

Übung RSA-Algorithmus

1. erzeugen Sie die Schlüssel für den RSA-Algorithmus (Schritte a) bis e) „geheim“ durchführen)
 - a) 2 Primzahlen p und q wählen
 - b) RSA-Modul n berechnen $n=p \cdot q$
 - c) $J(n)$ berechnen $J(n)=(p-1) \cdot (q-1)$
 - d) öffentlichen Schlüssel e wählen mit $\max(p,q) < e < J(n)$ und $J(n) \bmod e > 0$
 - e) einen geheimen Schlüssel d suchen mit $(d \cdot e) \bmod J(n) = 1$ (ggf. e nochmals ändern)
 - f) Den öffentlichen Schlüssel e und den verwendeten RSA-Modul n veröffentlichen (an Wandtafel)

2. Kodieren Sie mit dem öffentl. Schlüssel und dem RSA-Modul eines anderen Studenten (arbeiten Sie paarweise, aber nicht mit direkten Nachbarn!) eine Nachricht M (*Message*) und übermitteln Sie die kodierte Nachricht C (*Cipher*) öffentlich (an Wandtafel)
 - a) die Nachricht M ist eine Zahl (Bedingung $M < n$ n :RSA-Modul des anderen Studenten)
 $C = M^e \bmod n$
 - b) die Nachricht ist ein String (Kodierung Blank=00; A=01; B=02; C=03 ... Z=26) mit 10-20 Zeichen.
Wenn $M > n$ gilt, so ist M in mehreren Teilen zu kodieren (z.B. erste 4 Zeichen, zweite 4 Zeichen ...)

3. Dekodieren Sie die nach 2) erhaltenen Nachrichten C mit der Formel: $M = C^d \bmod n$

4. Versuchen Sie Nachrichten unter Nutzung der bekannten Informationen (Wandtafel) ‚auszuspionieren‘.
Dazu ist n in Faktoren zu zerlegen (Primfaktorzerlegung in p und q)
Tip: $\max(p,q) < e$ Verwenden Sie progr. Taschenrechner, Excel oder eigene Software