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

WS 2018/19
20. Nov. 2018

Übungen zur Vorlesung Kryptographie

Blatt 5

Aufgabe 17

Sei $N = pq$ ein RSA-Modul (d.h. $p \neq q$ ungerade Primzahlen) sowie e und 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

$$\lambda(N) := \operatorname{lcm}(p-1, q-1) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$$

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 18

Seien N, p, q, e, d wie in Aufgabe 17 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 $(N, e) := (47383481, 37)$.

---

b.w.

Aufgabe 19

Sei (N, e) der öffentliche Schlüssel eines RSA-Systems und

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

die Verschlüsselungs-Funktion.

a) Man zeige: Der Klartext x kann durch wiederholte Verschlüsselung des Geheimtexts $y = E(x)$ erhalten werden, d.h. es gibt eine positive ganze Zahl m, so dass $E^m(y) = x$. Dabei ist E^m durch vollständige Induktion definiert als $E^1 := E$ und $E^k := E \circ E^{k-1}$ für alle $k > 1$.

b) Man berechne m in den Fällen $(N, e) = (55, 3)$ und $(N, e) = (47383481, 37)$.

Aufgabe 20

Ein Mini-RSA-System mit öffentlichem Schlüssel $(N, e) = (62663, 17)$ werde als Ascii-Bigramm-Verschlüsselung

$$\mathbb{Z}_{256}^2 \to \mathbb{Z}_{256}^2, \quad (a, b) \mapsto (a_1, b_1),$$

benutzt, die wie folgt definiert sei:

$$x := a \cdot 256 + b, \quad y := x^e \bmod N, \quad y = a_1 \cdot 256 + b_1.$$

Der folgende Geheimtext aus 22 Bytes entstand auf diese Weise.

```
B186 E9E9 EF9D 3AD9 44F9 21D4 5B5F E46B 463E 6FD1 D3DF
```

Man finde den Klartext.
