VI. Public-Key-Kryptographie

Ein bisschen zu den mathematischen Grundlagen findet sich im Kapitel **??**.

VI.1. Definition

FIXME: Definition

VI.2. Sicherheitsbegriff: IND-CCA2-Sicherheit

FIXME: Definition

VI.3. Beispiel: Elgamal

Seien G eine Gruppe mit Erzeuger g, a zufällig.

- öffentlicher Schlüssel von Alice: g^a
- geheimer Schlüssel von Alice: a
- Verschlüsseln einer Nachricht m:
  - wähle b zufällig und berechne g^b
  - verschicke $(g^b, g^{ab} \oplus m)$[1]
- Entschlüsseln eines Chiffrats c: mithilfe von a

VI.4. Beispiel: RSA

Sei $N \in \mathbb{N}$ mit $N = p \cdot q$ für p, q prim. Wähle ein zu $\varphi(N) = (p-1)(q-1)$ teilerfremdes e mit $1 < e < \varphi(N)$ und berechne $d := e^{-1} \mod \varphi(N)$.

- öffentlicher Schlüssel: (e, N)
- geheimer Schlüssel: (d, N)
- Verschlüsseln einer Nachricht m: $c = m^e \mod N$
- Entschlüsseln eines Chiffrats c: $m = c^d \mod N$

VI.4.1. Die RSA-Funktion

Die Funktion $x \mapsto x^e \mod N$ wird auch als RSA-Funktion bezeichnet. Sie ist eine Permutation auf $(\mathbb{Z}/N\mathbb{Z})^\times$.

[1] oder $(g^b, g^{ab} \cdot m)$

VI.4.2. Textbook-RSA

Das oben beschriebene Verfahren wird oft auch als Textbook-RSA bezeichnet. Es ist nicht sicher, da gleiche Klartexte immer auf gleiche Chiffrate abgebildet werden.

Beispiel Auktionsangriff

FIXME: Bild Auktionsangriff, S. 20

VI.4.3. RSA-ES-OAEP

Hier kommt bei der Berechnung des Chiffrats eine Zufallszahl r ins Spiel: $c = ((m+h(r))\|(h(m+h(r))+r))^e$. Zur Entschlüsselung bilde zunächst c^d. Dann hashe den ersten Teil der Nachricht, um durch Addieren des Hashs zum zweiten Teil der Nachricht den Zufall zu bekommen. Nun kann die eigentliche Nachricht berechnet werden.

Sicherheit

RSA-ES-OAEP ist beweisbar sicher im Random Oracle Model: Ein Angreifer, der das IND-CCA2-Spiel gewinnt, kann benutzt werden, um die RSA-Funktion zu invertieren.