Einführung in die Kryptographie

Ulm, 27. 4. 2006

Was ist Kryptographie?

Kryptographie (oder Kryptologie) ist die Lehre von der *Datenverschlüsselung*.

Funktionen/Anwendungen:

- *Vertraulichkeit:* Austausch von vertraulichen Nachrichten
- Feststellen der *Identität* des Absenders bzw. der *Authentizität* einer Nachricht
- Feststellen der *Integrität* einer Nachricht
- *Zurechenbarkeit:* digitale Unterschrift
- *secret sharing*
- *zero knowledge proofs*

Was hat das mit Mathematik zu tun?

- Um die Sicherheit von kryptographischen Verfahren zu studieren, benutzt man Modelle aus der Wahrscheinlichkeits- und Komplexitätstheorie.

- Viele moderne Verschlüsselungsverfahren benutzen Methoden/Probleme der reinen Mathematik, insbesondere der Zahlentheorie.

Beispiel RSA: Die Sicherheit dieses Kryptoverfahrens beruht darauf, dass es 'schwierig' ist, grosse Zahlen in Primfaktoren zu zerlegen, z.B.

$$\begin{aligned} n &= 175817500179734793997558115 11 \\ &= p \cdot q, \end{aligned}$$

wobei

$$\begin{aligned} p &= 187363542873697, \\ q &= 93837625763863. \end{aligned}$$

Verschlüsselungsverfahren

Ein Verschüsselungsverfahren (Kryptosystem) besteht aus:

- *Klartextraum* $\mathcal{P}$ ($p \in \mathcal{P}$: *Klartexte*)
- *Chiffretextraum* $\mathcal{C}$ ($c \in \mathcal{C}$: *Chiffretexte*)
- *Schlüsselraum* $\mathcal{K}$ ($k \in \mathcal{K}$: *Schlüssel*)
- *Verschlüsselungsfunktionen*

$$\mathcal{E} = \{ E_k : \mathcal{P} \to \mathcal{C} \mid k \in \mathcal{K} \}$$

- *Entschlüsselungsfunktionen*

$$\mathcal{D} = \{ D_k : \mathcal{C} \to \mathcal{P} \mid k \in \mathcal{K} \}$$

Für jedes $e \in \mathcal{K}$ gibt es ein $d \in \mathcal{K}$ so, dass $\forall p \in \mathcal{P}$:

$$D_d(E_e(p)) = p.$$

Austausch einer vertraulichen Nachricht

- Alice möchte eine vertrauliche Nachricht $p \in \mathcal{P}$ an Bob schicken. Sie benutzt einen (geheimen) Verschlüsselungsschlüssel $e \in \mathcal{K}$ und berechnet:

  $$c := E_e(p).$$

  Sie sendet den Chiffretext c an Bob.

- Bob kennt den nötigen Entschlüsselungsschüssel $d \in \mathcal{K}$ und berechnet die vertrauliche Nachricht p durch:

  $$p := D_d(c).$$

- Eve kann die von Alice und Bob benutzte Leitung abhören und kennt deshalb den Chiffretext c. Ist das Kryptoverfahren sicher, so kann Eve aus der Kenntnis von c nichts über die Nachricht p oder die Schlüssel e, d erfahren.

(A)symmetrische Kryptosysteme

Wir unterscheiden zwischen zwei Arten von Kryptosystememem:

- *Symmetrische* oder *Private-Key-Verfahren*: der Entschlüsselungsschlüssel d ist aus dem Verschlüsselungsschlüssel e leicht zu berechnen (z.B. $e = d$).

  In diesem Fall müssen Alice und Bob vor Beginn der Kommunikation den geheimen Schlüssel e über eine sichere Leitung ausgetauscht haben.

- *Asymmetrische* oder *Public-Key-Verfahren*: der Entschlüsselungsschlüssel d ist aus dem Verschlüsselungsschlüssel e nicht mit vertretbarem Aufwand zu berechnen.

  Bei so einem Verfahren benötigt man keine sichere Leitung!

Öffentliche und private Schlüssel

- Bob wählt das Schlüsselpaar (e, d). Er sendet den *öffentlichen Schlüssel* e an Alice.

- Alice verschlüsselt die Nachricht p mit dem Schüssel e:

  $$c := E_e(p),$$

  und sendet den Chiffretext c an Bob.

- Bob entschlüsselt den Chiffretext c mit dem *privaten Schlüssel* d:

  $$p := D_d(c).$$

- Eve kennt den Chiffretext c und den öffentlichen Schlüssel e. Ist das Verfahren sicher, so kann sie daraus weder auf d noch auf p Rückschlüsse ziehen.

Die Verschiebungschiffre

Ein historisches (?) Beispiel (Julius Cäsar, ca. 50 v.Chr.):

- Klartext-, Chiffretext- und Schlüsselraum sind identisch:

$$\Sigma = \{A, B, \ldots, Z\} \cong \{0, 1, \ldots, 25\}.$$

- Verschlüsselungsfunktion E_e:

$$E_e : \Sigma \to \Sigma, \quad x \mapsto (x + e) \pmod{26}.$$

- Entschlüsselungsfunktion D_e:

$$D_e : \Sigma \to \Sigma, \quad x \mapsto (x - e) \pmod{26}.$$

Durch Iterieren erhält man ein Kryptosystem, dessen Klar- und Chiffretexte beliebige Zeichenketten $(w_1, w_2, \ldots)$, $w_i \in \Sigma$, sind.

Die Schwächen der Verschiebungschiffre

- Die Schüsselmenge ist zu klein: man kann ohne grossen Aufwand alle Möglichkeiten durchprobieren.

- Die statistischen Eigenschaften eines typischen Klartextes werden durch die Verschlüsselungsfunktion nicht verschleiert. Deshalb kann man eine Nachricht leicht durch eine Häufigkeitsanalyse entschlüsseln.

- Kennt man ein einziges Klartext-Chiffretext-Paar, so kennt man auch den verwendeten Schlüssel.