Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2015/16
16. Dez. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 9

Aufgabe 33

Sei $N = pq$ ein RSA-Modul (d.h. $p \neq q$ ungerade Primzahlen) und e, d der Verschlüsselungs- bzw. Entschlüsselungs-Exponent, d.h. $ed \equiv 1 \bmod \varphi(N)$ mit der Eulerschen Phi-Funktion $\varphi(N) = (p-1)(q-1)$. Es gilt dann $x^{ed} \equiv x \bmod N$ für alle $x \in \mathbb{Z}$.

Sei nun $\lambda(N) := \operatorname{lcm}(p-1, q-1)$ das kleinste gemeinsame Vielfache von $p-1$ und $q-1$ und d' definiert durch

$$ed' \equiv 1 \bmod \lambda(N).$$

Man zeige, dass man auch d' als Entschlüsselungs-Exponent benützen kann, dass also gilt

$$x^{ed'} \equiv x \bmod N \quad \text{für alle} \quad x \in \mathbb{Z}.$$

Was kann man über die Differenz $d - d'$ aussagen?

Aufgabe 34

Seien $p, q \geqslant 3$ teilerfremde ungerade Zahlen, die entweder prim oder Carmichael-Zahlen sind. Sei $N := pq$ und seien e und d natürliche Zahlen mit $ed \equiv 1 \bmod (p-1)(q-1)$. Man zeige

$$x^{ed} \equiv x \bmod N \quad \text{für alle} \quad x \in \mathbb{Z}.$$

Warum ist es beim RSA-Kryptosystem trotzdem vorzuziehen, für p und q Primzahlen und nicht Carmichael-Zahlen zu verwenden?

Aufgabe 35

Seien N, p, q, e, d wie in Aufgabe 33 und

$$E : \mathbb{Z}/N \to \mathbb{Z}/N, \quad x \mapsto E(x) := x^e,$$

die Verschlüsselungs-Funktion. Ein Fixpunkt von E ist ein Element $x \in \mathbb{Z}/N$ mit $E(x) = x$.

a) Man zeige, dass die Abbildung E mindestens 9 Fixpunkte besitzt (darunter die trivialen $x = 0, \pm 1$). Genauer beweise man für die Anzahl r der Fixpunkte die Formel

$$r = (1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1)).$$

b) Man überlege sich, wie man im Fall $r = 9$ aus der Kenntnis eines nicht-trivialen Fixpunkts die Faktorzerlegung von N ableiten kann.

c) Man berechne alle Fixpunkte im Fall $(N, e) := (47299541, 65)$.

---

b.w.

Aufgabe 36

Gegeben sei ein RSA-Modul $N = pq$, wobei p, q ungerade Primahlen mit $q < p < 2q$ sind. Weiter seien $1 < e, d < \varphi(N)$ ganze Zahlen mit $ed \equiv 1 \bmod \varphi(N)$, also $ed = 1 + k\varphi(N)$ mit einer ganzen Zahl k.

a) Man beweise die Abschätzung

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{3}{\sqrt{N}}.$$

b) Man zeige: Falls $d < \frac{1}{3}N^{1/4}$, ist k/d ein Näherungsbruch der Kettenbruch-Entwicklung von e/N, vgl. den in Aufgabe 16b) zitierten Satz aus der Theorie der Kettenbrüche.
Dies kann nach M.J. Wiener (1990) dazu dienen, den Entschlüsselungs-Exponenten d aus (N, e) zu berechnen.

c) Man führe den in b) angedeuteten sog. Wiener-Angriff in folgendem Beispiel durch: In hexadezimaler Schreibweise sei (N, e) gegeben als

```
 N = AA12 5101 C475 659A 4764 76F2 2B5D 89AC 8EF0 83AE 65EF F3EA 2BCE 4A99
1F17 2C1C 3651 66C1 9D4F C0DA DEEA C46A 2547 0C52 CE70 0F3D 1549 FDB9 9D7F
1D73 85AB E5A8 7AA4 B882 374F 4727 BFF1 EC2A 01BB CE85 3053 87F8 EDE2 7086
7B8D 85CA E6D0 7BB5 8218 E640 9B5F 552B 87EA A1F0 5BE1 F1CC AE71 9B68 0309
62B0 B2B9 08C0 E3EA E79D;

 e = 8BF0 0D77 7084 5320 6BC1 91CC 072A 7CA2 CD0D 46D8 1546 5BF3 DBAA F322
9201 040A 3FFA BA77 C535 95F6 CC12 79B1 4E98 5291 6512 FBB4 B33A EA2A 2548
9908 AF0F F50A D31A 2ACE 2D35 FF54 53C4 FE57 F7A8 0F10 B03E B2E3 6F0E 0217
C3F7 3BA8 C428 19B8 50D2 C980 13F6 5093 AB92 B47A F80C CC8E 6E9A BEBB 328D
4EB2 7A40 3845 3561 E439;
```

Es sei bekannt, dass $d < 2^{250}$. Man berechne d und finde die Faktorzerlegung von N.