SMS1 für MC, FHS Hagenberg
7. Übungsblatt für den 18. November 2004

Die Angaben finden Sie auch im Mathematica Notebook `ue7ws04.nb`.

1. Ein Text wurde nach RSA mit dem Public Key
   $n = 232646010703534527043004781508727467783$,
   $e = 135402440092004222070613872668215994 33$ zu
   $c = 197212580404504151079829847853402100374$
   verschlüsselt. Finden Sie den entschlüsselten Text durch Repeated Encryption.

   Können Sie den Private Key d angeben?

2. Sei n wie in Aufgabe 1. Eine Nachricht m ist mit $(n, 257)$ zu
   $c_1 = 18259032326704243019558919621285151147 5$
   und mit $(n, 17)$ zu
   $c_2 = 566827008573314185421059528748439823 67$
   verschlüsselt worden. Bestimmen Sie m.

3. Mit n wie in Aufgabe 1 und $e = 5$ ist eine Nachricht zu
   $c = 194909284449142526724561701134336102 4$
   verschlüsselt worden.

   Finden Sie die ursprüngliche Nachricht.

4. Sei n wie in Aufgabe 1, $(n, 23011967)$ ein RSA-Public-Key mit zugehörigem Private-Key
   $d = 164475374728334378198948086435160402327$.
   Bestimmen Sie die Faktoren von n wie in [1] beschrieben.

Literatur

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.