Primzahlen finden mit dem Sieb des *Eratosthenes*

Für die asymmetrische Kryptographie benötigen wir mathematische Funktionen, deren Anwendung mit einer Information (dem öffentlichen Schlüssel) sich durch Anwendung mit einer anderen Information (dem privaten Schlüssel) rückgängig machen lässt. Hier spielen **Primzahlen** eine wichtige Rolle, die einige besondere Eigenschaften aufweisen:

Definition:
Primzahlen sind alle natürlichen Zahlen größer als 1, die nur durch 1 und sich selber teilbar sind.
Alle natürlichen Zahlen größer als 1, die keine Primzahlen sind, heißen **zusammengesetzte Zahlen**.
Die 1 ist weder eine Primzahl noch ist sie zusammengesetzt!

Aufgabe 1: Nenne 10 Beispiele für Primzahlen!

Aufgabe 2: Überlege Dir eine Begründung, warum man die anderen Zahlen „zusammengesetzt" nennt! Nenne 10 Beispiele für zusammengesetzte Zahlen!

Wie findet man Primzahlen? Eine sehr effektive Methode ist das **Sieb des *Eratosthenes***.

Aufgabe 3: Informiere Dich unter der Adresse http://www.hbmeyer.de/eratosib.htm über die Funktionsweise des Primzahlsiebs! Bearbeite die auf dieser Seite genannte Aufgabe!

Zur Auswertung dieser Experimente überleg Dir Antworten auf die folgenden Fragen:

- Warum erhält man bereits alle Primzahlen ≤ 400, wenn man nur mit den Primzahlen ≤ 20 „siebt"?
- Wieso kann man sicher sein, dass wirklich nur noch Primzahlen in der Tabelle stehen?
- Warum nannte *Eratosthenes* das Verfahren, das er vermutlich gar nicht selber erfunden hat, „Sieb"?

Wichtig für die moderne Kryptologie im Allgemeinen und das RSA-Verfahren im Besonderen sind die so genannten **Semiprimzahlen**. Das sind natürliche Zahlen ***n***, die genau zwei unterschiedliche Primfaktoren ***p*** und ***q*** haben, so dass $n = p \cdot q$ gilt. Für die asymmetrische Kryptographie ist es wichtig, dass man aus dem öffentlichen Schlüssel ***e*** den privaten Schlüssel ***d*** nicht berechnen kann. Dies wird beim RSA-Verfahren dadurch abgesichert, dass es praktisch unmöglich ist, riesige Semiprimzahlen mit hunderten von Dezimalstellen in ihre beiden Primfaktoren zu zerlegen. Umgekehrt ist es sehr einfach, aus zwei großen Primzahlen durch Multiplikation eine Semiprimzahl zu erzeugen.

Aufgabe 4: Welche der folgenden Zahlen sind Primzahlen, welche sind Semiprimzahlen?
Falls es Semiprimzahlen sind: Gib die Faktoren an!

23, 55, 113, 119, 841, 1829, 3109, 9847, 10807, 13121, 14603, 15551, 16061, 16199,
1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

Hinweis: Du kannst die Zahlen mit dem Sieb des Eratosthenes faktorisieren, oder mit *CrypTool*:
Einzelverfahren -> RSA-Kryptosystem -> Faktorisieren einer Zahl...
Ist der größte Faktor rot dargestellt, so lässt er sich mit Klick auf den „Weiter"-Knopf in weitere Faktoren zerlegen.
Lässt sich eine Zahl nicht in vernünftiger Zeit faktorisieren, so lässt sich zumindest recht schnell feststellen, ob die Zahl eine Primzahl ist:
Einzelverfahren -> RSA-Kryptosystem -> Primzahltest

Aufgabe 5: Recherchiere: Was hat letzte Zahl mit der *RSA Factoring Challenge* zu tun?
(z.B. auf http://en.wikipedia.org/wiki/RSA_numbers)

Zusatzaufgabe: Recherchiere: Wer war eigentlich *Eratosthenes*?