Gregor Leander
14.04.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 1

Aufgabe 1: *Faktorisierung und RSA* (8 Punkte)

Bestimmen Sie für den unten gegebenen RSA Modul $n = pq$ die Primzahlen p und q mittels der in der Vorlesung beschrieben Vorgehensweise$n$.

$$n = 1000730021 \ .$$

Der öffentliche Exponent e und der private Exponent d mit $ed \equiv 1 \bmod (p-1)(q-1)$ seien hierbei

$$(e, d) = (17, 412020005) \ .$$

Können Sie eine offensichtliche Schwäche im Modulus 1000730021 finden? Verallgemeinern!

Aufgabe 2: *RSA mit kleinem öffentlichen Exponent I* (6+6 Punkte)

Alice möchte eine Nachricht m für Bob Einstein (B_1), Bob Zweigelt (B_2) und Bob Drexler (B_3) verschlüsseln.
Der öffentliche RSA Modul von B_i sei n_i f ür $i \in \{1, 2, 3\}$, wobei $n_i \neq n_j$ f ür $i \neq j$ gilt. Der öffentliche Exponent ist bei allen Personen B_i gleich 3. A berechnet $c_i = m^3 \mod n_i$ und sendet c_i an B_i.

A. Berechnen Sie die verschlüsselte Nachricht mit der Methode für kleine öffentliche Exponenten für folgende Parameter.

$$(n_1, e_1) = (667, 3) \ , \qquad (n_2, e_2) = (289, 3) \ , \qquad (n_3, e_3) = (121, 3)$$

und

$$c_1 = 167 \ , \qquad c_2 = 60 \ , \qquad c_3 = 56 \ .$$

B. Mit wie vielen (verschiedenen) öffentlichen RSA Schlüsseln muss eine Nachricht verschlüsselt werden, damit ein ähnlicher Angriff für einen gemeinsamen Exponenten $e = 5$ funktioniert? Beschreiben Sie den Angriff.

Abgabe: Freitag, 18.04.2008 bis 12:00 Uhr. Entweder im Kasten im Gebäude NA Ebene 02, oder per Mail an `mansour.alsawadi@rub.de`.