caesar-Rads gibt es?
2. Wie viele verschiedene Verschlüsslungen sind mit dem Caesar-Code möglich?
3. Bastele dir selbst ein solches Caesar-Rad oder schneide die obige Abbildung aus und trenne die beiden Buchstabenringe.
4. Verschlüssele das Wort GEHEIMTEXT mit einem Caesar-Code deiner Wahl. Tausche nun deinen verschlüsselten Text mit deinem Nachbarn aus und finde heraus, welche Verschlüsselungsvorschrift verwendet wurde.
5. Ähnlich wie beim Caesar-Rad kann man auch jedem Buchstaben eine Zahl zuordnen, im gewöhnlichen Alphabet die Zahlen 1-26, was wie folgt aussehen könnte:

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

   (a) Verschlüssele die Worte *und* und *Band* mit dieser Tabelle in eine Zahlenreihe.
   (b) Was fällt dir dabei auf?
   (c) Welche Probleme können entstehen, wenn man diesen Zahlencode einsetzt?
   (d) Wie könnte man die Zahldarstellung ändern, so dass diese Probleme nicht entstehen?
6. Wie sähe die Tabelle aus der vorigen Aufgabe aus, wenn man wie beim Caesar-Code die Zahlenreihe zum Beispiel um 2 verschiebt? Welche Zahlen werden den Buchstaben dann zugeordnet? Beachte, dass nur die Zahlen von 1 bis 26 vorkommen sollen.

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

Arbeitsblatt: Caesar-Code und Restklassen

Infos für Lehrkräfte:

- Dieses Arbeitsblatt kann bereits in den Stufen 5 und 6 eingesetzt werden. Schüler/-innen dieser Stufen sind meist sehr leicht für Geheimschriften etc. zu begeistern.
- Für Aufgabe 3 sollten die Schüler/-innen ggf. eine Schere mitbringen; alternativ eignet sich diese Aufgabe auch als Hausaufgabe.

Lösungen der Aufgaben:

1. Insgesamt gibt es 26 Einstellungen des Caesar-Rads (der Buchstabe a kann jedem der 26 Buchstaben zugeordnet werden).
2. Beim Caesar-Code gibt es 25 verschiedene Verschlüsslungen (die Zuordnung $a \to a$ ist keine Verschlüsselung, sondern erhält den Originaltext).
3. Für diese Aufgabe sollten die Schüler/-innen ggf. eine Schere mitbringen; diese Aufgabe ist auch als Hausaufgabe geeignet.
4. Je nach Einstellung des Caesar-Rads sind 25 verschiedene Lösungen möglich. Beispiel: Beim Verschieben um zwei Buchstaben erhält man IGJGKOVGZV.
5. (a) *und* liefert die Ziffernfolge 21144; *Band* liefert die Ziffernfolge 21144.
   (b) Die beiden Ziffernfolgen sind identisch.
   (c) Die Entschlüsselung ist nicht eindeutig möglich; 21144 kann sowohl *Band* als auch *und* bedeuten, also können Missverständnisse entstehen.
   (d) Hier sind verschiedene Antworten möglich: Der Grund für die auftretenden Probleme ist, dass teilweise eine, teilweise zwei Ziffern für einen Buchstaben verwendet werden, was zu Mehrdeutigkeiten führt (z.B. steht 12 sowohl für L als auch für AB, 14 sowohl für AD als auch für N). Dies kann z.B. dadurch verhindert werden, dass man jedem Buchstaben genau zwei Ziffern zuordnet, A also nicht 1, sondern z.B. 01, B dann die 02 usw. Es sind aber auch viele andere eindeutige Zuordnungen denkbar, etwa wenn man nicht die Zahlen von 1 bis 26, sondern die von 11 bis 36 verwendet.
6. Bei einem Verschieben um 2 sähe die Zahlenreihe folgendermaßen aus:

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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2

   Wenn die Schüler/-innen die Ergebnisse aus der vorigen Aufgabe bereits mit einfließen lassen, könnten anstelle der einziffrigen Zuordnungen bereits unterschiedliche zweiziffrige entstanden sein.

Arbeitsblatt: Modulo-Rechnen

Ersetzt man beim Caesar-Code die Buchstaben durch Zahlen und beginnt für A bei 3, so wird B durch 4 ersetzt usw. Was passiert mit Y und Z? Eigentlich müsste dann Y mit 27 und Z mit 28 verschlüsselt werden. Tatsächlich wird Y mit 1 verschlüsselt und Z mit 2. Y entspricht also der 1 und Z entspricht der 2, aber auch der 27 und der 28. Für diese beiden Buchstaben nimmt man also den Rest, den man erhält, wenn man durch 26 (Anzahl der Buchstaben im Alphabet) dividiert. (Buchstabe 27 und 28 existieren ja nicht). Dies ist ein Beispiel für das sogenannte "Rechnen modulo 26". Man schreibt dafür auch:
$\boxed{27 \bmod 26 = 1}$. Dies heißt, wenn wir 27 durch 26 teilen, erhalten wir den Rest 1. Entsprechend ist $28 \bmod 26 = 2$, denn $28 : 26 = 1$ Rest 2.

Weitere Beispiele:

$$\begin{aligned} 19 \bmod 4 = 3 \ , &\quad \text{denn} \quad 19 : 4 = 4 \text{ Rest } 3 &\quad \text{oder} \quad 19 = 4 \cdot 4 + 3 \ , \\ 5 \bmod 3 = 2 \ , &\quad \text{denn} \quad 5 : 3 = 1 \text{ Rest } 2 &\quad \text{oder} \quad 5 = 1 \cdot 3 + 2 \ , \\ 17 \bmod 6 = 5 \ , &\quad \text{denn} \quad 17 : 6 = 2 \text{ Rest } 5 &\quad \text{oder} \quad 17 = 2 \cdot 6 + 5 \ . \end{aligned}$$

Dies kann man auch allgemein definieren:

Definition: Teilt man eine natürliche Zahl a durch eine natürliche Zahl m, so erhält man einen Rest r. Für diesen Rest gilt $0 \leq r \leq m-1$. Die sogenannte Modulo-Funktion liefert zu gegebenen Zahlen a und m gerade diesen Rest r. Man schreibt auch:

$$a \bmod m = r \ .$$

Aufgaben:

1. Berechne
   a) $27 \bmod 4$ b) $26 \bmod 5$ c) $18 \bmod 3$ d) $18 \bmod 7$ e) $21 \bmod 9$
   f) $37 \bmod 10$ g) $100037 \bmod 10$ h) $107 \bmod 4$ i) $1 \bmod 2$ j) $3 \bmod 2$

2. (a) Es sei k irgendeine gerade Zahl. Berechne k mod 2.
   (b) Es sei k irgendeine ungerade Zahl. Berechne k mod 2.
   (c) Berechne 34 mod 4.
   (d) Berechne 134 mod 4.

3. (a) Vergleiche $25 \bmod 4$ und $(20 \bmod 4 + 5 \bmod 4) \bmod 4$
   (b) Vergleiche $25 \bmod 4$ und $(19 \bmod 4 + 6 \bmod 4) \bmod 4$
   (c) Vergleiche $26 \bmod 4$ und $(2 \bmod 4 \cdot 13 \bmod 4) \bmod 4$
   (d) Vergleiche $7^3 \bmod 4$ und $(7 \bmod 4)^3 \bmod 4$
   Dies sind Beispiele für die folgenden allgemeinen Regeln beim Modulo-Rechnen:

$$\begin{aligned} (a+b) \bmod m &= (a \bmod m + b \bmod m) \bmod m \\ (a-b) \bmod m &= (a \bmod m - b \bmod m) \bmod m \\ (a \cdot b) \bmod m &= (a \bmod m \cdot b \bmod m) \bmod m \\ (a^b) \bmod m &= (a \bmod m)^b \bmod m \end{aligned}$$

4. (a) Es sei n irgendeine natürliche Zahl, die mit den Ziffern $\ldots 34$ endet. Berechne $n \bmod 4$.
   (b) Wie kann man leicht überprüfen, ob eine Zahl durch 4 teilbar ist?

5. Es ist 10 Uhr am Vormittag (Mittwoch) und du hast in 50 Stunden einen Termin beim Zahnarzt und in 70 Stunden einen Computerkurs. Wann finden die Termine statt?

Arbeitsblatt: Modulo-Rechnen

Infos für Lehrkräfte:

Dieses Arbeitsblatt kann, evtl. mit Ausnahme von Aufgabe 3(d), für die die Kenntnis der Potenzschreibweise erforderlich ist, bereits ab Klasse 5 eingesetzt werden. In diesem Fall empfiehlt es sich, das Modulo-Rechnen an der Tafel einzuführen und einige Beispiele gemeinsam zu rechnen, bevor die Schüler/-innen die auf dem Arbeitsblatt gestellten Aufgaben selbständig lösen.

Lösungen der Aufgaben:

1. (a) $27 \bmod 4 = 6 \cdot 4 + 3 \bmod 4 = 3$
   (b) $26 \bmod 5 = 5 \cdot 5 + 1 \bmod 5 = 1$
   (c) $18 \bmod 3 = 6 \cdot 3 + 0 \bmod 3 = 0$
   (d) $18 \bmod 7 = 2 \cdot 7 + 4 \bmod 7 = 4$
   (e) $21 \bmod 9 = 2 \cdot 9 + 3 \bmod 9 = 3$
   (f) $37 \bmod 10 = 3 \cdot 10 + 7 \bmod 10 = 7$
   (g) $100037 \bmod 10 = 10000 \cdot 10 + 7 \bmod 10 = 7$
   (h) $107 \bmod 4 = 25 \cdot 4 + 7 \bmod 4 = 7 \bmod 4 = 1 \cdot 4 + 3 \bmod 4 = 3$
   (i) $1 \bmod 2 = 0 \cdot 2 + 1 \bmod 2 = 1$
   (j) $3 \bmod 2 = 1 \cdot 2 + 1 \bmod 2 = 1$
2. (a) Dividiert man eine gerade Zahl durch 2, so erhält man den Rest 0. k gerade $\Rightarrow k \bmod 2 = 0$
   (b) Dividiert man eine ungerade Zahl durch 2, so erhält man den Rest 1. k ungerade $\Rightarrow k \bmod 2 = 1$
   (c) $34 \bmod 4 = 2$
   (d) $134 \bmod 4 = 2$
3. In allen Teilaufgaben kommen jeweils die gleichen Ergebnisse heraus:
   (a) $(20 \bmod 4 + 5 \bmod 4) \bmod 4 = (0 + 1) \bmod 4 = 1 = 25 \bmod 4$
   (b) $(19 \bmod 4 + 6 \bmod 4) \bmod 4 = (3 + 2) \bmod 4 = 5 \bmod 4 = 1 = 25 \bmod 4$
   (c) $2 \bmod 4 \cdot 13 \bmod 4) \bmod 4 = (2 \cdot 1) \bmod 42 = 26 \bmod 4$
   (d) $7^3 \bmod 4 = 343 \bmod 4 = 3 = 27 \bmod 4 = 3^3 \bmod 4 = (7 \bmod 4)^3 \bmod 4 = 7^3 \bmod 4$
4. (a) $\ldots 34 \bmod 4 = \ldots \cdot 100 + 34 \bmod 4 = 0 + 2 \bmod 4 = 2$
   (b) Eine Zahl ist durch 4 teilbar, wenn ihre letzten beiden Ziffern durch 4 teilbar sind. Da 100 durch 4 teilbar ist, ändert eine Addition eines Vielfachen von Hundert zu einer Zahl nicht ihre Teilbarkeitseigenschaft beim Dividieren durch 4.
5. Der Termin beim Zahnarzt ist Freitag, 12 Uhr; der Computerkurs beginnt Samstag, 8 Uhr.

Arbeitsblatt: Restklassen (I)

Wenn wir alle ganzen Zahlen im Hinblick auf ihre Teilbarkeit durch z.B. die Zahl 6 untersuchen, können wir die ganzen Zahlen in 6 Teilmengen unterteilen, je nachdem, welcher (positive) Rest r bei der Division durch 6 übrig bleibt. Wir bezeichnen diese Teilmengen mit $[r]_6$ und nennen sie die Restklassen modulo 6. So ist beispielsweise

$$[0]_6 = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$$

die Restklasse 0 modulo 6, die alle ganzen Zahlen enthält, die durch 6 teilbar sind, und

$$[2]_6 = \{\ldots, -10, -4, 2, 8, 14 \ldots\}$$

ist die Restklasse 2 modulo 6, die alle ganzen Zahlen enthält, die bei Division durch 6 den *positiven* Rest 2 haben. So ist etwa

$$8 : 6 = 1 \text{ Rest } 2$$

und

$$-10 : 6 = -2 \text{ Rest } 2, \text{ denn } -10 = -2 \cdot 6 + 2 \ .$$

In der folgenen Tabelle sind die Restklassen modulo 6 nochmals zusammengefasst:

$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$6 \cdot k$	$6 \cdot k + 1$	$6 \cdot k + 2$	$6 \cdot k + 3$	$6 \cdot k + 4$	$6 \cdot k + 5$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
-12	-11	-10	-9	-8	-7
-6	-5	-4	-3	-2	-1
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Verdeutlichung der dritten Spalte dieser Tabelle:

$$\begin{aligned} -10 &= -2 \cdot 6 + 2 \\ -4 &= -1 \cdot 6 + 2 \\ 2 &= 0 \cdot 6 + 2 \\ 8 &= 1 \cdot 6 + 2 \\ 14 &= 2 \cdot 6 + 2 \end{aligned}$$

Man kann entsprechend natürlich auch andere Zahlen als die 6 nehmen und kommt dann zur allgemeinen Definition von Restklassen modulo einer natürlichen Zahl m:

Definition: Die *Restklasse* einer ganzen Zahl a modulo einer Zahl m ist die Menge all der Zahlen, die bei Division durch m denselben (*positiven*) Rest lassen wie a. Die Restklasse von a modulo m bezeichnet man als $[a]_m$, und es gilt

$$[a]_m = \{b \in \mathbb{Z} | \text{ es gibt ein } k \in \mathbb{Z} \text{ mit } b = k \cdot m + a\} \ .$$

Man kann die ganzen Zahlen also in Restklassen einteilen. Jede Zahl, die zu einer Restklasse gehört, heißt auch Repräsentant der Restklasse.

Aufgaben:

1. (a) Versuche die obige Tabelle in Worte zu fassen.
   (b) Fertige eine entsprechende Tabelle für $m = 5$ an.
   (c) Bestimme $[0]_3$, $[1]_3$ und $[1]_4$.
   (d) Gib drei verschiedene Repräsentanten der Restklassen $[3]_7$ und $[2]_8$ an.
   (e) Kennst Du Anwendungen von Restklassen im täglichen Leben?

Arbeitsblatt: Restklassen (I) Infos für Lehrkräfte:

Dieses Arbeitsblatt dient dazu, den Begriff der Restklassen einzuführen und die Schüler/-innen hiermit vertraut zu machen.

Lösungen der Aufgaben:

1. (a) Die erste Spalte der Tabelle enthält die Elemente von $[0]_6$, d.h. alle ganzen Zahlen, die durch 6 teilbar sind bzw. die sich in der Form $6 \cdot k$ mit $k \in \mathbb{Z}$ schreiben lassen.
   Die zweite (dritte,..., sechste) Spalte der Tabelle enthält die Elemente von $[1]_6$ ($[2]_6$, $[3]_6$, $[4]_6$, $[5]_6$), d.h. alle ganzen Zahlen, die bei Division durch 6 den Rest 1 (2, 3, 4, 5) ergeben bzw. die sich in der Form $6 \cdot k + 1$ ($6 \cdot k + 2, \ldots, 6 \cdot k + 5$) schreiben lassen.

   (b)

$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$5 \cdot k$	$5 \cdot k + 1$	$5 \cdot k + 2$	$5 \cdot k + 3$	$5 \cdot k + 4$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

   (c) $[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$
   $[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
   $[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

   (d) Die Lösungen sind nicht eindeutig.
   -4, 3 und 10 sind drei Repräsentanten von $[3]_7 = \{\ldots, -11, -4, 3, 10, 17 \ldots\}$
   -14, 2 und 18 sind drei Repäsentanten von $[2]_8 = \{\ldots, -14, -6, 2, 10, 18 \ldots\}$

   (e) Uhrzeit (Rechnen modulo 12 bzw. modulo 24), schriftliches Dividieren (Rechnen modulo 10), Caesar-Code (Rechnen modulo 26), Euro und Cent (Rechnen modulo 100), ...

Arbeitsblatt: Restklassen (II)

Definition: Die *Restklasse* einer ganzen Zahl a modulo einer Zahl m ist die Menge all der Zahlen, die bei Division durch m denselben (*positiven*) Rest lassen wie a. Die Restklasse von a modulo m bezeichnet man als $[a]_m$, und es gilt

$$[a]_m = \{b \in \mathbb{Z} | \text{ es gibt ein } k \in \mathbb{Z} \text{ mit } b = k \cdot m + a\} \quad .$$

Man kann die ganzen Zahlen also in Restklassen einteilen. Jede Zahl, die zu einer Restklasse gehört, heißt auch Repräsentant der Restklasse.

Beispiele: $[0]_6 = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$ und $[2]_6 = \{\ldots, -10, -4, 2, 8, 14 \ldots\}$

Man kann für Restklassen eine natürliche Addition und eine natürliche Multiplikation definieren. Dazu nimmt man jeweils einen Repräsentanten der zu addierenden/multiplizierenden Restklassen, addiert bzw. multipliziert diese Repräsentanten und bestimmt, zu welcher Restklasse die Summe bzw. das Produkt gehören. Das Ergebnis ist tatsächlich unabhängig davon, welche Repräsentanten man ausgewählt hat.

Beispiel: Man will Produkt und Summe von $[4]_7$ und $[5]_7$ berechnen. Betrachten wir dazu einerseits die Repräsentanten 4 und 5, andererseits die Repräsentanten 11 und 12. Dann gilt

$4 + 5 = 9$, $\quad 9 \bmod 7 = 2$	$11 + 12 = 23$, $\quad 23 \bmod 7 = 2$
$4 \cdot 5 = 20$, $\quad 20 \bmod 7 = 6$	$11 \cdot 12 = 132$, $\quad 132 \bmod 7 = 6$

Auch für andere Wahlen von Repräsentanten kommen immer dieselben Ergebnisse heraus. Daher schreibt man auch

$$\begin{aligned} [4]_7 + [5]_7 &= [2]_7 \\ [4]_7 \cdot [5]_7 &= [6]_7 \end{aligned}$$

Aufgaben:

1. Zeige, dass für alle Repräsentanten $a \in [4]_7$ und $b \in [5]_7$ gilt: $a + b \in [2]_7$. Benutze dafür, dass sich a und b schreiben lassen als $a = 7 \cdot k_1 + 4$ und $b = 7 \cdot k_2 + 5$ mit ganzen Zahlen k_1 und k_2 und ermittle, welchen Rest $a + b$ bei Division durch 7 hat.

2. Zeige, dass für alle Repräsentanten $a \in [4]_7$ und $b \in [5]_7$ gilt: $a \cdot b \in [6]_7$. Benutze dafür, dass sich a und b schreiben lassen als $a = 7 \cdot k_1 + 4$ und $b = 7 \cdot k_2 + 5$ mit ganzen Zahlen k_1 und k_2 und ermittle, welchen Rest $a \cdot b$ bei Division durch 7 hat.

3. Leicht darstellen kann man Addition und Multiplikation von Restklassen mit Tabellen. Wenn aus dem Zusammenhang klar ist, welche Restklassen man betrachtet, kann man die Symbole $[\ ]_m$ auch weglassen.

   (a) Zeige, dass für die Restklassen modulo 3 folgende Additions- und Multiplikationstabelle gilt:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

   (b) Ermittle Additions- und Multiplikationstabelle für die Restklassen modulo 6.

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

·	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Arbeitsblatt: Restklassen (II)

Infos für Lehrkräfte:

Dieses Arbeitsblatt geht davon aus, dass der Begriff der Testklasse den Schüler/-innen bereits vertraut ist (z.B: durch das Arbeitsblatt Restklassen (I)).

Bei der letzten Aufgabe ist auch folgende Erweiterung denkbar: Die Schüler/-innen können bei der letzten Aufgabe auch in verschiedene Gruppen eingeteilt werden, die Multiplikationstabellen für Restklassen modulo unterschiedlicher Zahlen m aufstellen. Dann kann man den Begriff des multiplikativen Inversen einführen und anhand der Multiplikationstabellen untersuchen, unter welchen Voraussetzungen ein solches existiert (wenn m eine Primzahl ist, oder, allgemeiner, wenn m und der Repräsentant teilerfremd sind).

Lösungen der Aufgaben:

1. Für alle Repräsentanten $a \in [4]_7$ und $b \in [5]_7$ gibt es $k_1 \in \mathbb{Z}$ und $k_2 \in \mathbb{Z}$, so dass

$$\begin{aligned} a &= k_1 \cdot 7 + 4 \\ b &= k_2 \cdot 7 + 5 \end{aligned}$$

   Damit gilt

$$a + b = k_1 \cdot 7 + 4 + k_2 \cdot 7 + 5 = (k_1 + k_2) \cdot 7 + 9 = (k_1 + k_2 + 1) \cdot 7 + 2 \in [2]_7$$

2. Man geht analog wie bei der vorigen Aufgabe vor und erhält

$$\begin{aligned} a \cdot b &= (k_1 \cdot 7 + 4) \cdot (k_2 \cdot 7 + 5) \\ &= (k_1 \cdot k_2 \cdot 7 + k_1 + k_2) \cdot 7 + 4 \cdot 5 \\ &= (k_1 \cdot k_2 \cdot 7 + k_1 + k_2) \cdot 7 + 20 \\ &= (k_1 \cdot k_2 \cdot 7 + k_1 + k_2) \cdot 7 + 2 \cdot 7 + 6 \\ &= (k_1 \cdot k_2 \cdot 7 + k_1 + k_2 + 2) \cdot 7 + 6 \\ &\in [6]_7 \end{aligned}$$

3. (a)

$$
\begin{array}{rlcl}
0+0=0\ , & 0 \bmod 3 = 0 & \Longrightarrow & [0]_3 + [0]_3 = [0]_3 \\
0+1=1\ , & 1 \bmod 3 = 1 & \Longrightarrow & [0]_3 + [1]_3 = [1]_3 \\
0+2=2\ , & 2 \bmod 3 = 2 & \Longrightarrow & [0]_3 + [2]_3 = [2]_3 \\
1+0=1\ , & 1 \bmod 3 = 1 & \Longrightarrow & [1]_3 + [0]_3 = [1]_3 \\
1+1=2\ , & 2 \bmod 3 = 2 & \Longrightarrow & [1]_3 + [1]_3 = [2]_3 \\
1+2=3\ , & 3 \bmod 3 = 0 & \Longrightarrow & [1]_3 + [2]_3 = [0]_3 \\
2+0=2\ , & 2 \bmod 3 = 2 & \Longrightarrow & [2]_3 + [0]_3 = [2]_3 \\
2+1=3\ , & 3 \bmod 3 = 0 & \Longrightarrow & [2]_3 + [1]_3 = [0]_3 \\
2+2=4\ , & 4 \bmod 3 = 1 & \Longrightarrow & [2]_3 + [2]_3 = [1]_3 \\
0\cdot 0=0\ , & 0 \bmod 3 = 0 & \Longrightarrow & [0]_3 \cdot [0]_3 = [0]_3 \\
0\cdot 1=0\ , & 0 \bmod 3 = 0 & \Longrightarrow & [0]_3 \cdot [1]_3 = [0]_3 \\
0\cdot 2=0\ , & 0 \bmod 3 = 0 & \Longrightarrow & [0]_3 \cdot [2]_3 = [0]_3 \\
1\cdot 0=0\ , & 0 \bmod 3 = 0 & \Longrightarrow & [1]_3 \cdot [0]_3 = [0]_3 \\
1\cdot 1=1\ , & 1 \bmod 3 = 1 & \Longrightarrow & [1]_3 \cdot [1]_3 = [1]_3 \\
1\cdot 2=2\ , & 2 \bmod 3 = 2 & \Longrightarrow & [1]_3 \cdot [2]_3 = [2]_3 \\
2\cdot 0=0\ , & 0 \bmod 3 = 0 & \Longrightarrow & [2]_3 \cdot [0]_3 = [0]_3 \\
2\cdot 1=2\ , & 2 \bmod 3 = 2 & \Longrightarrow & [2]_3 \cdot [1]_3 = [2]_3 \\
2\cdot 2=4\ , & 4 \bmod 3 = 1 & \Longrightarrow & [2]_3 \cdot [2]_3 = [1]_3
\end{array}
$$

(b)

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Arbeitsblatt: Modulares Potenzieren

Für das Modulo-Rechnen gelten u.a. die folgenden Rechenregeln:

$$\begin{aligned}(a \cdot b) \bmod m &= (a \bmod m \cdot b \bmod m) \bmod m \\ (a^b) \bmod m &= (a \bmod m)^b \bmod m\end{aligned}$$

Aufgaben:

1. Versuche in Worte zu fassen, welche Ansätze bei den folgenden Rechenbeispielen verwendet werden, um $7^4 \bmod 12$ und $82^{17} \bmod 20$ zu berechnen.

$$\begin{aligned}7^4 \bmod 12 &= 7^2 \cdot 7^2 \bmod 12 \\ &= 49 \cdot 49 \bmod 12 \\ &= (49 \bmod 12 \cdot 49 \bmod 12) \bmod 12 \\ &= (1 \cdot 1) \bmod 12 \\ &= 1 \bmod 12 \\ &= 1\end{aligned}$$

$$\begin{aligned}82^{17} \bmod 20 &= 2^{17} \bmod 20 \\ &= 2^{16} \cdot 2^1 \bmod 20 = (2^4)^4 \cdot 2 \bmod 20 \\ &= 16^4 \cdot 2 \bmod 20 = (-4)^4 \cdot 2 \bmod 20 \\ &= (-4)^2 \cdot (-4)^2 \cdot 2 \bmod 20 \\ &= 16^2 \cdot 2 \bmod 20 \\ &= (-4)^2 \cdot 2 \bmod 20 = 16 \cdot 2 \bmod 20 \\ &= 32 \bmod 20 \\ &= 12\end{aligned}$$

2. Berechne

   (a) $8^9 \bmod 7$

   (b) $6^9 \bmod 7$

   (c) $54^{16} \bmod 55$

   (d) $3^{333} \bmod 26$ (Tip: Benutze $3^3 \bmod 26 = 27 \bmod 26 = 1 \bmod 26 = 1$)

   (e) $2^{268} \bmod 17$ (Tip: Benutze $2^4 \bmod 17 = 16 \bmod 17 = (-1) \bmod 17$)

   (f) $2^{269} \bmod 17$ (Tip: Verwende das Ergebnis von (e) oder benutze, dass $2^4 \bmod 17 = 16 \bmod 17 = (-1) \bmod 17$)

   (g) $2^{270} \bmod 19$ (Tip: Benutze, dass $2^9 \bmod 19 = -1 \bmod 19$.)

   (h) $2^{271} \bmod 19$ (Tip: Verwende das Ergebnis von (g) oder benutze, dass $2^9 \bmod 19 = -1 \bmod 19$.

   (i) $3^{333} \bmod 15$
   Tip: Zeige zunächst, dass $3^4 \bmod 15 = 6 \bmod 15$, und nutze außerdem, dass $6^k \bmod 15 = 6$ ist.

Arbeitsblatt: Modulares Potenzieren

Infos für Lehrkräfte: Viele der Aufgaben erfordern ein sicheres Beherrschen der Potenzregeln und gute Fähigkeiten im Kopfrechnen. Gegebenenfalls sollten die Potenzregeln vorab noch einmal wiederholt werden.

Beim modularen Potenzieren mit (Taschen-)Rechnern muss ggf. darauf geachtet werden, dass kein Overflow auftritt.

Lösungen der Aufgaben:

1. Beim *ersten Beispiel* benutzt man im ersten Ansatz, dass $7^2 \bmod 12 = 49 \bmod 12 = 1$. Daraus folgt sofort und ohne größeren Rechenaufwand:

   $$7^4 \bmod 12 = (7^2 \bmod 12)^2 \bmod 12 = 1^2 \bmod 12 = 1 \ .$$

   Beim *zweiten Beispiel* wird deutlich, dass das modulare Potenzieren leichter werden kann, wenn es möglich ist, zu *kleinen* negativen Zahlen überzugehen:

   $$16^4 \bmod 20 = (-4)^4 \bmod 20 = 16^2 \bmod 20 = (-4)^2 \bmod 20 = 16$$

2. (a) $8^9 \bmod 7 = (8 \bmod 7)^9 \bmod 7 = 1^9 \bmod 7 = 1 \bmod 7 = 1$

   (b)

   $$\begin{aligned} 6^9 \bmod 7 &= (6 \bmod 7)^9 \bmod 7 = (-1 \bmod 7)^9 \bmod 7 \\ &= (-1)^9 \bmod 7 = -1 \bmod 7 = 6 \end{aligned}$$

   (c) $54^{16} \bmod 55 = (-1)^{16} \bmod 55 = 1 \bmod 55 = 1$

   (d) $3^{333} \bmod 26 = 3^{3 \cdot 111} \bmod 26 = (3^3)^{111} \bmod 26 = 1^{111} \bmod 26 = 1 \bmod 26 = 1$

   (e) $2^{268} \bmod 17 = 2^{4 \cdot 67} \bmod 17 = (2^4)^{67} \bmod 17 = (-1)^{67} \bmod 17$
   $= -1 \bmod 17 = 16$

   (f) $2^{269} \bmod 17 = 2 \cdot (2^4)^{67} \bmod 17 = 2 \cdot (-1)^{67} \bmod 17 = -2 \bmod 17 = 15$

   (g) Es gilt $2^9 \bmod 19 = 512 \bmod 19 = 18 \bmod 19 = -1 \bmod 19$. Damit folgt

   $$\begin{aligned} 2^{270} \bmod 19 &= 2^{9 \cdot 30} \bmod 19 \\ &= (2^9)^{30} \bmod 19 \\ &= (-1)^{30} \bmod 19 \\ &= 1 \end{aligned}$$

   (h) Es gilt $2^9 \bmod 19 = 512 \bmod 19 = 18 \bmod 19 = -1 \bmod 19$. Damit folgt

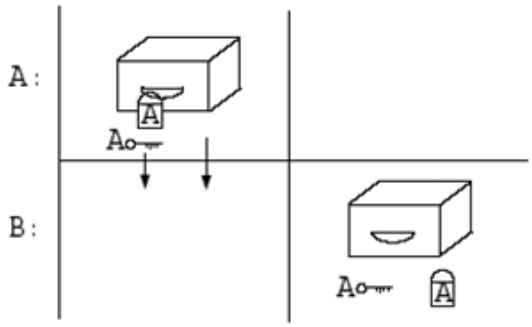
   $$\begin{aligned} 2^{271} \bmod 19 &= 2 \cdot 2^{9 \cdot 30} \bmod 19 \\ &= 2 \cdot (2^9)^{30} \bmod 19 \\ &= 2 \cdot (-1)^{30} \bmod 19 \\ &= 2 \cdot 1 \bmod 19 \\ &= 2 \bmod 19 \\ &= 2 \end{aligned}$$

(i) Es gilt: $3^4 \bmod 15 = 81 \bmod 15 = 6$ sowie $6 \cdot 6 \bmod 15 = 36 \bmod 15 = 6$, woraus $6^k \bmod 15 = 6$ per vollständiger Induktion folgt. Damit gilt:

$$\begin{aligned} 3^{333} \bmod 15 &= 3 \cdot 3^{4 \cdot 83} \bmod 15 \\ &= 3 \cdot 81^{83} \bmod 15 \\ &= 3 \cdot 6^{83} \bmod 15 \\ &= 3 \cdot 6 \bmod 15 \\ &= 18 \bmod 15 \\ &= 3 \end{aligned}$$

Arbeitsblatt: Symmetrische und asymmetrische Verschlüsselung

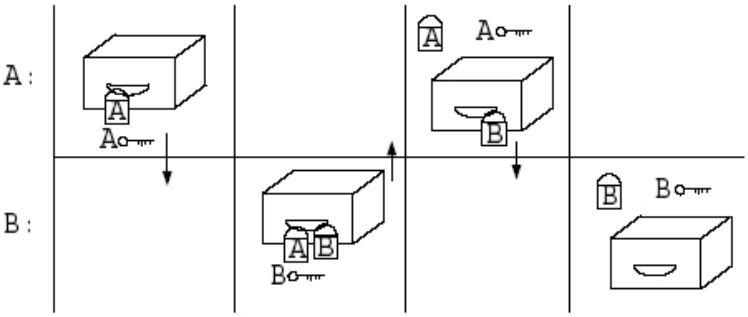
Klassische Kryptographie – symmetrische Verschlüsselung



Aufgabe 1: Was ist der Nachteil an dieser Methode?

Paradoxon: Will man ein Geheimnis austauschen, muss man schon vorher ein Geheimnis ausgetauscht haben.

70er Jahre: neue Idee nach Whitfield Diffie & Martin Hellman asymmetrische Verschlüsselung:



Aufgabe 2: Fasse die Schritte in Worte!

1. _____
2. _____
3. _____
   _____
4. _____

Problem: In der Kryptographie nimmt man an, dass das *Ver*-schlüsselungsverfahren nicht geheim gehalten werden kann, somit bietet nur ein einziger Schlüssel zum Ver- und Entschlüsseln keine Sicherheit.

Lösungen: Man verwendet asymmetrische Verschlüsselungen. Wenn der Schlüssel zum Verschlüsseln jedem zugänglich gemacht wird, also ein öffentlicher Schlüssel ist, befinden wir uns in der Public Key Kryptographie.

Wichtig hierbei ist: Aus dem Wissen über den Schlüssel für die Verschlüsselung darf man nichts über das Verfahren der Entschlüsselung herausbekommen!

Arbeitsblatt: Symmetrische und asymmetrische Verschlüsselung

Lösungen der Aufgaben:

Aufgabe 1: Um die verschlüsselte Nachricht zu übermitteln, muss auch der Schlüssel ausgetauscht werden. Jeder, der den Schlüssel abfängt, kann auch die Nachricht entschlüsseln. man müsste also auch den Schlüssel *sicher*, d.h. verschlüsselt übermitteln. Hierfür bräuchte man aber wieder einen Schlüssel, der sicher ausgetauscht werden müsste, usw.

Aufgabe 2:

1. A verschlüsselt seine Nachricht mit seinem Schlüssel und versendet die Nachricht (ohne Schlüssel) an B
2. B verschlüsselt die Nachricht mit seinem eigenen Schlüssel und sendet die doppelt verschlüsselte Nachricht zurück an A.
3. A wendet seinen Schlüssel auf die doppelt verschlüsselte Nachricht an, entfernt so seine Verschlüsselung und sendet die jetzt nur noch mit dem Schlüssel von B verschlüsselte Nachricht zurück an B.
4. B entschlüsselt die Nachricht mit seinem Schlüssel und kann den Inhalt lesen.

Arbeitsblatt: Einwegfunktionen

Als *Einwegfunktion* bezeichnet man eine Abbildung f von einer Menge X in eine Menge Y, für die $f(x)$ für jedes Element von x leicht zu berechnen ist, während es für (fast) jedes $y \in Y$ extrem schwer ist, ein Urbild x (d.h. ein $x \in X$ mit $f(x) = y$) zu finden.

Aufgaben:

1. Inwiefern entspricht das Telefonbuch einer Einwegfunktion?

2. Beschreibe, inwiefern die folgenden Vorgänge Einwegfunktionen entsprechen:
   (a) Erbsen und Linsen mischen
   (b) Farben mischen
   (c) Geld ausgeben
   (d) Sand und Kies mischen

3. Eine spezielle Variante von Einwegfunktionen sind die *Trapdoor-Einwegfunktionen* (trapdoor = Geheimtür), die sich nur dann einfach lösen lassen, wenn man eine (geheime) Zusatzinformation besitzt. Erkläre, inwiefern ein Briefkasten als Bild für eine Trapdoor-Einwegfunktion angesehen werden kann.

Mathematische Beispiele für Einwegfunktionen:

- Die Multiplikation zweier (großer) Primzahlen ist einfach, während die Umkehrung (d.h. die Primfaktorzerlegung) schwer (aufwändig) ist.

- Quadrieren modulo n, wobei n das Produkt zweier großer Primzahlen p und q ist.

Arbeitsblatt: Einwegfunktionen

Information für Lehrkräfte:

Auf diesem Arbeitsblatt wird der Abbildungsbegriff benutzt. Gegebenenfalls müsste dieser im Unterricht vorher noch einmal verdeutlicht werden.

Lösungen der Aufgaben:

1. Das Telefonbuch entspricht einer Einwegfunktion, weil es mit ihm sehr leicht möglich ist, aus Namen und Wohnort die Telefonnummer herauszufinden. Um aus einer gegebenen Telefonnummer aber zurück auf Namen und Wohnort des Besitzers der Nummer schließen zu können, müsste man große Teile des Telefonbuches durchsuchen, was sehr zeitaufwändig ist.

   Bei elektronischen Telefonbüchern mit Suchfunktion erledigt diese Arbeit der Computer, d.h. elektronische Telefonbücher sind *keine* Beispiele für Einwegfunktionen.

2. (a) Erbsen und Linsen mischen: Dies ist eine Einwegfunktion, weil das Auseinandersortieren von Erbsen und Linsen schwierig und zeitaufwändig ist.

   (b) Farben mischen: Dies ist eine Einwegfunktion, weil das Entmischen von Farben nur sehr schwierig möglich ist.

   (c) Geld ausgeben: Auch dies könnte man als Einwegfunktion bezeichnen, denn Geld auszugeben ist sehr viel einfacher als Geld zu verdienen.

   (d) Sand und Kies mischen: Dies ist eine Einwegfunktion, wenn man nicht über ein feines Sieb verfügt, mit dem man Sand und Kies wieder leicht entmischen könnte.

   (e) eine Zahl mit 7 multiplizieren: Dies ist keine Einwegfunktion; durch einfache Division kommt man leicht auf die ursprüngliche Zahl zurück.

3. Ein Briefkasten lässt sich leicht leeren, wenn man den zugehörigen Schlüssel besitzt. Der Schlüssel entspricht der *Trapdoor*. Wer keinen Schlüssel für den Briefkasten hat, kommt nicht einfach an den Inhalt heran.

Memo: RSA auf einen Blick

Alice | **Kommunikation zwischen Alice und Bob** | **Bob**

Alice wählt zwei verschiedene Primzahlen p und q, z.B. $p = 5$ und $q = 11$. Alice berechnet

$$n = pq = 55$$

sowie

$$m = (q-1)(p-1) = 40 \ .$$

Alice wählt eine Zahl a, die zu m teilerfremd ist, z.B.

$$a = 7 \ .$$

Alice gibt die Zahlen n und a als ihren öffentlichen Schlüssel bekannt:

$$\begin{aligned} n &= 55 \\ a &= 7 \end{aligned}$$

Bobs Nachricht ist eine Zahl x, die kleiner als n ist, z.B. $x = 8$. Bob verschlüsselt sie gemäß

$$\begin{aligned} y &= x^a \bmod n \\ &= 8^7 \bmod 55 = 2 \end{aligned}$$

Bob sendet y an Alice:

$$y = 2 \ .$$

Alice berechnet aus a und m das multiplikative Inverse von a modulo m:

$$\begin{aligned} b &= a^{-1} \bmod m \\ &= 7^{-1} \bmod 40 = 23 \ . \end{aligned}$$

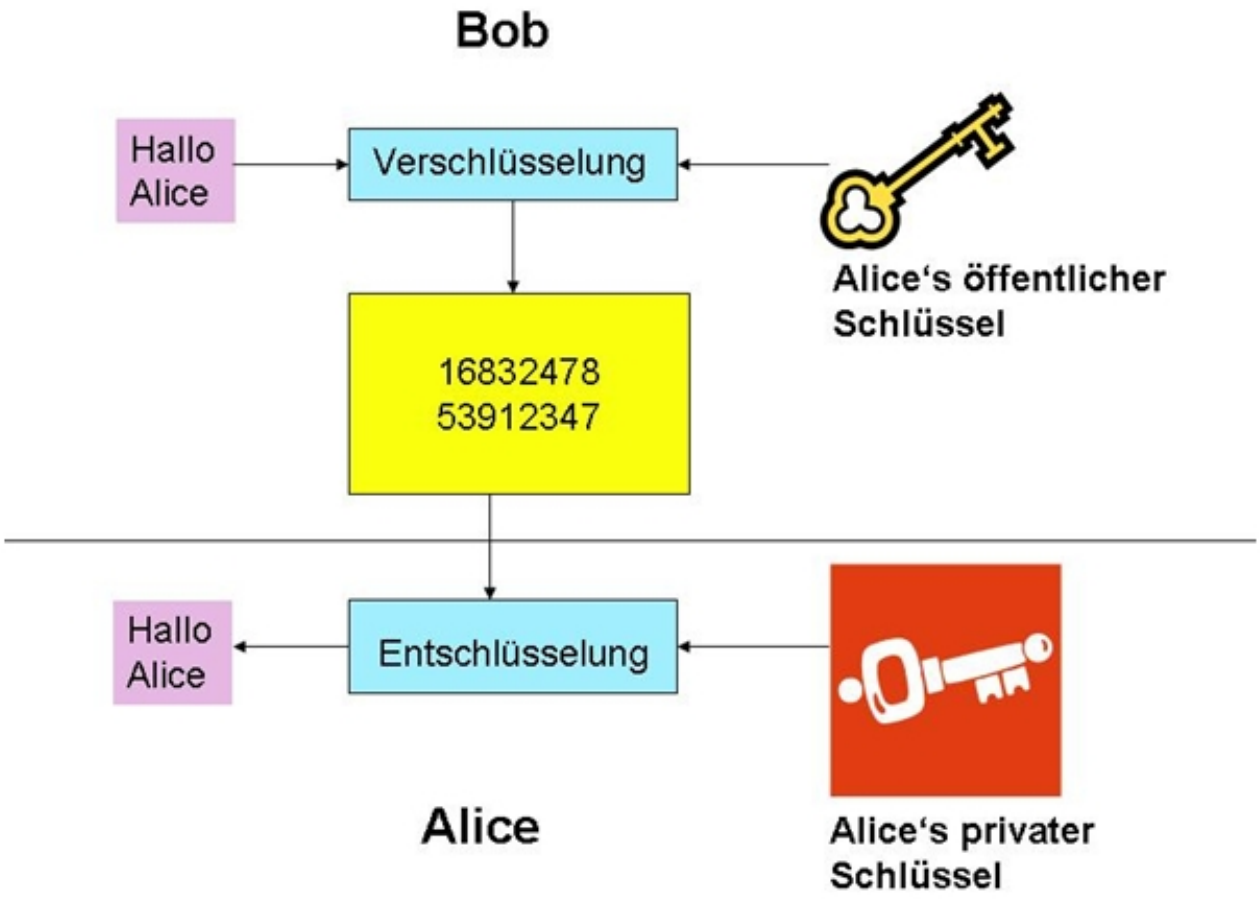
Sie kann Bobs Nachricht mit der Formel

$$x = y^b \bmod n = 2^{23} \bmod 55 = 8$$

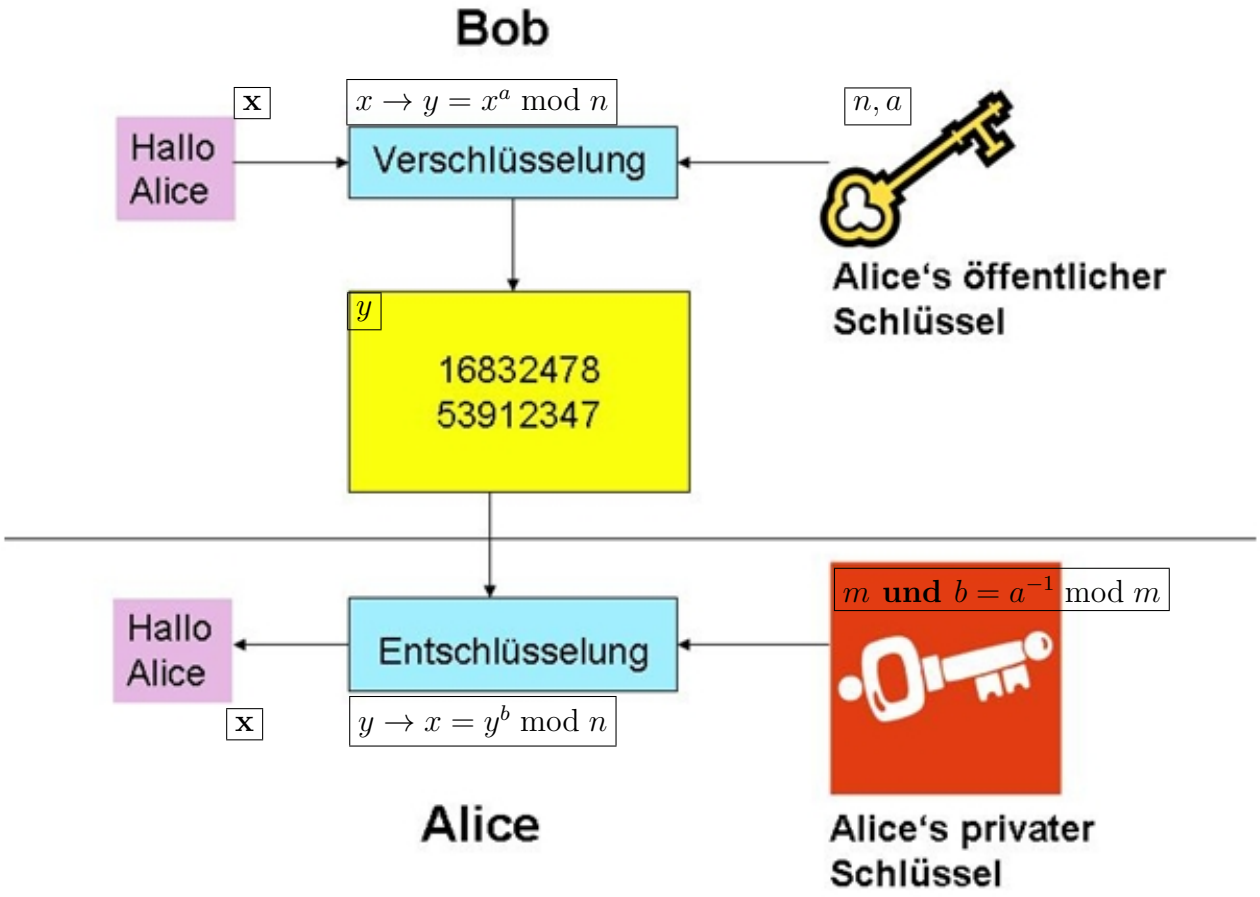
wieder entschlüsseln.

Arbeitsblatt: RSA-Verfahren

Beschrifte das folgende Schaubild mit den Variablen, die im Memo *RSA auf einen Blick* verwendet wurden.



Arbeitsblatt: RSA-Verfahren



Arbeitsblatt: Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen

Es gibt verschiedene Möglichkeiten, um den größten gemeinsamen Teiler zweier Zahlen a und b, im folgenden kurz als $\mathrm{ggT}(a,b)$ bezeichnet, zu bestimmen. Man kann dies beispielsweise über eine Primfaktorzerlegung der beiden Zahlen und anschließenden Abgleich der gemeinsamen Primfaktoren vornehmen oder auch mit dem Euklidischen Algorithmus. Ist von keiner der beiden Zahlen die Primfaktorzerlegung bekannt, so ist der Euklidische Algorithmus das schnellste Verfahren zur Bestimmung des ggT.

Nehmen wir beispielsweise an, wir wollen $\mathrm{ggT}(8,5)$ bestimmen. Es gilt

$$8 : 5 = 1 \text{ Rest } 3 \ .$$

Basis des Euklidischen Algorithmus ist jetzt, dass ggT(8,5)=ggT(5,3) gilt, d.h. anstatt den ggT der beiden ursprünglichen Zahlen 8 und 5 zu ermitteln, reicht es aus, den ggT aus der kleineren dieser beiden Zahlen (hier 5) und dem Rest (hier 3), der entsteht, wenn wir die gegebenen beiden Zahlen durcheinander dividieren, zu bestimmen. (Dies gilt allgemein; wir verzichten hier jedoch auf einen Beweis.) Dieser Ansatz kann mehrfach angewendet werden:

$$5 : 3 = 1 \text{ Rest } 2 \qquad \Longrightarrow \qquad \mathrm{ggT}(5,3) = \mathrm{ggT}(3,2)$$

sowie

$$3 : 2 = 1 \text{ Rest } 1 \qquad \Longrightarrow \qquad \mathrm{ggT}(3,2) = \mathrm{ggT}(2,1)$$

und schließlich

$$2 : 1 = 2 \text{ Rest } 0 \ .$$

Der letzte von 0 verschiedene Rest ist dann der ggT der beiden ursprünglichen Zahlen. Es gilt somit: ggT(8,5)=ggT(5,3)=ggT(3,2)=ggT(2,1)=1 .

Ein weiteres Beispiel für den Euklidischen Algorithmus:
Zu bestimmen sei ggT(120,72). Es gilt

$$\begin{aligned} 120 : 72 = 1 \text{ Rest } 48 \qquad &\Longrightarrow \qquad \mathrm{ggT}(120,72) = \mathrm{ggT}(72,48) \\ 72 : 48 = 1 \text{ Rest } 24 \qquad &\Longrightarrow \qquad \mathrm{ggT}(72,48) = \mathrm{ggT}(48,24) \\ 48 : 24 = 2 \text{ Rest } 0 \qquad &\Longrightarrow \qquad \mathrm{ggT}(48,24) = 24 \ . \end{aligned}$$

Wir haben also

$$\mathrm{ggT}(120,72) = \mathrm{ggT}(72,48) = \mathrm{ggT}(48,24) = 24 \ .$$

Aufgabe 1: Bestimme mit dem Euklidischen Algorithmus den ggT von
a) 24 und 9
b) 36 und 18
c) 75 und 45
d) 720 und 288
e) 1071 und 1029

Arbeitsblatt: Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen

Lösungen der Aufgaben:

1. (a)

$$\begin{aligned} 24 : 9 = 2 \text{ Rest } 6 \quad &\Longrightarrow \quad \text{ggT}(24,9) = \text{ggT}(9,6) \\ 9 : 6 = 1 \text{ Rest } 3 \quad &\Longrightarrow \quad \text{ggT}(9,6) = \text{ggT}(6,3) \\ 6 : 3 = 2 \text{ Rest } 0 \quad &\Longrightarrow \quad \text{ggT}(6,3) = 3 \ . \end{aligned}$$

Also: ggT(24,9)=ggT(9,6)=ggT(6,3)=3

(b)

$$36 : 18 = 2 \text{ Rest } 0 \quad \Longrightarrow \quad \text{ggT}(36,18) = 18$$

(c)

$$\begin{aligned} 75 : 45 = 1 \text{ Rest } 30 \quad &\Longrightarrow \quad \text{ggT}(75,45) = \text{ggT}(45,30) \\ 45 : 30 = 1 \text{ Rest } 15 \quad &\Longrightarrow \quad \text{ggT}(45,30) = \text{ggT}(30,15) \\ 30 : 15 = 2 \text{ Rest } 0 \quad &\Longrightarrow \quad \text{ggT}(30,15) = 15 \ . \end{aligned}$$

Also: ggT(75,45)=ggT(45,30)=ggT(30,15)=15

(d)

$$\begin{aligned} 720 : 288 = 2 \text{ Rest } 144 \quad &\Longrightarrow \quad \text{ggT}(720,288) = \text{ggT}(288,144) \\ 288 : 144 = 2 \text{ Rest } 0 \quad &\Longrightarrow \quad \text{ggT}(288,144) = 144 \ . \end{aligned}$$

Also: ggT(720,288)=ggT(288,144)=144

(e)

$$\begin{aligned} 1071 : 1029 = 1 \text{ Rest } 42 \quad &\Longrightarrow \quad \text{ggT}(1071,1029) = \text{ggT}(1029,42) \\ 1029 : 42 = 24 \text{ Rest } 21 \quad &\Longrightarrow \quad \text{ggT}(1029,42) = \text{ggT}(42,21) \\ 42 : 21 = 2 \text{ Rest } 0 \quad &\Longrightarrow \quad \text{ggT}(42,21) = 21 \ . \end{aligned}$$

Also: ggT(1071,1029)=ggT(1029,42)=ggT(42,21)=21

Arbeitsblatt: Multiplikatives Inverses modulo einer Zahl m

Dieses Arbeitsblatt beschreibt, wie man die multiplikative Inverse berechnet. Arbeitet die Schritte sorgsam durch und beantwortet die Fragen.

Definition: Sind a und m zwei *teilerfremde* positive ganze Zahlen, so ist die multiplikative Inverse b zu a modulo m die eindeutig bestimmte positive Zahl $b < m$, welche die Gleichung

$$(b \cdot a) \bmod m = 1$$

erfüllt. Diese Gleichung können wir auch schreiben als

$$1 = k \cdot m + b \cdot a \qquad \text{mit } k \in \mathbb{Z}. \tag{1}$$

Suche das multiplikative Inverse durch Ausprobieren: Sei $a = 13$ und $m = 16$. Wir suchen eine Zahl b, so dass $(13 \cdot b) \bmod 16 = 1$ ist.

$$\begin{aligned} 13 \cdot 2 \bmod 16 &= 10 \\ 13 \cdot 3 \bmod 16 &= 7 \\ 13 \cdot 4 \bmod 16 &= 4 \\ 13 \cdot 5 \bmod 16 &= 1 \end{aligned}$$

Wenn a und m größer werden ...: Ausprobieren führt nur bei kleinen Zahlen zum Ziel, bei großen Zahlen kann der Rechenaufwand riesig werden.

Mache dir folgendes klar: Wenn es uns gelingt, die Zahl 1 als Linearkombination der Zahlen a und m zu schreiben, d.h. wenn wir eine Darstellung der Form (1) finden, ist $b \bmod m$ gerade die gesuchte multiplikative Inverse.

Um eine solche Darstellung zu finden, verwenden wir den Euklidischen Algorithmus, der folgendermaßen abläuft: Wir starten mit den beiden Gleichungen

$$\begin{aligned} &\text{(I)} && \boxed{16} &&= \boxed{1} \cdot 16 + \boxed{0} \cdot 13 \\ &\text{(II)} && \boxed{13} &&= \boxed{0} \cdot 16 + \boxed{1} \cdot 13 \end{aligned}$$

Da die 13 nur *einmal* in die 16 passt, berechnen wir Gleichung (III) als

$$\text{(III)} = \text{(I)} - 1 \cdot \text{(II)}$$

und erhalten

$$\text{(III)} \qquad \boxed{3} = \boxed{1} \cdot 16 + \boxed{-1} \cdot 13 \ .$$

Die 3 (linke Seite von Gleichung (III)) passt *viermal* in die 13 (linke Seite von Gleichung (II)). Daher berechnen wir Gleichung (IV) als

$$\text{(IV)} = \text{(II)} - 4 \cdot \text{(III)}$$

und erhalten

$$\text{(IV)} \qquad \boxed{1} = \boxed{-4} \cdot 16 + \boxed{5} \cdot 13 \ .$$

Auf der linken Seite von Gleichung (IV) ist jetzt eine $\boxed{1}$ erzeugt worden. Damit haben wir die multiplikative Inverse modulo 16 zu 13 gefunden. Es ist die Zahl, die auf der rechten Seite als Faktor bei der 13 steht, modulo 16, also $5 \bmod 16 = 5$. Dies können wir leicht überprüfen und finden in der Tat $5 \cdot 13 \bmod 16 = 65 \bmod 16 = 1$.

Ein zweites Beispiel: Als zweites Beispiel betrachten wir jetzt $a = 13$ und $m = 160$. Wir suchen also wieder eine positive Zahl $b < 160$, so dass $(13 \cdot b) \bmod 160 = 1$ gilt. Dazu gehen wir genauso vor wie im ersten Beispiel, verwenden aber ein etwas kürzeres Schema. In der Spalte Erläuterung sind die Gleichungen nochmals ausgeschrieben; die Spalte Koeffizienten enthält nur die Koeffizienten dieser Gleichungen, die aber ausreichen, wenn wir das Verfahren erst einmal gut kennen.

Gleichung	Koeffizienten			Erläuterung
(I)	160	1	0	Dies steht für $\boxed{160} = \boxed{1} \cdot 160 + \boxed{0} \cdot 13$
(II)	13	0	1	Dies steht für $\boxed{13} = \boxed{0} \cdot 160 + \boxed{1} \cdot 13$
				Wie oft geht 13 in 160? 12 mal; also (III) = (I) $- 12 \cdot$ (II)
(III)	4	1	-12	Dies steht für $\boxed{4} = \boxed{1} \cdot 160 + \boxed{\text{-12}} \cdot 13$
				Wie oft geht 4 in 13? 3 mal; also (IV) = (II) $- 3 \cdot$ (III)
(IV):	$\boxed{1}$	-3	$\boxed{37}$	Dies steht für $\boxed{1} = \boxed{\text{-3}} \cdot 160 + \boxed{37} \cdot 13$

Das Verfahren hat jetzt in der ersten Spalte eine 1 erzeugt. Damit haben wir die multiplikative Inverse zu 13 mod 160 gefunden. Sie steht in der letzten Spalte des Verfahrens und lautet 37 mod 160 = 37. Manchmal dauert es auch einige Schritte länger, bis die 1 in der ersten Spalte entsteht.

Aufgaben:

1. Mache Dir klar, wie der oben beschriebene Algorithmus funktioniert.

2. Finde
   a) die multiplikative Inverse von 15 modulo 26
   b) die multiplikative Inverse von 5 modulo 48

Arbeitsblatt: Multiplikatives Inverses modulo einer Zahl m

Bemerkungen für Lehrkräfte: Das Arbeitsblatt besteht aus zwei Seiten. Es kann in Kleingruppen bearbeitet werden, damit sich die Schüler/-innen bei Verständnisproblemen gegenseitig helfen können.

Je nach Leistungsstärke und Homogenität in der Klasse mag es ratsam sein, das Vorgehen bei dem auf dem Arbeitsblatt beschriebenen Algorithmus noch einmal detailliert an der Tafel zu erläutern (oder von leistungsstarken Schüler/-innen erläutern zu lassen), bevor die Schüler/-innen sich mit Aufgabe 2 beschäftigen.

Lösungen der Aufgaben:

1. Je nach Leistungsstärke der Klasse mag es ratsam sein, das Vorgehen bei dem auf dem Arbeitsblatt beschriebenen Algorithmus noch einmal detailliert an der Tafel zu erläutern, bevor die Schüler/-innen sich mit Aufgabe 2 beschäftigen.

2. (a) Wir verwenden den auf dem Arbeitsblatt angegebenen Algorithmus, um das multiplikative Inverse von 15 modulo 26 zu ermitteln:

Gleichung	Koeffizienten			Erläuterung
(I)	26	1	0	Dies steht für $\boxed{26} = \boxed{1} \cdot 26 + \boxed{0} \cdot 15$
(II)	15	0	1	Dies steht für $\boxed{15} = \boxed{0} \cdot 26 + \boxed{1} \cdot 15$
				Wie oft geht 15 in 26? 1 mal; also (III) = (I) − (II)
(III)	11	1	−1	Dies steht für $\boxed{11} = \boxed{1} \cdot 26 + \boxed{-1} \cdot 15$
				Wie oft geht 11 in 15? 1 mal; also (IV) = (II) − (III)
(IV)	4	−1	2	Dies steht für $\boxed{4} = \boxed{-1} \cdot 26 + \boxed{2} \cdot 15$
				Wie oft geht 4 in 11? 2 mal; also (V) = (III) − 2 · (IV)
(V):	3	3	−5	Dies steht für $\boxed{3} = \boxed{3} \cdot 26 + \boxed{-5} \cdot 15$
				Wie oft geht 3 in 4? 1 mal; also (VI) = (IV) − (V)
(VI)	$\boxed{1}$	−4	$\boxed{7}$	Dies steht für $\boxed{1} = \boxed{-4} \cdot 26 + \boxed{7} \cdot 15$

Damit haben wir das multiplikative Inverse von 15 modulo 26 gefunden. Es ist $7 \bmod 26 = 7$.
Probe: $7 \cdot 15 \bmod 26 = 105 \bmod 26 = 4 \cdot 26 + 1 \bmod 26 = 1 \bmod 26 = 1$

(b) Wir verwenden den auf dem Arbeitsblatt angegebenen Algorithmus, um das multiplikative Inverse von 5 modulo 48 zu ermitteln:

Gleichung	Koeffizienten			Erläuterung
(I)	48	1	0	Dies steht für $\boxed{48} = \boxed{1} \cdot 48 + \boxed{0} \cdot 5$
(II)	5	0	1	Dies steht für $\boxed{5} = \boxed{0} \cdot 48 + \boxed{1} \cdot 5$
				Wie oft geht 5 in 48? 9 mal; also (III) = (I) − 9 · (II)
(III)	3	1	−9	Dies steht für $\boxed{3} = \boxed{1} \cdot 48 + \boxed{-9} \cdot 5$
				Wie oft geht 3 in 5? 1 mal; also (IV) = (II) − (III)
(IV)	2	−1	10	Dies steht für $\boxed{2} = \boxed{-1} \cdot 48 + \boxed{10} \cdot 5$
				Wie oft geht 2 in 3? 1 mal; also (V) = (III) − (IV)
(V):	$\boxed{1}$	2	$\boxed{-19}$	Dies steht für $\boxed{1} = \boxed{2} \cdot 48 + \boxed{-19} \cdot 5$

Damit haben wir die multiplikative Inverse von 5 modulo 48 gefunden. Es ist $-19 \bmod 48 = 29$.
Probe: $5 \cdot 29 \bmod 48 = 145 \bmod 48 = 3 \cdot 48 + 1 \bmod 48 = 1 \bmod 48 = 1$

Literatur

[1] A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter: *Moderne Verfahren der Kryptographie.* Vieweg, 2006.

[2] A. Beutelspacher: *Geheimsprachen.* Verlag C.H. Beck oHG, 4. Auflage 2005.

[3] http://www.idn.uni-bremen.de/pubs/Examensarbeit_Einhaus_2.pdf

[4] http://www.oemg.ac.at/DK/Didaktikhefte/2007%20Band%2040/VortragDorfmayr.pdf

[5] http://de.wikibooks.org/wiki/Beweisarchiv:_Kryptografie:_Kryptosysteme:_Korrektheit_des_RSA-Kryptosystems