Sicherheit im Internet

Digitale Signatur
Beispielprogramm

Dr.sc.nat.
Michael J.M. Wagner
http://www.wagnertech.de

Inhalt

- Motivation
- Voraussetzung
- Funktionsprinzip
- Einsatz
- Zertifizierungsstellen
- Demo
- Literatur

- Zusammenfassung in der Notizansicht

Motivation

e-mail-Verkehr:

- Nicht „abhörsicher“ -> Verschlüsselung
- Keine Authentizität des Absenders
- Keine Integrität des Inhalts

-----> Digitale Signatur

Voraussetzung (1)

- Asymmetrische Schlüssel
  - RSA - Verfahren:
    - Primzahlprodukt n: 47 * 71 = 3337
    - Privater Schlüssel e: 79
    - Öffentlicher Schlüssel d: 1019
    - Verschlüsselung: $c = m^e \pmod n$
    - Entschlüsselung: $m = c^d \pmod n$

- Herleitung Notizansicht

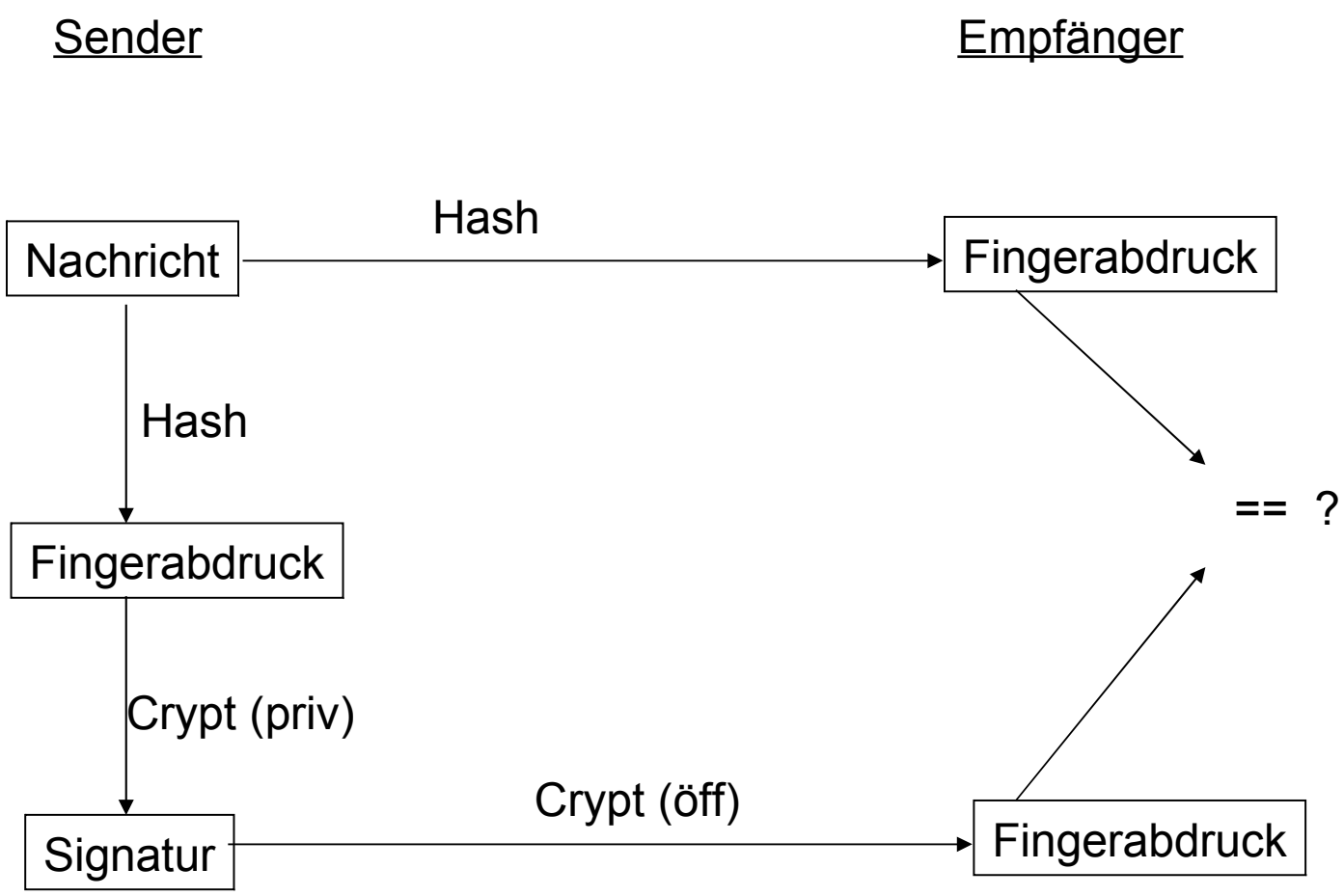
Voraussetzung (2)

- Hash - Funktuion
  - „kollisionsfrei“
  - 160 Bit Länge
- erzeugt aus der Nachricht einen charakte-ristischen, kompakten Fingerabdruck

Voraussetzung (3)

- Zertifikat
  - bestätigt Absender - Schlüssel - Beziehung
  - Name des Schlüsselinhabers
  - öffentlicher Schlüssel
  - Hinweise zu den Algorithmen
  - Laufende Nummer, Gültigkeitsdatum
  - Signatur des Ausstellers

Funktionsprinzip



Beschreibung s. Notizansicht

Einsatz

- Privater Schlüssel + Algorithmus auf Chipkarte
  - von SigG gefordert
  - Kartenleser nötig
  - z.B. Public Key Service (DTAG)
- Pretty Good Privacy
  - Quasi-Standard
  - in viele e-mail-Programme integriert

Zertifizierungsstellen

- DTAG (PKS)
- Heise-Verlag (PGP)
- DFN (PEM, X.509, PGP)
- TC Trust Center (X.509, PGP)

Demo

- Voraussetzung:
  - Java Virtual Machine
- Werkzeuge:
  - Hash.class (Beschreibung s. folgende Folien)
  - Crypt.class (Beschreibung s. folgende Folien)
  - Zertifikat
- Anleitung
  - siehe Notizen zu dieser Folie

Hash.java

- Einfacher Hash-Algorithmus:
  - Addition der ASCII-Repräsentation jedes Zeichens
  - Modolo des auch für die Verschlüsselung verwendeten Schwellwertes n
- Aufruf:

  Hash <n> < <Nachricht>
- Anmerkung: Diese Hash-Funktion ist nicht kollisionsfrei (Zahlendreher)

- Code in der Notizansicht

Crypt.java

- Implementiert die Funktion
  $x^e \bmod n$
- Aufruf:

  Crypt <x> <e> <n>

- Code in der Notizansicht

Literatur

- Bitzer, Brisch „Digitale Signatur“, Springer 1999
- X.509: Standard zur Erstellung von Zertifikaten
- Rivest, Shamir, Adleman „A Method for Obtaining Digital Signatures and Public Key Cryptosystems“, Comm.ACM 21/2 (1978)
- Schneier „Angewandte Kryptographie“, Addison-Wesley 1996