

3. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Alice und Bob haben sich jeweils ein Schlüsselpaar zu einem Public-Key-Kryptosystem erzeugt und sich gegenseitig verschlüsselte Mails zugeschickt. Nun hat Bob seinen privaten Schlüssel verloren. Welche der folgenden Aussagen sind richtig?

- a) Bob kann keine verschlüsselten Mails mehr an Alice senden.
- b) Bob kann zwar noch verschlüsselte Mails an Alice senden, aber Alice kann diese Mails nicht mehr entschlüsseln.
- c) Alice kann keine verschlüsselten Mails mehr an Bob senden.
- d) Alice kann zwar noch verschlüsselte Mails an Bob senden, aber Bob kann diese Mails nicht mehr entschlüsseln.
- e) Bob kann noch alte verschlüsselte Mails, die er von Alice bekommen hatte, entschlüsseln.

Übung 2

Ist zur Bestimmung des \ominus -Inversen zu einem $a \in \mathbb{Z}_p \setminus \{0\}$, p Primzahl, das Ausprobieren (d.h., zu $x = 1, 2, 3, \dots$ wird sukzessive berechnet, ob $1 = a \cdot x \bmod p$ gilt) ein polynomialer Algorithmus?

Übung 3

Was halten Sie von dem folgenden Algorithmus zur Berechnung von $a \bmod m$, $a, m \in \mathbb{N}$?

```
function modulo(a,m)
{
    while (a>=m)
        a:=a-m;
    return a;
}
```

Übung 4

Ein Algorithmus A ruft polynomial oft einen polynomialen Hilfsalgorithmus B auf.

Hat A polynomiale Laufzeit?

Genauer: Bei Inputgröße n ruft A polynomial oft (bzgl. n) den Algorithmus B auf, wiederum mit Inputgröße n .

Übung 5

Berechnen Sie

- a) $5^{32} \bmod 9$.
- b) $11^{27} \bmod 18$.
- c) $8^{120} \bmod 11$.
- d) $7^{16} \bmod 13$.