Überblick Kryptographie

Ulrich Kühn

Deutsche Telekom Laboratories, TU Berlin

Seminar Kryptographie

19. Oktober 2005

Übersicht

Was ist Kryptographie?

Symmetrische Kryptographie

Asymmetrische Kryptographie

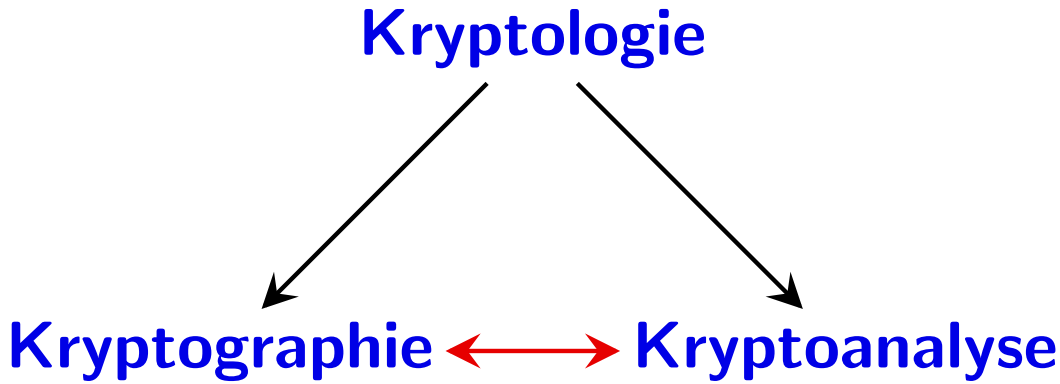
Beispiele für asymmetrische Verfahren

PKI

Identitätsbasierte Kryptographie

Was ist Kryptographie?

Zwei Seiten einer Medallie:



Häufig Kryptographie := Kryptologie.

Wichtig: Interaktion Kryptographie – Kryptoanalyse.

Geschichte

Seit der Antike: Unsystematischer Einsatz (u.a. Cäsar). Mehr "Black Art", weniger Wissenschaft,

ab Ende 19. Jh: Systematisierung

2. Weltkrieg: Brechen der deutschen und japanische Chiffriermaschinen durch polnische, britische, amerikanische Wissenschaftler, massiver Maschineneinsatz.

70er Jahre: DES, Public-Key Kryptographie

Seitdem: "Öffentliche" Wissenschaft, breiter Einsatz: Mobiltelefonie, Banken / Geldautomaten, Internet, e-Commerce, ...

Ziele beim Einsatz von Kryptographie

- Geheimhaltung von Information
  - "Ich sehe was, was Du nicht siehst"
  - Klassisches Einsatzgebiet der Kryptographie, meist bei Militär, Diplomaten, Geheimdiensten
- Integrität von Daten
  - "Ich bin sicher, dass die Daten nicht verändert wurden"
  - Eingesetzt z.B. im Bankenbereich
- Authentizität von Kommunikationspartnern
  - "Ich weiss, dass Du es bist"
- ...

Konzepte in der Kryptographie

- Bedrohungsmodelle
  $\longrightarrow$ Welche Angreifer, welche Möglichkeiten / Freiheiten?
- Kryptographische Primitive: Symmetrisch / Asymmetrisch
  $\longrightarrow$ Blockchiffren, Stromchiffren, MACs, ...
  $\longrightarrow$ Public-key Verschlüsselung, Signaturverfahren, ...
  $\longrightarrow$ Kryptographische Hashfunktionen
- Kryptographische Protokolle:
  $\longrightarrow$ Zero-Knowledge Protokolle
  $\longrightarrow$ Multiparty Computation

Prinzip von Kerckhoffs

Auguste Kerckhoffs (1835–1903) zur Sicherheit von Kryptoverfahren:

- Das System muss praktisch, wenn nicht gar mathematisch, unbrechbar sein.
- Das System selbst darf nicht geheim sein, darf keine Probleme verursachen, wenn es dem Feind bekannt wird.
- Es muß einfach sein, den Schlüssel ohne Aufzeichnungen zu übertragen [...], sowie bei verschiedenen Parteien zu ändern.
- [...]

Claude Shannon (1916–2001) "Der Feind kennt das System".

Symmetrische Verschlüsselungsverfahren

Definition:

- Klartextmenge M, Chiffretextmenge C, Schlüsselmenge K
- Effizient berechenbare (randomisierte) Algorithmen

  (Schüsselgenerator $\mathcal{G} : \ldots \rightarrow K$,)
  Verschlüsselungsalgorithmus $\mathcal{E} : K \times M \rightarrow C$,
  Entschlüsselungalgorithmus $\mathcal{D} : K \times C \rightarrow M$

  und Konsistenzbedingung

$$\forall m \in M, k \leftarrow \mathcal{G}() : m = \mathcal{D}(k, \mathcal{E}(k, m)).$$

Beispiele für Symmetrische Primitive

Blockchiffren:

- DES, $M = C = \{0,1\}^{64}, K = \{0,1\}^{56}$
- AES, $M = C = \{0,1\}^{128}, \log_2(|K|) \in \{128, 192, 256\}$

Stromchiffren:

- RC4, $M = C = (\{0,1\}^8)^*, K = \bigcup_{N=1}^{256} \{0,1\}^{8N}$
- GSM-Verschlüsselung (Luftschnittstelle)
- (Blockchiffre mit Betriebsmodus)

Symmetrisch vs. Asymmetrisch

Symmetrische Kryptographie:

- Ein Schlüssel zum Ver- und Entschlüsseln
- Jeder Teilnehmer einer Kommunikationsbeziehung kennt diesen einen Schlüssel
- Schlüsselverteilung schwierig, Geheimhaltung!

Asymmetrische Kryptographie:

- Schlüsselpaar (PK, SK), getrennt für Ver- und Entschlüsselung
- SK kann aus PK nicht effizient berechnet werden
- PK öffentlich, Verteilung "nur" authentisch $\longrightarrow$ PKI.

Asymmetrische Kryptographie

- Verschlüsselung
  - Verschlüsselung mit PK
  - Entschlüsselung mit SK
- Digitale Signaturen
  - Signatur mit SK
  - Verifikation mit PK
- Nutzbar sind Falltür-Einwegfunktionen:
  - Leicht berechenbar
  - Schwer umkehrbar
  - Leicht umkehrbar mit Zusatzinformation
- Welche Funktionen eignen sich?

Asymmetrische Kryptographie (2)

Kandidaten:

- Zahlentheoretische Probleme
  - Faktorisierung vs. Multiplikation in $\mathbb{Z}$
  - Exponentierung vs. DLP
    - in $(\mathbb{Z}_p^\times, *)$ bzw. Untergruppen
    - Punktgruppe von elliptischen Kurven
- Quadratische Gleichungssysteme in vielen Variablen
  $\longrightarrow$ multivariate Kryptographie
- Codes $\longrightarrow$ Code-basierte Kryptographie
- ...

Beispiel: RSA

Verfahren von Rivest, Shamir, Adleman:

- Beruht auf Schwierigkeit, große Zahlen zu faktorisieren ?
- p, q große Primzahlen

$$\begin{aligned} N &= pq \\ e &: (e, \phi(N)) = 1 \\ d &: ed \equiv 1 \pmod{\phi(N)} \end{aligned}$$

- $PK = (N, e)$
- $SK = (N, d, p, q, \dots)$

Beispiel: RSA (2)

Funktionsweise:

- Verschlüsselungsverfahren:
  - Verschlüsseln: $c = m^e \bmod N$
  - Entschlüsseln: $m' = c^d \bmod N$
- Signaturverfahren:
  - Paddingverfahren $\mu(.)$
  - Signieren: $s = \mu(m)^d \bmod N$
  - Verifizieren: $t = s^e \bmod N$, $\mu^{-1}(t) \stackrel{?}{=} m$
- Homomorphieeigenschaft
  $\longrightarrow$ Angriffe, $\longrightarrow$ Anonymität bei E-Cash

Beispiel: ElGamal

ElGamal-Verfahren:

- Systemparameter $H = (\mathbb{Z}_p^\times, *)$, $G =< g >\subset H$ mit $q = |G|$ prim
- $SK : x \leftarrow_R \{1, \ldots, q-1\}$, $PK : y = g^x$

Funktionsweise:

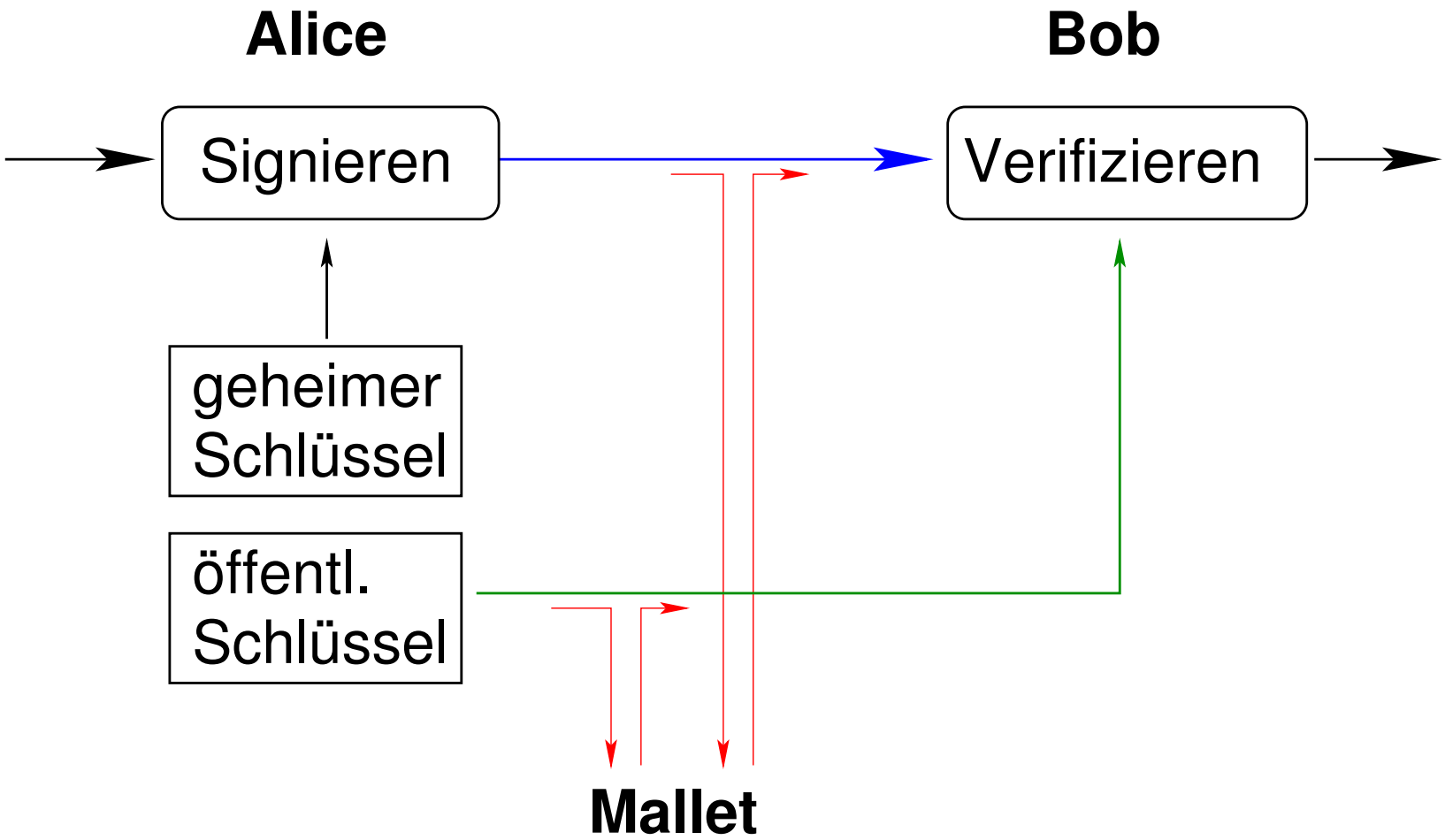
- Verschlüsselungsverfahren:
  - Verschlüsseln: $k \leftarrow_R \{1, \ldots, q-1\}, r = g^k, s = y^k m$ $\rightarrow c = (r, s)$
  - Entschlüsseln: geg. $c = (r, s) : m' = (r^x)^{-1} s$
  - Padding nötig wg. Multiplikativität
- Signaturverfahren existiert, aber unüblich
  - Variante Digital Signature Algorithm ▸ DSA

Beispiel: ElGamal (2)

Sicherheit

- Sicherheit beruht auf Diffie-Hellman-Entscheidungsproblem:
  geg. g^a, g^b, g^c, gilt $g^{ab} = g^c$?
  $\longrightarrow$ Computational Diffie-Hellman Problem
  $\longrightarrow$ Discrete Logarithm Problem
- Sicherheit gg. Chosen-Plaintext-Angriff
- Unsicher in $(\mathbb{Z}_N, +)$, $G = (\mathbb{Z}_p^\times, *)$
- Interessant: Punktgruppe elliptischer Kurven über $\mathrm{GF}(p), \mathrm{GF}(2^p)$

Public Key Infrastructure: Angriffsmodell



Signieren $\leftrightarrow$ Entschlüsseln

Verifizieren $\leftrightarrow$ Verschlüsseln

Public Key Infrastructure

Problem

Öffentlicher Schlüssel muss authentisch zum Partner übermittelt werden $\longrightarrow$ *Man-in-the-Middle-Angriff*
Alternative Formulierung: Sicherstellung der authentischen Zuordnung zwischen Identität I *und* PK_I.

Lösung

Zertifikat bestätigt Zuordnung: Signierung von (I, PK_I) durch vertrauenswürdige Einrichtung (CA).

- Verlagert Problem eine Ebene höher !?
- Aber: Wenige CAs + Schlüssel $\longrightarrow$ Vertrauensanker
- "Public Key Infrastructure"

Public Key Infrastructure: Beispiele

Beispiele:

- Signaturgesetz bzw. EU-Richtlinie
  $\longrightarrow$ Zweistufige Hierarchie
- Web $\longrightarrow$ Serverzertifikate, (https://...)
- Firmeninterne PKI $\longrightarrow$ meist für interne Anwendungen
- Gesundheitswesen $\longrightarrow$ Heilberufeausweis, eGK, etc.

Aber:

- Aufwendige Prozesse
- Certificate Revocation "Ist das Zertifikat noch aktuell?"
  $\longrightarrow$ Last der Prüfung beim Kommunikationspartner

Identitätsbasierte Kryptographie

Alternativen?

PKI nötig für Zuordnung von Identität und Schlüssel. Geht es auch anders?

Identitätsbasierte Kryptographie:

- Identität (z.B. Name, Email-Adresse) direkt als Schlüssel
- Basiert auf Idee von Shamir (1984)
- Geheimer Schlüssel hängt von Identität und Systemparametern ab $\longrightarrow$ Private Key Generator nötig

Identitätsbasierte Kryptographie (2)

Identitätsbasierte Kryptosysteme:

- **Setup:** Erzeugt Systemparameter P und Master Secret für Private Key Generator PKG
- **Extract:** PKG liefert zu Identität I einen geheimen Schlüssel SK_I.
- **Encrypt / Verify:** Nutzt P und Identität I des Empfängers / Signieres als öffentlichen Schlüssel.
- **Decrypt / Sign:** Nutzt SK_I zum Entschlüsseln / Signieren einer Nachricht.

Identitätsbasierte Kryptographie (3)

Beispiele:

- Boneh-Franklin: Verschlüsselungssystem
  - Weil-Paarung auf elliptischen Kurven als bilineare Abbildung
- Signaturverfahren: (Shamir), Hess
- Hierarchische Systeme: Gentry-Silverberg

Varianten: Paarungs-basierte Verfahren

- Certificate-based Cryptography
- Certificate-less Cryptography

Weitere Themengebiete in der Kryptologie

- Kryptographische Hashfunktionen
  $\longrightarrow$ Kollisionsresistenz, (2-te) Urbilder schwer zu finden
  $\longrightarrow$ Idealisiert als zufällige Funktionen
- Betriebsmodi (Modes of Operation) von Blockchiffren
- Message Authentication Codes
- Kryptographische Protokolle, z.B.
  - Schlüsselaustausch / -transport
  - Zero-Knowledge
  - Multiparty computation
  - Wahlprotokolle
- Kryptoanalyse

Appendix

Beispiel: DSA

Digital Signature Algorithm:

- q prim, 160 bit, p prim mit $p = qz + 1$, 1024 bit.
- Wähle h mit $g = h^z \bmod p \neq 1$
- $SK : x \leftarrow_R \mathbb{Z}_q \setminus \{0\}$, $PK : (p, q, g, y = g^x)$

Funktionsweise:

- Signieren:
  - $k \leftarrow_R \mathbb{Z}^{\times}_{q-1}$, $r = (g^k \bmod p) \bmod q$
  - $s = (k^{-1}(H(m) + xr)) \bmod q$.
  - Signatur ist (r, s)
- Verifizieren:
  - $w = s^{-1} \bmod q$, $u_1 = H(m)w \bmod q$, $u_2 = rw \bmod q$.
  - $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$.
  - Gültig, falls $v = r$.

◂ ElGamal