

CLUB APOLLO 13 AUFGABE 4

Verschlüsselung

Diese Aufgabe aus der Mathematik wird vom Fachgebiet Zahlentheorie der Leibniz Universität Hannover gestellt. Weitere Informationen zum Studiengang der Mathematik finden Sie unter <http://www.maphy.uni-hannover.de/>

In der modernen Zeit ist die digitale Datenübertragung nicht mehr wegzudenken, so findet ein Großteil der Kommunikation digital via E-Mail statt. Außerdem werden immer mehr Geschäfte auf digitalem Wege übers Internet getätigt; Einkaufen per Mausklick, Online-Banking oder einfach nur die Authentifizierung in einem Onlineforum sind längst keine Fremdwörter mehr. Doch je mehr diese Art der Kommunikation zunimmt, desto mehr stellt sich die Frage nach der Geheimhaltung. Kann wirklich nur der Empfänger die E-Mail lesen? Oder kann sie vielleicht jeder lesen? Ist es für mich sicher, wenn ich Überweisungen online tätige? Oder kann jeder auf mein Konto zugreifen, oder in meinem Namen Bestellungen aufgeben?



Ein Zweig der Mathematik beschäftigt sich genau damit. In der Zahlentheorie, genauer in der **Kryptographie**, erforscht man Methoden, um Daten verschlüsselt zu übermitteln, d.h. man möchte Wege finden, wie zwei Personen in Kontakt treten können, ohne dass ein Dritter mitlesen kann.

a) Einfache Verschlüsselungen (7 Punkte)

Eine Möglichkeit zur Datenverschlüsselung ist eine **Substitutionschiffre**. Dabei werden die Buchstaben der eigentlichen Nachricht durch andere Buchstaben oder Zeichen ersetzt, so dass im ersten Moment eine unlesbare Nachricht entsteht, beispielsweise könnte man immer E durch Z und F durch A ersetzen (für die anderen Buchstaben entsprechend).

Wenn man jetzt weiß, welcher Buchstabe in der Nachricht für welchen Buchstaben im Original steht (man bezeichnet dies auch als **Schlüssel** für die Verschlüsselung) kann man die Nachricht entschlüsseln. Doch wie sieht es aus, wenn man den Schlüssel nicht kennt?

1. Eine recht einfache Verschlüsselungsmethode ist ein **Verschiebechiffre** (Spezialfall der Substitutionschiffre). Dabei wird jeder Buchstabe des Alphabets um eine bestimmte Stelle verschoben; verschiebt man beispielsweise um 2 Stellen, so wird aus einem A ein C und aus einem B ein D. Entschlüsseln Sie folgende Nachricht, die auf diese Art chiffriert wurde:

Xcymy Gynbixy qclx uowb Wuymul-Wbczzly ayhuhhn.

2. Da eine Verschiebechiffre sehr einfach zu knacken ist, verschlüsselt ein Freund von Ihnen seine E-Mails mit einer Substitutionschiffre. Sie haben nun folgende Nachricht erhalten, aber leider kennen Sie den Schlüssel nicht mehr:

Rud dcl zcnoa nrudst hadv myn brv oadyavs. Hazba brud arnpcud cqp ozarudah Kao lar hrv.

Versuchen Sie herauszufinden, welche Nachricht sich dahinter verbirgt (Hinweis: Häufigkeitsanalyse). Erklären Sie Ihr Vorgehen.

Es gibt mehrere Methoden dieser Art um Nachrichten zu verschlüsseln. Einige sind schwerer zu entschlüsseln als andere. Eines haben sie jedoch alle gemeinsam: Man muss sich vorher einmal über einen bestimmten Schlüssel verständigen, sonst ist es (im Idealfall) unmöglich, dass der Empfänger diese lesen kann. Allerdings würde es sich als sehr umständlich herausstellen, wenn z.B. eine Bank mit jedem Kunden einmal einen individuellen Schlüssel vereinbaren müsste. Nicht nur, dass dies sehr viele verschiedene wären, man müsste auch persönlich zur Bank gehen um den Schlüssel zu erhalten.

In den 70er Jahren gelang es Mathematikern, ein Kryptosystem zu entwickeln, bei dem es nicht mehr nötig war vorher den Schlüssel auszutauschen, sondern bei dem man den Schlüssel sogar frei publizieren konnte. Dieses Verfahren heißt RSA und bildet die Grundlage z.B. für die sichere Verschlüsselung von E-Mails oder Bankgeschäften.

Das **RSA-Verfahren** funktioniert in folgenden Schritten:

1. Wähle zwei Primzahlen p und q und berechne ihr Produkt $n = p \cdot q$. Die Zahl n wird auch als **Modul** bezeichnet.
2. Berechne $\varphi(n) = (p-1) \cdot (q-1)$.
3. Wähle eine Zahl e , für die $1 < e < \varphi(n)$ gelten soll, und die teilerfremd zu $\varphi(n)$ ist. Diese Zahl e ist unser **Verschlüsselungsexponent**.
4. Berechne eine Zahl d , für die gelten soll $d \cdot e \equiv 1 \pmod{\varphi(n)}$ (Hinweis: Modulo-Rechnung, erweiterter euklidischer Algorithmus). Dieses d wird auch als **Entschlüsselungsexponent** bezeichnet.

Der **öffentliche Schlüssel** (also das, was jeder sehen darf) besteht dann aus e und n . Nachrichten verschlüsselt man dann, indem man sie in Zahlenfolgen umwandelt und dann für jede Zahl m der Nachricht eine Zahl c berechnet mit

$$c \equiv m^e \pmod{n}$$

berechnet (Hinweis: modulares Potenzieren).

Alle anderen Informationen bleiben geheim. Die Entschlüsselung erfolgt, indem man für die übertragenen Zahlen c den Wert $m \equiv c^d \pmod{n}$ berechnet und so wieder die ursprüngliche Nachricht erhält. Auf diese Art kann man einzelne Buchstaben oder auch längere Zeichenketten auf einmal verschlüsseln.

b) Mittlerer Teil, Verschlüsselung mit RSA (11 Punkte)

1. Verschlüsseln Sie die Nachricht "Hallo" mit den Parametern $p = 13$, $q = 17$, $e = 11$. Um die Buchstaben in Zahlen umzuwandeln identifizieren Sie diese einfach mit ihrer Stellung im Alphabet (A=1, B=2, etc.).
2. Entschlüsseln Sie die Nachricht
076 111 056 164 185 041 076 111 184 200 041
mit den Parametern $p = 13$, $q = 17$, $e = 11$.
3. Doch wie sieht es aus, wenn man eine Nachricht entschlüsseln möchte, aber einen Teil der Parameter nicht kennt? Entschlüsseln Sie folgende Nachricht, von der Sie nur die öffentlichen Parameter ($n = 50429$, $e = 30757$) kennen.
13718 26362 00001 50085 17439 11060 00001 50085 40675 04024 45801.
Erklären Sie ausführlich Ihre Lösung.
4. Wo liegen Ihrer Meinung und Ihrer Erfahrung nach Vor- und Nachteile des RSA-Verfahrens? Begründen Sie Ihre Antworten.

c) Für Profis (7 Punkte)

Wie Sie festgestellt haben, hängt sehr viel von den verwendeten Primzahlen ab. Je größer die Primzahlen p und q sind, desto sicherer ist das Verfahren, denn ein Spion muss zunächst die Zahl n in die beiden Faktoren zerlegen, um dann $\varphi(n)$ und auch d zu berechnen. In der aktuellen Forschung ist man deshalb bemüht, möglichst große Primzahlen zu finden.

Schreiben und dokumentieren Sie ein Computerprogramm, welches möglichst effizient in der Lage ist

1. zu entscheiden, ob eine vorgegebene Zahl eine Primzahl ist, und
2. selbstständig eine Primzahl zu finden.

Anschließend soll das Programm überprüfen, ob 3088390861 eine Primzahl ist, und eine Primzahl p finden, für die $p > 2^{20}$ gilt.

Natürlich gibt es einige mathematische Verfahren, welche die Suche erleichtern können (Probedivision, Fermat-Test, Miller-Rabin-Test,...).

Das Programm kann in einer beliebigen Programmiersprache geschrieben sein (wie bei der vorangegangenen Apollo-Aufgabe).

Viel Erfolg bei der vierten Aufgabe!

Falls Sie Fragen zu den Aufgaben haben oder eine Hilfestellung benötigen, so schauen Sie doch einfach mal in unser Forum: <http://www.unikik.uni-hannover.de/forum/>

Einsendeschluss: Donnerstag, der 20. Dezember 2007, 23:59.

Senden Sie Ihre Lösungen per E-Mail an: leydecker@unikik.uni-hannover.de.

Die E-Mail sollte nicht größer als 3 MB sein (Die Dateien können gezippt sein)! Bitte geben Sie auch Ihren Teamnamen, die Namen der Gruppenmitglieder sowie deren Schulen an. Bitte schreiben Sie in der Betreffzeile der E-Mail Ihren Gruppennamen und benennen Sie Ihre angehängten Dateien danach.

Sie können/sollten Ihre Lösung auch dann abgeben, wenn Sie die letzte Teilaufgabe (die Profiaufgabe) nicht gelöst haben! Vielleicht gelingt Ihnen das ja bei der letzten Aufgabe.

Die Teilnahmebedingungen und weitere Informationen finden Sie unter

<http://www.unikik.uni-hannover.de/apollo13/>