Zahlen und das Hüten von Geheimnissen (G. Wiese, 23. April 2009)

Probleme unseres Alltags

- E-Mails lesen:
  Niemand außer mir soll meine Mails lesen!
- Geld abheben mit der EC-Karte:

  Niemand außer mir soll an mein Geld kommen!
- Telefonieren mit dem Handy:

  Niemand anderes soll auf meine Kosten telefonieren!
- Einkaufen im Internet:
  Niemand anderes soll das auf meine Rechnung tun!
- Sicherheit des Reisepasses:

  Niemand soll den Pass fälschen können!

Zur Datensicherheit braucht man kryptographische Verfahren.

Die Zahlentheorie spielt hierbei eine entscheidende Rolle!

Übrigens...

In unserem Rechenbeispiel haben wir die Primzahl 13 benutzt. Die in Wirklichkeit verwendete Primzahl sollte aber nicht 13, sondern mindestens so groß sein wie diese:

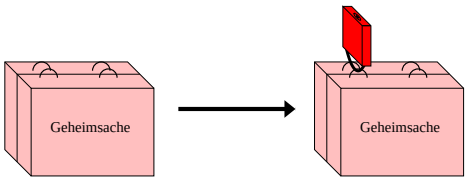
> 17976931348623159077293051907890247336179769789423065727343008115773267580
> 55009631327084773224075360211201138798713933576587897688144166224928474306
> 39474124377767893424865485276302219601246094119453082952085005768838150682
> 34246288147391311054082723716335051068458629823994724593847971630483535632
> 9624224137859

Natürlich übernimmt dann der Computer die Rechenarbeit...

Das Verschicken der Nachricht

Die Nachricht ist N, zum Beispiel 6.

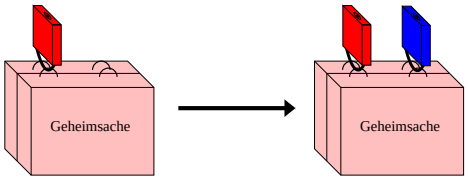
1. Schritt: Abschließen mit rotem Schloss



Berechne A als den Rest von $\underbrace{N \cdot N \cdot \ldots \cdot N}_{5-\text{mal}} = N^5$ beim Teilen durch 13.
Zum Beispiel: Der Rest von $\underbrace{6 \cdot 6 \cdot \ldots \cdot 6}_{5-\text{mal}} = 6^5$ beim Teilen durch 13 ist 2.

Jetzt wird A, also im Beispiel 2, an den Empfänger verschickt.

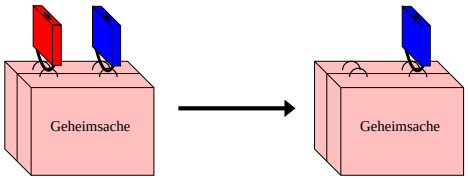
2. Schritt: Abschließen mit blauem Schloss



Berechne B als den Rest von $\underbrace{A \cdot A \cdot \ldots \cdot A}_{7-\text{mal}} = A^7$ beim Teilen durch 13.
Zum Beispiel: Der Rest von $\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{7-\text{mal}} = 2^7$ beim Teilen durch 13 ist 11.

Jetzt wird B, also im Beispiel 11, zurück an den Absender verschickt.

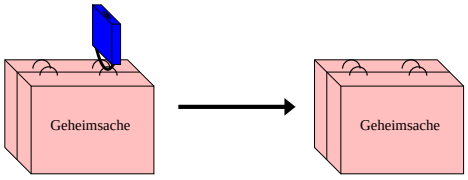
3. Schritt: Entfernen des roten Schlosses



Berechne C als den Rest von $\underbrace{B \cdot B \cdot \ldots \cdot B}_{5-\text{mal}} = B^5$ beim Teilen durch 13.
Zum Beispiel: Der Rest von $\underbrace{11 \cdot 11 \cdot \ldots \cdot 11}_{5-\text{mal}} = 11^5$ beim Teilen durch 13 ist 7.

Jetzt wird C, also im Beispiel 7, an den Empfänger verschickt.

4. Schritt: Entfernen des blauen Schlosses



Erhalte N als den Rest von $\underbrace{C \cdot C \cdot \ldots \cdot C}_{7-\text{mal}} = C^7$ beim Teilen durch 13.
Zum Beispiel: Der Rest von $\underbrace{7 \cdot 7 \cdot \ldots \cdot 7}_{7-\text{mal}} = 7^7$ beim Teilen durch 13 ist 6.

Wir haben die Nachricht N, also im Beispiel 6, erhalten!

Warum funktioniert das?

13 ist eine **Primzahl**. Das ist eine ganze Zahl größer als 1, die nur durch 1 und sich selbst teilbar ist.
Beispiele für Primzahlen: 2, 3, 5, 7, 11, 13, 17, 19. Keine Primzahlen: 4, 6, 8, 9.
Am Anfang des Studiums lernt man, dass es unendlich viele Primzahlen gibt.

Die benutzten Zahlen 5 und 7 haben folgende Eigenschaft:

Der Rest von $2^{5\cdot 5} = \underbrace{2\cdot 2\cdot \ldots \cdot 2}_{25-\text{mal}}$ beim Teilen durch 13 ist 2.
Der Rest von $3^{5\cdot 5} = \underbrace{3\cdot 3\cdot \ldots \cdot 3}_{25-\text{mal}}$ beim Teilen durch 13 ist 3.
usw. für alle Zahlen zwischen 1 und 12, z. B.
Der Rest von $12^{5\cdot 5} = \underbrace{12\cdot 12\cdot \ldots \cdot 12}_{25-\text{mal}}$ beim Teilen durch 13 ist 12.

Das gleiche gilt für 7:

Der Rest von $2^{7\cdot 7} = \underbrace{2\cdot 2\cdot \ldots \cdot 2}_{49-\text{mal}}$ beim Teilen durch 13 ist 2.
Der Rest von $3^{7\cdot 7} = \underbrace{3\cdot 3\cdot \ldots \cdot 3}_{49-\text{mal}}$ beim Teilen durch 13 ist 3.
usw. für alle Zahlen zwischen 1 und 12.

Im Studium lernt man, dass das an folgender Eigenschaft liegt:

Der Rest von $5\cdot 5$ beim Teilen durch 12 ist 1, denn $25 = 2\cdot 12$ Rest 1.
Der Rest von $7\cdot 7$ beim Teilen durch 12 ist 1, denn $49 = 4\cdot 12$ Rest 1.

Allgemein gilt Obiges nämlich für jede Zahl, die beim Teilen durch 12 den Rest 1 lässt.
Zum Beispiel für 13, denn $13 = 1\cdot 12$ Rest 1. Diese Aussage heißt der *kleine Satz von Fermat*:

Der Rest von $2^{13} = \underbrace{2\cdot 2\cdot \ldots \cdot 2}_{13-\text{mal}}$ beim Teilen durch 13 ist 2.
Der Rest von $3^{13} = \underbrace{3\cdot 3\cdot \ldots \cdot 3}_{13-\text{mal}}$ beim Teilen durch 13 ist 3.
usw. für alle Zahlen zwischen 1 und 12.

Für Fortgeschrittene:

Wir schreiben $a \equiv b$, wenn a und b beim Teilen durch 13 denselben Rest lassen. Zum Beispiel: $49 \equiv 10$.

Regel für das Rechnen mit Resten (bei der Verschlüsselung bereits benutzt):

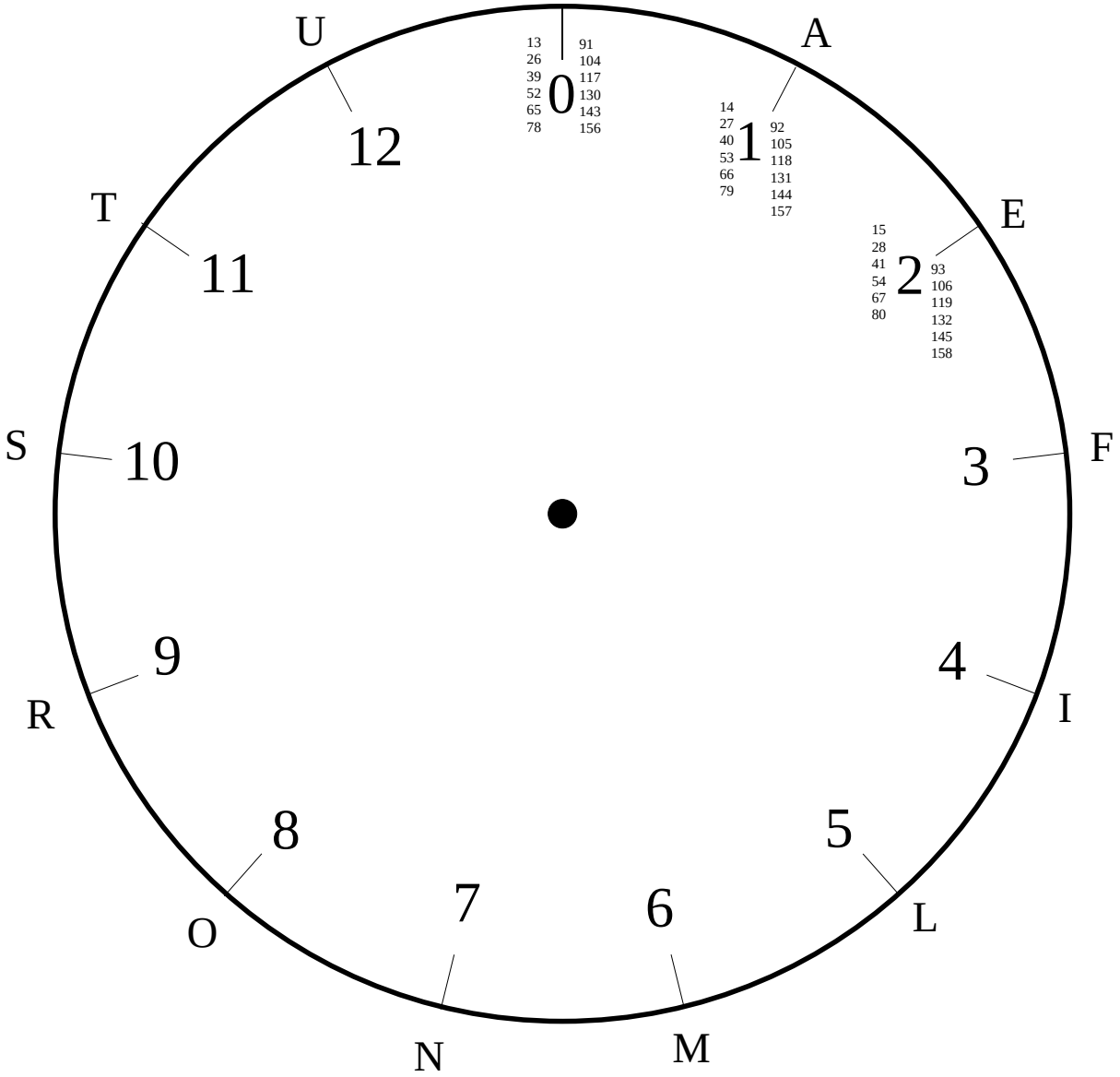
Sind $a \equiv r$ und $b \equiv s$, dann gilt auch $a\cdot b \equiv r\cdot s$.
Zum Beispiel: $49 \equiv 10$ und $82 \equiv 4$. Daher $49\cdot 82 \equiv 10\cdot 4 \equiv 1$.

Grund, warum das Verfahren funktioniert: Wir benutzen die Rechenregeln für das Potenzieren.

Nachricht: N
1. Schritt: $A \equiv N^5$
2. Schritt: $B \equiv A^7 \equiv (N^5)^7 \equiv N^{5\cdot 7}$
3. Schritt: $C \equiv B^5 \equiv (N^{5\cdot 7})^5 \equiv N^{5\cdot 5\cdot 7} \equiv (N^{5\cdot 5})^7 \equiv N^7$
4. Schritt: $C^7 \equiv (N^7)^7 \equiv N^{7\cdot 7} \equiv N$
Wir finden also die Nachricht N wieder!

Die 13er Restuhr

Die **große** Zahl ist der Rest der kleinen Zahl beim Teilen durch 13.



Wie bestimmt man den Rest einer Zahl beim Teilen durch 13*?*

1. Methode: Bestimme den Rest von 20 beim Teilen durch 13.
Fange bei 0 an und laufe im Uhrzeigersinn 20 Schritte weiter. Du endest auf der 7 und das ist der gesuchte Rest:

$$20 = 1 \cdot 13 \text{ Rest } 7.$$

2. Methode: Bestimme den Rest von 110 beim Teilen durch 13.
Suche das größte Vielfache von 13, das kleiner gleich 110 ist. Die ersten paar Vielfachen von 13 stehen neben der 0 und Du findest 104. Jetzt berechnest Du die Differenz $110 - 104 = 6$. Der gesuchte Rest ist 6:

$$110 = 8 \cdot 13 \text{ Rest } 6.$$

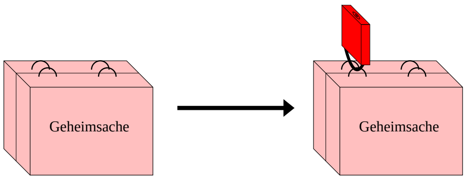
3. Methode (mit Taschenrechner): Bestimme den Rest von 347 beim Teilen durch 13.
Teile 347 durch 13. Du findest $26,69\ldots$. Nimm die Zahl vor dem Komma (ohne Rundung), also 26, und berechne die Differenz $347 - 26 \cdot 13 = 9$. Der gesuchte Rest ist 9.

$$347 = 26 \cdot 13 \text{ Rest } 9.$$

Geheimer $(5,5)$-Schlüssel für den Absender (13er Restuhr)

Nachricht (6-8 Zeichen): ____ ____ ____ ____ ____ ____ ____ ____

1. Schritt: Abschließen mit rotem Schloss

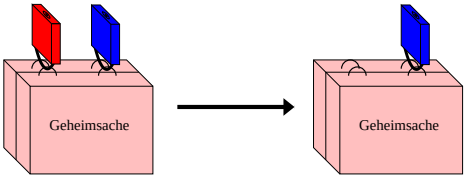


Nachricht		Ergebnis A
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐
☐	$\frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square} \cdot \frac{\_\_}{\square}$	☐

Beispiel

M	$\frac{6}{\boxed{6}} \cdot \frac{10}{\boxed{6}} \cdot \frac{8}{\boxed{6}} \cdot \frac{9}{\boxed{6}}$	2

3. Schritt: Entfernen des roten Schlosses



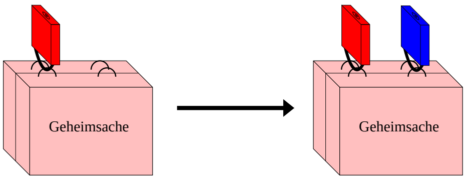
Ergebnis B **Ergebnis C**

Beispiel

$$11 \cdot 11^{\frac{4}{\ }} \cdot 11^{\frac{5}{\ }} \cdot 11^{\frac{3}{\ }} \cdot 11 \quad 7$$

Geheimer $(7, 7)$-Schlüssel für den Empfänger (13er Restuhr)

2. Schritt: Abschließen mit blauem Schloss

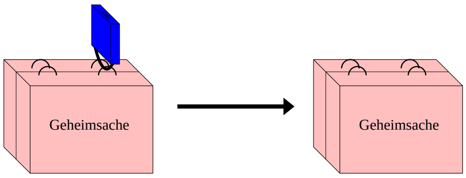


Ergebnis A **Ergebnis B**

Beispiel

$\boxed{2} \cdot \boxed{2} \overset{4}{\text{—}} \cdot \boxed{2} \overset{8}{\text{—}} \cdot \boxed{2} \overset{3}{\text{—}} \cdot \boxed{2} \overset{6}{\text{—}} \cdot \boxed{2} \overset{12}{\text{—}} \cdot \boxed{2} \quad \boxed{11}$

4. Schritt: Entfernen des blauen Schlosses



Ergebnis C **Nachricht**

Die Nachricht lautet: ____ ____ ____ ____ ____ ____ ____ ____

<u>Beispiel</u>

$7 \cdot \frac{10}{7} \cdot \frac{5}{7} \cdot \frac{9}{7} \cdot \frac{11}{7} \cdot \frac{12}{7}$ 6 ⇝ M

Ergebnis A von _____ an _____:

Ergebnis B von _____ an _____:

Ergebnis C von _____ an _____:

Ergebnis A von _____ an _____:

Ergebnis B von _____ an _____:

Ergebnis C von _____ an _____:

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.

Schicke Nachricht an: _____.