

# Sicherheit in mobilen Netzen

Vaida Klimmek

14. Dezember 2004

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- Sicherheit in GSM-Netzen
- Sicherheit in Wireless LANs
- Sicherheit in anderen mobilen Netzen
- Fazit

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- Sicherheit in GSM-Netzen
- Sicherheit in Wireless LANs
- Sicherheit in anderen mobilen Netzen
- Fazit

# Bedeutung der Sicherheit

---

**Was ist Sicherheit?**

# Bedeutung der Sicherheit

---



# Bedeutung der Sicherheit

---

## Sicherheit in Kommunikationsnetzwerken:

- Schutz der Privatsphäre.
- Schutz gegen unberechtigten Zugang.
- Schutz gegen Mißbrauch von Daten.
- Bildung des Vertrauens.

# Bedeutung der Sicherheit

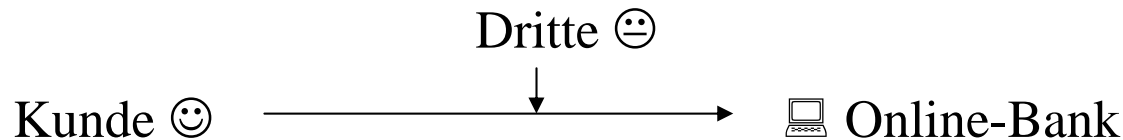
---

## Sicherheitsziele:

- Vertraulichkeit
- Authentifizierung
- Autorisierung
- Integrität
- Nicht-Anfechtbarkeit
- Zugriffssteuerung
- Verfügbarkeit

# Bedeutung der Sicherheit

Ziel: Banküberweisung über Mobiltelefon



**Authentizität:** Ist die Bank wirklich meine Bank? Ist der Kunde wirklich der richtige Kunde?

**Integrität:** Wird der Inhalt der Überweisung richtig übertragen?

**Vertraulichkeit:** Wurde die Übertragung nicht vom Dritten mitgehört?

**Nicht-Anfechtbarkeit:** Kann die Bank den Erhalt der Überweisung leugnen?

**Zugriffssteuerung:** Kann der Dritte auf das Online-Banking System zugreifen?

**Verfügbarkeit:** Ist das System im vereinbarten Zeitraum zugreifbar?

# Bedeutung der Sicherheit

---

## Typische Gefahrenquellen:

- Menschliche Fehler: Preisgabe von Passwörtern
- Programme mit Schadfunktionen: Viren, Würmer, Trojaner...
- Spoofing: Angriff auf Authentifizierung durch Vortäuschen falscher Identität.
- Denial-of-Service-Angriffe (DoS): Angriff auf Verfügbarkeit durch Einspielen von Nachrichten mit dem Ziel der serverseitigen Überlastung.

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- Sicherheit in GSM-Netzen
- Sicherheit in Wireless LANs
- Sicherheit in anderen mobilen Netzen
- Fazit

# Grundlagen der Kryptografie

---

- Einführung in die Kryptografie
- Symmetrische Verschlüsselung
- Public-Key-Verfahren
- Hashfunktionen
- Authentifizierung, Signierung und Zertifikate

# Grundlagen der Kryptografie

---

- Einführung in die Kryptografie
- Symmetrische Verschlüsselung
- Public-Key-Verfahren
- Hashfunktionen
- Authentifizierung, Signierung und Zertifikate

# Einführung in die Kryptografie

---

Begriffe von Kryptografie und Kryptologie:

„Beide bezeichnen die Kunst und die Wissenschaft, die sich damit beschäftigt, Methoden zur Verheimlichung von Nachrichten zu entwickeln.“

Man unterscheidet zwischen

„**Kryptografie**, der Wissenschaft von der Entwicklung von Kryptosystemen, **Kryptoanalyse**, der Kunst diese zu brechen und [...] **Kryptologie** die Gesamtheit dieser Wissenschaften.“<sup>2</sup>

# Einführung in die Kryptografie

---

**Verschlüsselung** ist der wesentliche Teil der Kryptografie.

Im Bezug auf Schlüssel unterscheidet man:

- *symmetrische* Verschlüsselung (secret key Verfahren)
- *asymmetrische* Verschlüsselung (public key Verfahren)

Wichtigste Angriffsarten:

- Man-in-the-Middle-Angriff
- Brute-force-Angriff

# Grundlagen der Kryptografie

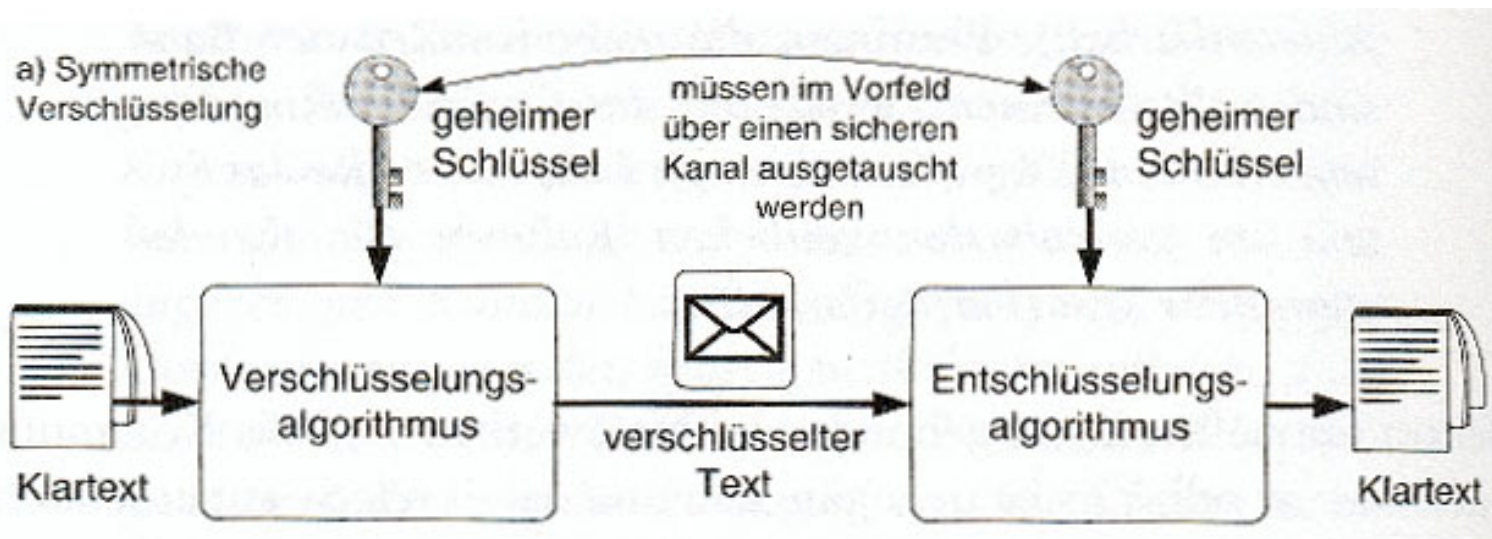
---

- Einführung in die Kryptografie
- Symmetrische Verschlüsselung
- Public-Key-Verfahren
- Hashfunktionen
- Authentifizierung, Signierung und Zertifikate

# Symmetrische Verschlüsselung

Merkmale:

- Gleicher Schlüssel zwischen beiden Kommunikationspartnern.
- Gleicher Schlüssel zum Chiffrieren und Dechiffrieren.



# Symmetrische Verschlüsselung

---

## Nachteile:

- Der Schlüssel muss noch vor der Sitzung übertragen werden.
- Der Schlüssel muss über einen sicheren Kanal übertragen werden (zeitaufwendig).
- Der Schlüssel muss geheim bleiben.
- Keine spontane Kommunikation möglich.

# Symmetrische Verschlüsselung

---

Bekannteste symmetrische  
Verschlüsselungsverfahren:

- DES (Data Encryption Standard)
- TDEA (Triple Data Encryption Algorithmus)
- AES (Advanced Encryption Standard)

# Symmetrische Verschlüsselung

---

## DES (Data Encryption Standard)

- 1977 von IBM entwickelt
- der erste publizierte Algorithmus
- Blockchiffrierung mit 64 Bit Blocklänge und 56 Bit Schlüssel

## Nachteil:

- Zu kurzer Schlüssel -> Brute-Force-Angriffe

# Symmetrische Verschlüsselung

---

## TDEA (Triple Data Encryption Algorithmus)

- 1979 entwickelt
- Als Nachfolger von DES gegen Brute-Force-Angriffe
- Dreifache Anwendung des DES Algorithmus
- 168 Bit Schlüssellänge

# Symmetrische Verschlüsselung

---

## AES (Advanced Encryption Standard)

- Im Jahr 2000 entwickelt von Rijndael.
- Gewinner einer Ausschreibung im Jahr 1997

### Folgende Kriterien sollten erfüllt werden:

- mindestens 20 Jahre Sicherheit
- mindestens 128 Bit Schlüssellänge
- einfach implementierbar
- Open Source

### Vorteile:

- Mögliche Blocklänge 128, 160, 192, 224 und 256 Bit.
- Mögliche Schlüssellänge: 128, 192 und 256 Bit.

# Grundlagen der Kryptografie

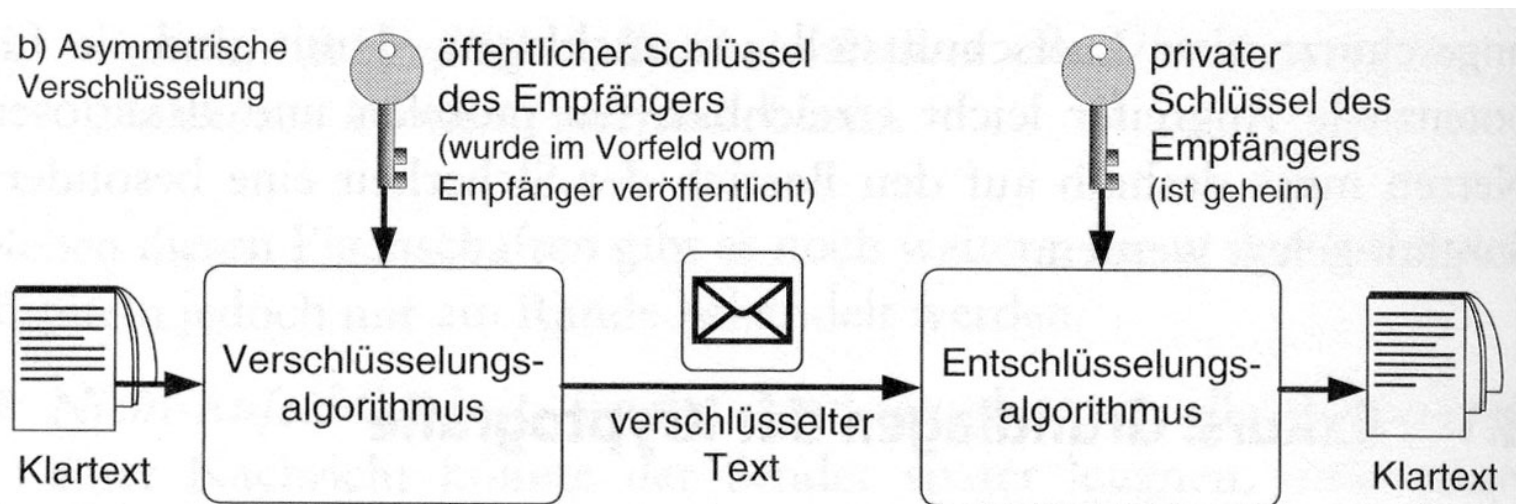
---

- Einführung in die Kryptografie
- Symmetrische Verschlüsselung
- **Public-Key-Verfahren**
- Hashfunktionen
- Authentifizierung, Signierung und Zertifikate

# Public-Key-Verfahren

## Merkmale:

- Unterschiedliche Chiffrier- und Dechiffrierschlüssel
- Geheimer (privater) Dechiffrierschlüssel
- Öffentlicher (public) Chiffrierschlüssel



# Public-Key-Verfahren

---

## Vorteile:

- Der Schlüssel muss nicht vor der Sitzung übertragen werden.
- Der Schlüssel muss nicht über einen sicheren Kanal übertragen werden.
- Nur privater Schlüssel muss geheim bleiben.  
Öffentlicher Schlüssel für Entschlüsselung nutzlos.
- Spontane Kommunikation möglich.

# Public-Key-Verfahren

---

Das bekannteste asymmetrische  
Verschlüsselungsverfahren:

- RSA
- Diffie-Helman-Schlüsselaustausch

# Public-Key-Verfahren

---

## RSA

- Im Jahr 1978 entwickelt
- Benannt nach den Erfindern Rivest, Shamir und Adleman

## Vorteile von RSA:

- Bei großen Primzahlen  $p$  und  $q$  können Brute-Force-Angriffe vermieden werden.
- Sicherer Schlüssel mit 1024 Bit Längen.

## Nachteile:

- Große Schlüssellänge  $\rightarrow$  lange Rechenzeit.
- Langsam im Vergleich mit symmetrischen Verfahren.

# Public-Key-Verfahren

---

## Diffie-Hellmann-Schlüsselaustausch

- 1976 veröffentlicht
- Verbindet symmetrische und asymmetrische Algorithmen
- Schlüsselaustausch mit asymmetrischem Verfahren
- Verschlüsselung mit symmetrischem Verfahren
- Schutz gegen Brute-Force-Angriffe

# Grundlagen der Kryptografie

---

- Einführung in die Kryptografie
- Symmetrische Verschlüsselung
- Public-Key-Verfahren
- **Hashfunktionen**
- Authentifizierung, Signierung und Zertifikate

# Hashfunktionen

---

Hashfunktionen bilden beliebig lange Daten auf einen vorgegebenen kurzen Wert ab.

Folgende Kriterien müssen erfüllt werden:

- Einfache Hashwertberechnung  $h = H(x)$ .
- Aus  $h$  ist praktisch unmöglich ursprüngliche Nachricht zu berechnen.
- Kein gleicher Hashwert bei mehreren Eingaben

# Hashfunktionen

---

## Bekannteste Verfahren:

- SHA-1: von NSA entwickelt.
- MD5: von Rivest entwickelt.

# Grundlagen der Kryptografie

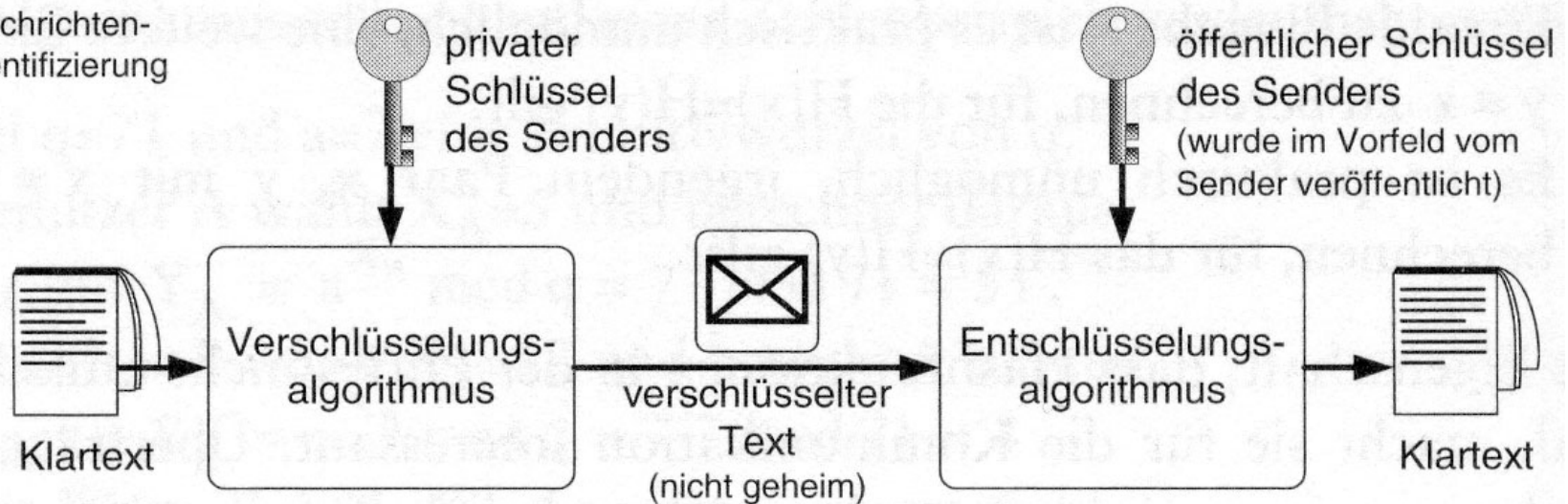
---

- Einführung in die Kryptografie
- Symmetrische Verschlüsselung
- Public-Key-Verfahren
- Hashfunktionen
- Authentifizierung, Signierung und Zertifikate

# Authentifizierung

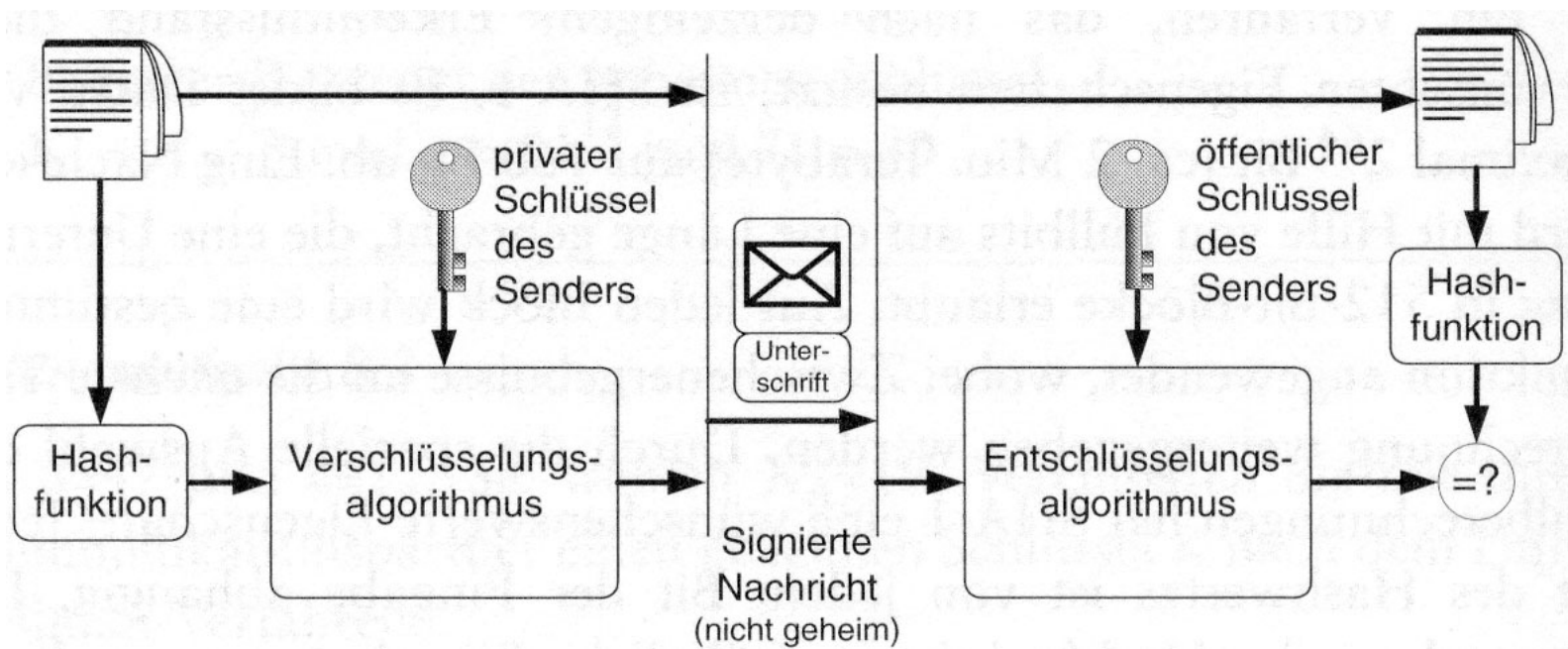
Asymmetrische Verfahren werden zur Authentifizierung eingesetzt.

a) Nachrichten-  
authentifizierung



# Signierung

Signierung (auch digitale Unterschrift genannt)  
basiert auf Verfahren der Authentifizierung.



# Zertifikate

---

Zertifizierungsstellen verwalten den öffentlichen Schlüssel.

Zertifikat enthält folgende Daten:

- Identität der Person
- Identität der Zertifizierungsstelle
- Datumsbereich der Gültigkeit
- Öffentlichen Schlüssel der Person
- digitale Unterschrift der Zertifizierungsstelle

Signaturgesetz SigG im Jahr 2001 regelt die Aufgaben der Zertifizierungsstellen und Inhalt der Zertifikate.

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- **Sicherheit in GSM-Netzen**
- Sicherheit in Wireless LANs
- Sicherheit in anderen mobilen Netzen
- Fazit

# Sicherheit in GSM-Netzen

---

- Authentifizierung
- Verschlüsselung
- Sicherheit und Roaming
- Anonymität
- Kritik am Sicherheitskonzept

# Sicherheit in GSM-Netzen

---

Folgende Sicherheitsziele werden verfolgt:

- Schutz vor nicht autorisiertem Telefonieren.
- Schutz vor dem Abhören einer Sprach- oder Datenverbindung.
- Schutz vor der Bestimmung des Aufenthaltsortes des Teilnehmers

# Sicherheit in GSM-Netzen

---

Wichtige Bestandteile des Sicherheitskonzeptes:

- Kryptografische Funktionen A3, A5 und A8
- Authentifikationsschlüssel  $K_i$
- Verschlüsselungsschlüssel  $K_c$
- SIM-Karte, die enthält:
  - Schlüssel  $K_i$
  - Implementierungen von A3 und A8
  - IMSI (Internation Mobile Subscriber Identity)
- Das Mobiltelefon, mit der Implementierung A5
- Datenbanken des Mobilfunkbetreibers, mit dem Authentication Center AUC (feste Zuordnung von IMSI und  $K_i$ )

# Sicherheit in GSM-Netzen

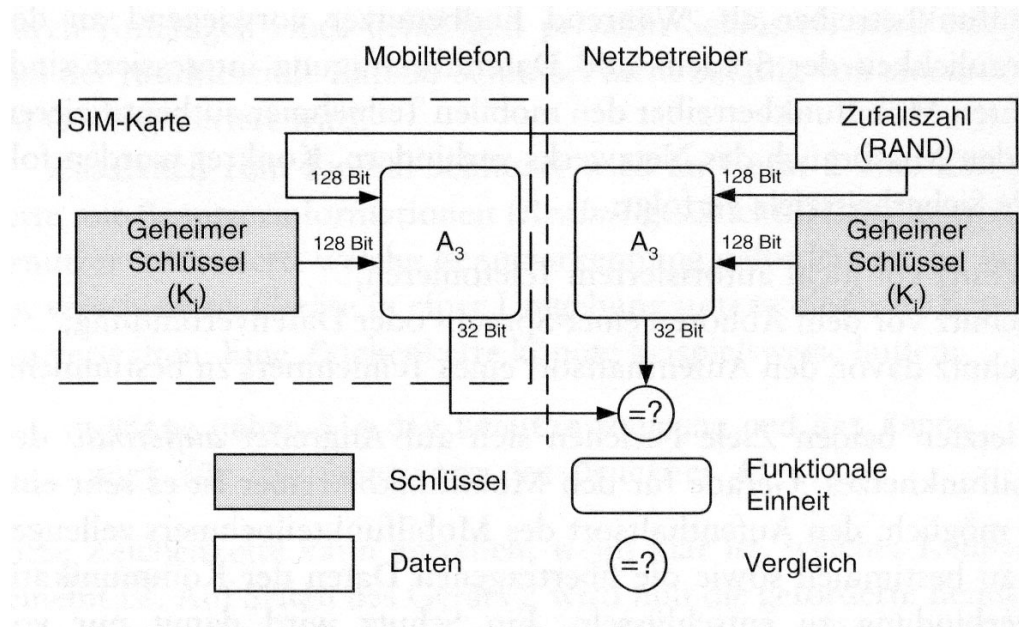
---

- Authentifizierung
- Verschlüsselung
- Sicherheit und Roaming
- Anonymität
- Kritik am Sicherheitskonzept

# Authentifizierung

Zugangsberechtigungsprüfung in zwei Schritten und einer Richtung Netzbetreiber -> Mobilfunkteilnehmer:

- PIN - Nutzer weist sich gegenüber der SIM-Karte aus.
- Challenge-Response-Verfahren: SIM-Karte weist sich gegenüber dem Netzbetreiber aus.



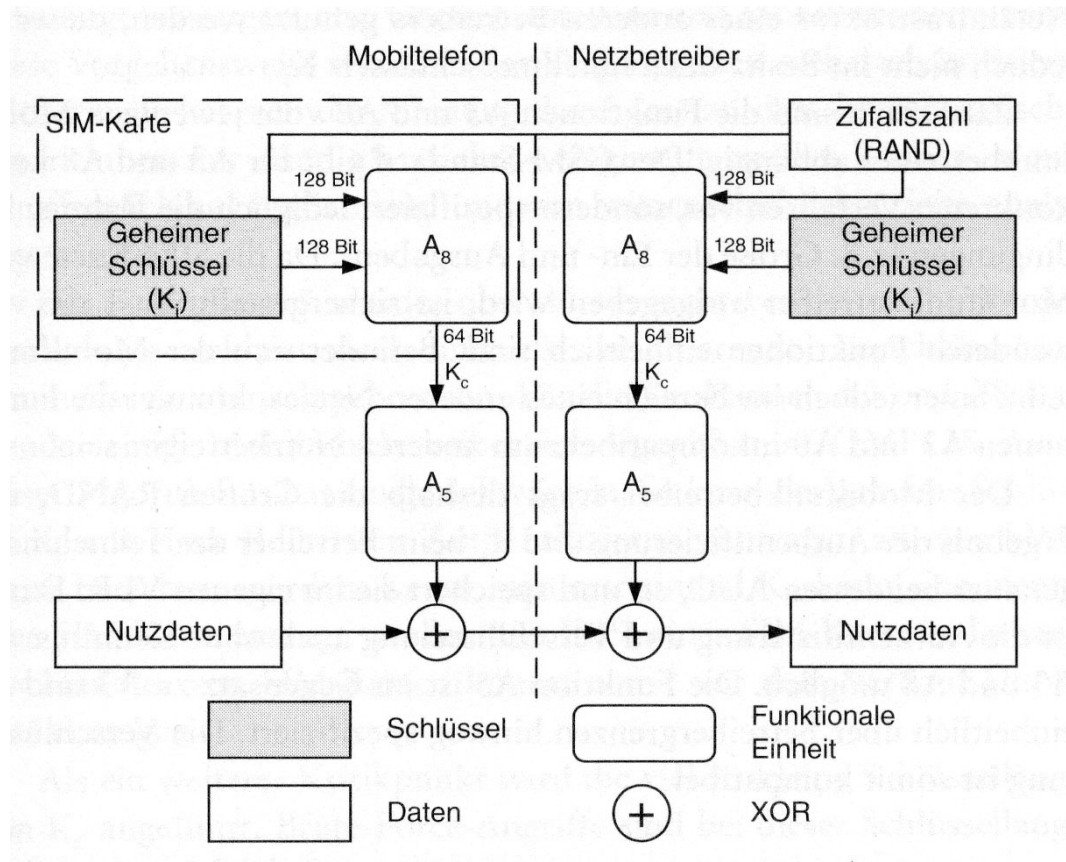
# Sicherheit in GSM-Netzen

---

- Authentifizierung
- Verschlüsselung
- Sicherheit und Roaming
- Anonymität
- Kritik am Sicherheitskonzept

# Verschlüsselung

Verschlüsselung nur bei erfolgreicher Authentifizierung.



# Sicherheit in GSM-Netzen

---

- Authentifizierung
- Verschlüsselung
- Sicherheit und Roaming
- Anonymität
- Kritik am Sicherheitskonzept

# Sicherheit und Roaming

---

Zusicherung der Authentizität und Verschlüsselung beim Roaming.

Problem: Die Funktionen A3 und A8 sind nicht kompatibel.

Lösung: Erfragen der Zufallszahl RAND, des Ergebnisses der Authentifizierung und des Schlüssels  $K_c$  bei dem Betreiber des Teilnehmers (AUC) und Speicherung der Informationen in VLR (Visitors Location Register).

# Sicherheit in GSM-Netzen

---

- Authentifizierung
- Verschlüsselung
- Sicherheit und Roaming
- Anonymität
- Kritik am Sicherheitskonzept

# Anonymität

---

Gewährleistung der Anonymität durch Einführung von Temporary Mobile Subscriber Identity TMSI.

Prinzip:

- Nach Authentifikation wird TMSI dem Teilnehmer zugeordnet.
- Mit LAI (Location Area Identity) eindeutige Zuordnung des Teilnehmers.
- Beim Wechseln in neuen VLR -> neues TMSI/LAI Paar.

# Sicherheit in GSM-Netzen

---

- Authentifizierung
- Verschlüsselung
- Sicherheit und Roaming
- Anonymität
- Kritik am Sicherheitskonzept

# Kritik am Sicherheitskonzept

---

- Geheimhaltung der Funktionen A3 und A8 aber standardisierte Schnittstellen.
- COMP128-Algorithmus für Funktionen A3 und A8 -> Berechnung des Schlüssels  $K_i$  -> SIM-Karten-Duplikate.
- Zu kleine Schlüssellänge bei dem Schlüssel  $K_c$  -> Brute-Force-Angriff auf Schlüssel.
- „Eine Richtung“ Authentifikation -> Man-in-the-Middle-Angriff

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- Sicherheit in GSM-Netzen
- **Sicherheit in Wireless LANs**
- Sicherheit in anderen mobilen Netzen
- Fazit

# Sicherheit in Wireless LANs

---

- Die Authentifizierung
- WEP
- Kritik an WEP

# Sicherheit in Wireless LANs

---

## Sicherheitskonzept nach IEEE 802.11:

- Zugriffslisten bei Access Point.
- Gemeinsames Kennwort bei allen Access Points und Stationen.
- Gemeinsames Kennwort für die Verschlüsselung von allen Paketen.

# Sicherheit in Wireless LANs

---

- Die Authentifizierung
- WEP
- Kritik an WEP

# Authentifizierung

---

## Prinzip:

- Zugriffslisten von MAC-Adressen der zugelassenen Stationen hinterlegt bei Access Points.

## Vorteile:

- Einfaches Konzept.
- Leicht zu realisieren.

## Nachteile:

- Enormer Verwaltungsaufwand bei größeren Netzen.
- MAC-Adressen können geändert werden.

# Sicherheit in Wireless LANs

---

- Die Authentifizierung
- WEP
- Kritik an WEP

# WEP

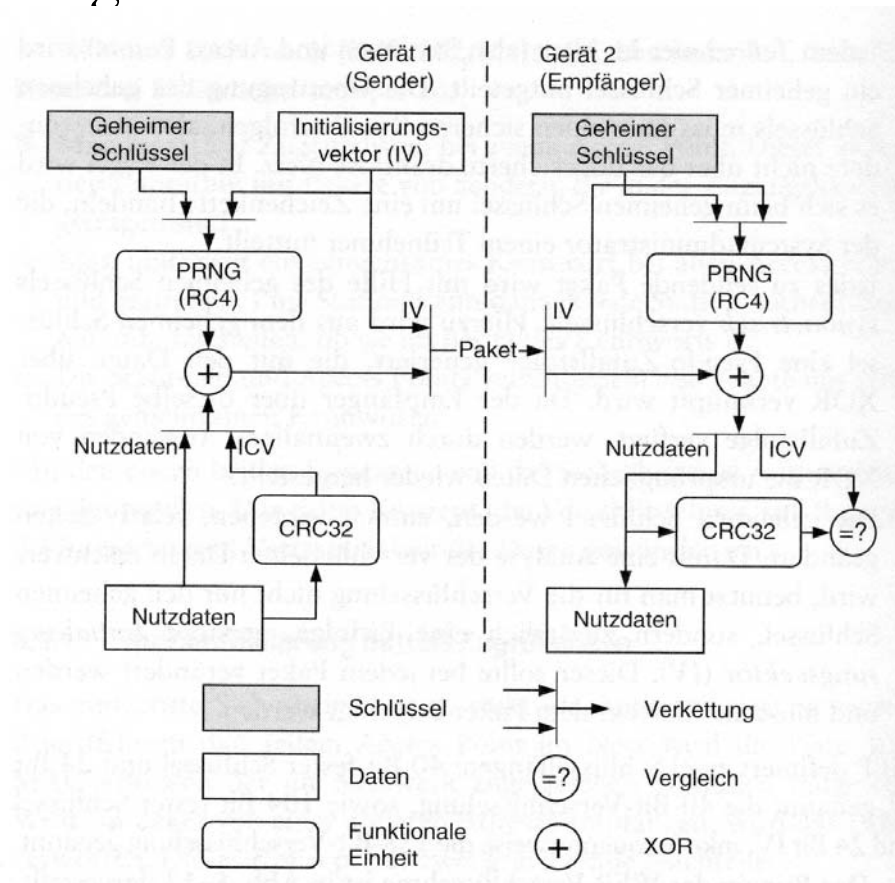
---

- Wired Equicalent Privacy (WEP) im Standard 802.11.
- Sicherheitskonzept zur Verschlüsselung und Authentifizierung.

## Prinzip von WEP:

- Geheimer Schlüssel für jeden Teilnehmer (wird durch sicheren Kanal übertragen).
- Symmetrische Verschlüsselung jedes Pakets mit geheimen Schlüssel.
- Geheimer Schlüssel wird selten geändert.
- Zusätzlich bei der Verschlüsselung Initialisierungsvektor (IV bei jedem Paket verändert und als Klartext beigefügt).

## Verschlüsselung nach WEP:



# WEP

---

## Prinzip der Authentifizierung:

- Prüfsumme gemäß Cyclic Redundancy Check (CRC) nur mit Kennwort.
- Explizite Authentifizierung mit 128 Bit Zufallsfolge. Die Daten werden unverschlüsselt versendet. Der Empfänger muss die Zufallsfolge mit WEP verschlüsseln und zurücksenden. Sender vergleicht beide Werte.

## Verschlüsselungen nach Schlüssellängen:

- 40-Bit-Verschlüsselung: 40 Bit fester Schlüssel und 24 Bit IV.
- 128-Bit-Verschlüsselung: 104 Bit fester Schlüssel und 24 Bit IV.

# Sicherheit in Wireless LANs

---

- Die Authentifizierung
- WEP
- Kritik an WEP

# Kritik an WEP

---

- Kein Schutz gegen Angreifer aus dem gleichen Netz.
- Zu kurzer Schlüssel bei 40-Bit-Verschlüsselung -> Brute-Force-Angriff
- Zu selten oder gar keine Änderung von IV.
- Schwächen des Algorithmus RC4 -> „Wörterbuch“ für IV Werte.
- Access Point.
- Integrität mit CRC-Verfahren nicht gewährleistet.
- WEP2: 128 Bit Schlüssellänge aber weiterhin RC4 Algorithmus.

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- Sicherheit in GSM-Netzen
- Sicherheit in Wireless LANs
- **Sicherheit in anderen mobilen Netzen**
- Fazit

# Sicherheit in anderen Netzen

---

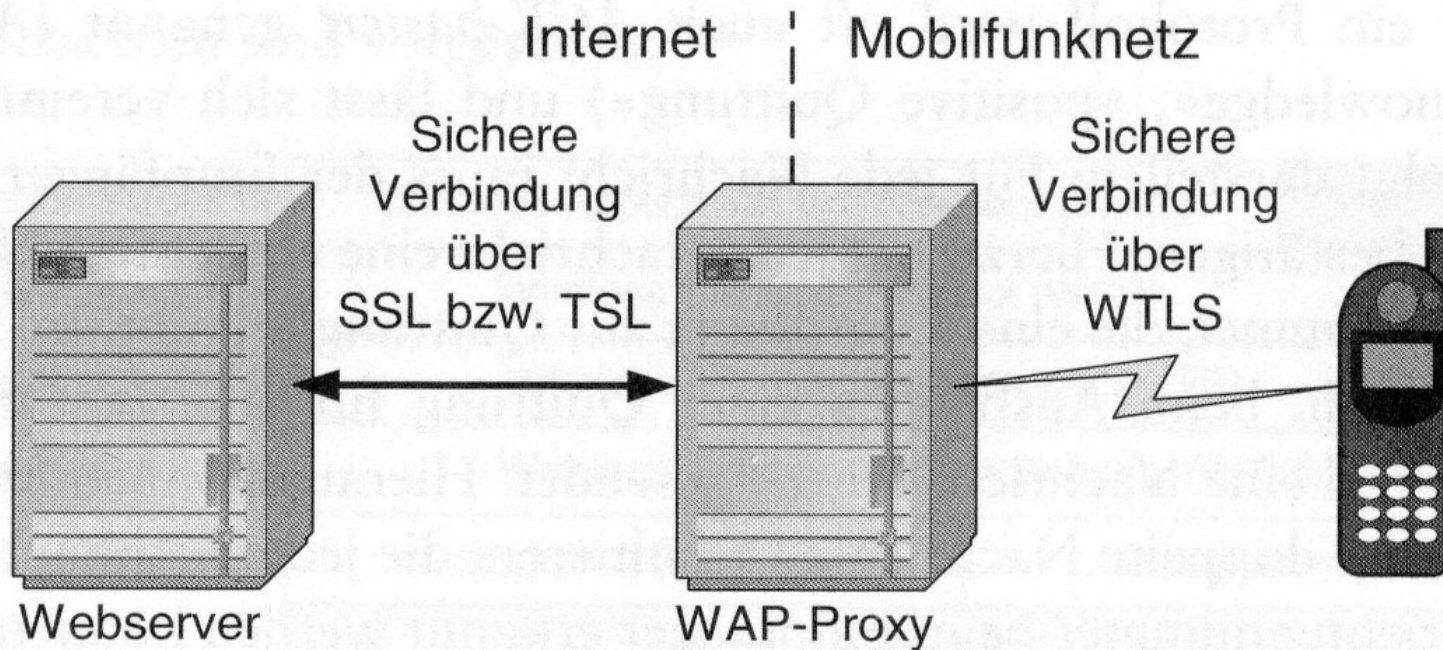
- WAP
- Satellitensystemen

# Sicherheit in anderen Netzen

---

- WAP
- Satellitensystemen

## Sicherheitskonzept:



# WTLS

---

Spezielle Protokollschicht WTLS stammt aus TLS und wurde für drahtlose Netze optimiert.

Sicherheitsziele:

- Sicherung der Datenintegrität.
- Schutz gegen Mithören.
- Authentifikation.
- Schutz gegen Denial-of-Service-Angriffe.

Sicherheitskonzept:

- Asymmetrisches Verschlüsselungsverfahren für Vereinbarung des gemeinsamen Schlüssels.
- Symmetrische Verschlüsselung für Anwendungsnachrichten.
- Hashfunktionen zur Authentifizierung.

# WTLS

---

## Sitzungszustand:

- Sitzungserkennung durch Server
- Zertifikat des Kommunikationspartners
- gemeinsame Komprimierungsmethode
- symmetrischer Verschlüsselungsalgorithmus
- Hashfunktion zu authentifizierten Nachrichten
- Master Secret für Schlüsselbildung

## WTLS Protokolle:

- Handshake-Protokoll
- Change-Cipher-Protokoll
- Alert-Protokoll

## Handshake-Protokoll:

- Einrichtung der sicheren Verbindung.
- Vereinbarung der Verfahren und Schlüssel zwischen Client und Server:
  - Schlüsselaustauschverfahren
  - symmetrisches Verschlüsselungsverfahren
  - Hashfunktionen
  - Komprimierungsverfahren
  - Festlegung der Häufigkeit von neuen Vereinbarungen für kryptografischen Informationen
- eventuell Austausch der Zertifikate

# WTLS

---

## Change-Cipher-Protokoll:

- Definieren der Vereinbarungen als gültig.
- Besteht aus einer Nachricht.
- Diese Nachricht wird innerhalb des Handshake-Protokolls versendet.
- Gehört aber nicht zum Handshake-Protokoll.

# WTLS

---

## Alert-Protokoll:

- Meldet sicherheitsrelevante Fehler dem Kommunikationspartner.
- Bei schwerwiegender Sicherheitsverletzung Beendung der Verbindung.

## Allert-Nachrichten werden verschickt:

- bei ungültigem Zertifikat
- bei Veränderung der Nachricht während des Transports.

## Denial-of-Service-Angriffe

Problem 1: Datagramme auf Transportebene.

Lösung: Mit WTLS nach Aufbau der sicheren Verbindung leichte Erkennung der fremden Nachrichten mit Hilfe von zusätzlichen Informationen, wie Nachrichtennummern.

Problem 2: Angriffe auf Handshake-Nachrichten, Hello-Nachrichten sind nicht verschlüsselt.

Lösung: Änderung von kryptografischen Parameter erst nach Finish-Nachricht.

Problem 3: Geringe Rechenkapazität beim Client.

Lösung: Berechtigung Schlüsselabgleichsanfragen zu ignorieren.

# Sicherheit in anderen Netzen

---

- WAP
- Satellitensystemen

# Satellitensystemen

---

„Forschern der Ruhr-Universität Bochum ist es bei der Untersuchung der Satelliten-Internet-Zugänge (DSL über Satellit) der **Telekom**[1], Megasys und Netsystems gelungen, umfangreiche Informationen über einzelne Personen zu ermitteln. So konnten sie in einem Zeitraum von 24 Stunden in den Datenströmen eines Astra-Transponders Name, Adresse, Geburtsdatum, Einkommen und EC-Kartenummer eines Opfers mitlesen. Auch war es möglich, die E-Mail-Kommunikationen zwischen kommerziellen Nutzern abzuhören. Dazu benutzten sie nur einen handelsüblichen PC, eine DVB-S-Karte und eine Satellitenschüssel.“ von 26.11.2004

# Satellitensystemen

---

„LONDON – Hackers have reportedly seized control of one of Britain's military communication satellites and issued blackmail threats.” von Nachrichtenagentur Reuters  
28.02.1999

Denial-of-Service-Angriff auf GPS mit „Jammer”. „[...] Ein solches Gerät wurde auf der Moscow Air Show 98 von einem Russen erstmals der Öffentlichkeit vorgestellt und versetzte die dort anwesenden Militärs vieler Länder in hektische Aufregung.”

# Gliederung

---

- Bedeutung der Sicherheit in mobilen Netzen
- Grundlagen der Kryptografie
- Sicherheit in GSM-Netzen
- Sicherheit in Wireless LANs
- Sicherheit in anderen mobilen Netzen
- **Fazit**

# Fazit

---

- Sicherheit bei drahtlosen Netzen ist längst noch nicht den Drahtgebundenen Netzen gleich.
- Sicherheitsmechanismen erfüllen nicht die Anforderungen für eine Nutzung in sensiblen Bereichen.
- Zusätzliche Absicherung bei Wireless LAN notwendig, z.B. durch Firewall.
- Satellitensysteme sind genauso stör anfällig und unsicher.

Vielen Dank  
für Ihre  
Aufmerksamkeit