Das RSA-Verfahren

3. Bobs Geheimnachricht: 99

4. Alice erhält […] 99 als Botschaft von Bob.
   Alice' Entschlüsselung: B = 99^{17} mod 253 = 88

Aufgaben:

A) Vergleiche die Formeln der Ver- und Entschlüsselung: Bei gleicher Struktur unterscheiden sich die Inhalte der Formeln. Formuliere hier aus, wie:

Bob verschlüsselt mit Alice' öffentlichem Schlüssel (e als Exponent).
Alice entschlüsselt mit ihrem privaten Schlüssel (d als Exponent).
Die Modulzahl ist bei beiden die selbe (N)

Wechselseitige Kommunikation

Möchte nun Alice auf Bobs Nachricht antworten, so muss das Vorgehen zur Schlüsselerzeugung von Bob gerade noch einmal vorgenommen werden: Bob muss einen geheimen und einen privaten Schlüssel erzeugen, damit Alice ihm antworten und ebenso verfahren kann wie er. Führe hier nochmals das Procedere nach der Anleitung für Alice (s. oben) an einem Beispiel mit nicht zu großen Zahlen für Bob durch:

- X Wahl zweier Primzahlen p = individuell q = individuell
- X Wahl von e mit $1 < e < (p-1)\cdot(q-1)$. e = ...
- X Geheimer Schlüssel: $1 = (e \cdot d) \bmod (p-1)\cdot(q-1) \Rightarrow d$ =.....
- X Öffentlicher Schlüssel (e ; N) = ... → an Alice
- X Alice' Verschlüsselung mit Bobs öffentlichem Schlüssel $S = B^e \bmod N$ = …
- X Bobs Entschlüsselung mit seinem privatem Schlüssel: $B = S^d \bmod N$ = ...