Kryptographie – Eine Einführung

Jan Tobias Mühlberg
<muehlber@fh-brandenburg.de>

Gliederung

1. Motivation
2. Die Ziele der Kryptographie
3. Kryptographische Verfahren
   - Geschichtliches
   - Modernes
4. Zur Sicherheit kryptographischer Verfahren

Motivation – Problemstellung

- ungeschützter Transport von E-Mails über das Internet
- mehrfache Zwischenspeicherung
- gesetzliche Regelungen können Anbieter zwingen, E-Mails zu archivieren

Motivation – Lösungsansatz

- Kryptographie:
  - Absender und Adressat tauschen einen geheimen „Schlüssel“ aus
  - der Absender verschlüsselt eine E-Mail mit diesem Schlüssel und versendet sie
  - nur der Empfänger kann sie entschlüsseln

Motivation – Warum es nicht so einfach ist!

- Kann ein Angreifer nicht einfach alle denkbaren Schlüssel durchprobieren?
- Wie sicher ist das alles? Kann man sich überhaupt darauf verlassen?
- Wie kann man einen geheinen Schlüssel sicher austauschen?

Die Ziele der Kryptographie

- **Vertraulichkeit** – Eine Nachricht soll nur von den Adressaten gelesen werden können.
- **Authentizität** – Der Ursprung einer Nachricht soll zweifelsfrei nachweisbar sein.
- **Integrität** – Die Nachricht soll den Empfänger nachweisbar korrekt und unmanipuliert erreichen.

Kryptographische Verfahren

- Verschlüsselungsverfahren transformieren einen allgemein lesbaren **Klartext** in einen, für nicht Eingeweihte unlesbaren **Geheimtext**.
- Da Computer intern alles, auch Text, als eine Folge von Zahlen darstellen, sind moderne kryptographische Verfahren nicht mehr als **Rechenvorschriften**.

Kryptographische Verfahren

- Die Verfahren benutzt für die Umwandlung von Klar- in Geheimtext und wieder zurück ein **Schlüssel**, der wiederum auch nur eine Menge von Zeichen ist.

Caesar Chiffre

Klartext:	a	b	c	d	e	f	g	h	i	j	k	l	m
Geheimtext:	D	E	F	G	H	I	J	K	L	M	N	O	P
Klartext:	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ein Beispiel:

DQJULIILPPRUJHQJUDXHQ ≈ angriffimmorgengrauen

Moderne Verfahren

- **asymmetrische** Verfahren
- große Schlüssellängen erschweren das Ausprobieren aller Möglichkeiten
- jeder Teilnehmer besitzt ein Schlüsselpaar, einen **öffentlichen** und einen **privaten Schlüssel**
- **öffentliche Schlüssel** werden frei zugänglich hinterlegt

Moderne Verfahren

- **private Schlüssel** werden um jeden Preis geheimgehalten
- Nachrichten die mit dem **öffentlichen Schlüssel verschlüsselt** sind, können man nur mit dem zugehörigen **privaten Schlüssel entschlüsselt** werden, und umgekehrt.

Verschlüsseln

- eine Nachricht wird vom Absender mit dem **öffentlichen Schlüssel des Empfängers** verschlüsselt
- sie kann damit nur vom Adressaten, der den zugehörigen privaten Schlüssel besitzt, gelesen werden

Signieren

- eine Nachricht wird vom Absender mit seinem **eigenen privaten Schlüssel** verschlüsselt
- sie kann damit von jedem entschlüsselt werden. . .

Zur Sicherheit

- das Durchprobieren aller möglichen Schlüssel ist auch mit den schnellsten Computern kaum möglich
- ganz wichtig: gute Passworte verwenden
- ganz wichtig: konsequent sein und wichtige Daten nie unverschlüsselt herumliegen lassen