Aufgabe 1. Schreibe ein Modul, welches RSA-Verschlüsselung implementiert. Mache dir vorher Gedanken, wie dein Nachrichtenraum aussehen soll.

Aufgabe 2. Schreibe ein „Key-Recovering-Program“, dass dein eben geschriebenes Modul verwendet um zu einem öffentlichen Schlüssel den privaten Schlüssel durch (systematisches) Ausprobieren ermittelt.
Verwende dazu auch OpenMP.

Aufgabe 3. Unter

http://bit.ly/xuf2Ry

findest du den Heise-Artikel zu unsicheren RSA-Keys. Finde einige dieser Schlüssel, verstehe das Format indem sie abgespeichert sind und versuche sie zu knacken.