Das Rucksackproblem

Das sogenannte Rucksackproblem bezeichnet das folgende Problem: Man hat einen Rucksack, der nur ein bestimmtes Gewicht tragen kann. In dem Rucksack sollen möglichst viele und wertvolle Dinge transportiert werden. Das Gewicht und der Wert dieser Waren sind bekannt.

Eine Möglichkeit, eine gute Rucksackladung zu erhalten, funktioniert wie folgt: Man berechnet den Quotienten aus Nutzen (hier Wert) und verbrauchten Ressourcen (hier Gewicht) für alle Waren. Dann packt man das Objekt mit dem größten Quotienten, welches noch in den Rucksack passt, ein. Dies wiederholt man so lange, bis kein Objekt mehr in den Rucksack passt.

Klasse 5-6

Theo ist Musiker und hat am Wochenende einen Auftritt. Vom Veranstalter des Konzerts hat er 15 Minuten für seinen Auftritt bekommen. Natürlich möchte er möglichst viele Zuschauer zufriedenstellen. Daher hat er vorher eine Umfrage unter seinen Fans gemacht, um deren Lieblingslieder herauszufinden. Das Ergebnis ist in der folgenden Tabelle zu entnehmen:

Name	Song 1	Song 2	Song 3	Song 4	Song 5	Song 6	Song 7
Dauer	4 min	2 min	3.5 min	6 min	5 min	3 min	2 min
Stimmen	100	60	70	132	120	75	70

Welche Songs sollte Theo spielen, um innerhalb der 15 Minuten den Lieblingssong möglichst vieler Fans zu spielen? Nutze dazu den oben beschriebenen Weg zur Ermittlung der optimalen Setlist.

Klasse 7-9

Bearbeite zunächst die erste Aufgabe!
Das Rucksackproblem kann auch dazu genutzt werden, um Nachrichten zu verschlüsseln. Stellt man sich vor, man kennt nur das Gewicht des Rucksacks, aber nicht das Gewicht der möglichen Gegenstände, so ist es sehr schwer herauszufinden, was sich im Rucksack befindet. Genau auf diesem Prinzip basiert eine Verschlüsselung. Hier betrachten wir eine vereinfachte Variante des *Merkle-Hellman-Kryptosystem*.
Der private Schlüssel ist dabei eine Liste von "Gewichten". Im Folgenden benutzen wir den privaten Schlüssel $S = \{2, 3, 6, 13\}$. Überlegt man sich nun noch einen Multiplikator n, so lässt sich der öffentliche Schlüssel errechnen. Dieser wird von jedem benötigt, der eine verschlüsselte Nachricht schicken möchte. Diese verschlüsselte Nachricht kann man dann mit dem privaten Schlüssel wieder in die ursprüngliche Nachricht verwandeln. Hier nehmen wir den Multiplikator $n = 73$. Damit errechnet sich der öffentliche Schlüssel P durch Multiplikation des privaten Schlüssels mit dem Multiplikator.

$$\begin{aligned} P &= \{n \cdot 2, n \cdot 3, n \cdot 6, n \cdot 13\} \\ &= \{146, 219, 438, 949\} \end{aligned}$$

Eine beispielhafte Verschlüsselung wird nun anhand der Nachricht 1100 gezeigt. Jede Zahl der Nachricht wird mit der entsprechenden Zahl des öffentlichen Schlüssels multipliziert. Anschließend addiert man alle diese Zahlen zusammen und erhält die verschlüsselte Nachricht.

P	146	219	438	949	
Nachricht	1	1	0	0	
Produkt	$146 \cdot 1$	$219 \cdot 1$	$438 \cdot 0$	$949 \cdot 0$	
Summe	146	+ 219	+ 0	+ 0	= 365

Die verschlüsselte Nachricht lautet also 365!

Verschlüssele nun selbst die folgende Nachricht:

01001100 11110110 01110011 01110101 01101110 01100111

Verschlüssele dazu immer jeweils einen Block von 4 Ziffern.

Klasse 10-12

Bearbeite zunächst die ersten beiden Aufgaben!
In unserer vereinfachten Verschlüsselung genügt es die verschlüsselte Nachricht durch den Multiplikator n zu dividieren, um dann herauszufinden, welche Gewichte zu diesem Gesamtgewicht führen.
Nimmt man das Beispiel der vorherigen Aufgabe so ist das Gewicht des Rucksacks $\frac{365}{73} = 5$. Da der private Schlüssel geschickt gewählt wurde, stellt man die Elemente auf die folgende Weise wieder her:

1. Finde das schwerste Element, dessen Gewicht kleiner ist als das des Rucksacks.
2. Entferne dieses Element aus dem Rucksack.
3. Falls der Rucksack noch nicht leer ist, fange wieder bei 1. an.

Betrachten wir das Beispiel von oben, so ist das Gewicht des Rucksacks 5. Das schwerste Element aus dem privaten Schlüssel $S = \{2, 3, 6, 13\}$, das leichter ist als der Rucksack ist also die 3. Das heißt die letzten beiden Ziffern unserer Nachricht sind 0 (sie sind nicht im Rucksack). Die zweite Ziffer ist eine 1 (ist im Rucksack). Nach dem Entfernen der 3 ist das Gewicht des Rucksacks 2. Also ist auch die erste Ziffer eine 1 (das erste Gewicht des privaten Schlüssels ist im Rucksack).
Die ursprüngliche Nachricht ist also 1100.
Entschlüsselt die Nachricht:

657 1533 657 949 1606 657 657 1606

Ein Binär zu ASCII Konvertierer hilft das ganze in Klartext darzustellen!

Begründete Ergebnisse mit Lösungsweg bitte bis Ende des Monats bei Frau Rust (Ru) abgeben oder in das Fach legen lassen. Nicht vergessen, den Namen, die Klasse/den Kurs und die Mathematiklehrkraft auf dem Lösungszettel mit anzugeben. Viel Erfolg!