Kryptosysteme, Keymanagment (KSK3) für CMS
5. Übungsblatt für den 14. November 2006

17. Erkläre und verstehe die *Mathematica*-Funktion

```
ListOfNaturalsQ[lst_] :=
   VectorQ[lst, IntegerQ[#] && (# > 0) &]
```

18. (*) Erkläre und verstehe die *Mathematica*-Funktion

```
SIQ[lst_?ListOfNaturalsQ] :=
   Apply[And, Thread[FoldList[Plus, 0, Most[lst]] < lst]]
```

(*Hinweis:* Studiere zuerst in der Online-Hilfe unter *The Mathematica Book* den Abschnitt *Principles of Mathematica→Expressions*).

19. Bob schickt mit dem Merkle-Hellman-Kryptosystem die verschlüsselte Nachricht $C = 183$ an Alice. Der geheime Schlüssel von Alice ist

$$(b, m, v_1, v_2, v_3, v_4, v_5) = (57, 101, 3, 5, 9, 20, 53).$$

Wie lautet ihr öffentlicher Schlüssel? Welchen Klartext (Bitfolge) entschlüsselt sie?

20. Gib alle 10-glatten Zahlen an, die kleiner gleich 25 sind.