GET http://anon.nowhere.com/
>please type in your name
>set cookie

Starke Anonymität im Internet

Hannes Federrath
Freie Universität Berlin

> Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Systemadministrator
  - Nachbar ...

Funküberwachungsantenne (AN/FLR9)

> Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Sys-admin
  - Nachbar ...

Bad Aibling Interception facility of the ECHELON system

Source: http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/

> Anonymität im Internet ist eine Illusion

Electronic Mail: Log-Dateien zeigen Kommunikationsbeziehungen

```
>tail syslog
Oct 15 16:32:06 from=<feder@tcs.inf.tu-dresden.de>, size=1150
Oct 15 16:32:06 to=<hf2@irz.inf.tu-dresden.de>
```

World Wide Web: Log-Dateien zeigen Interessensdaten

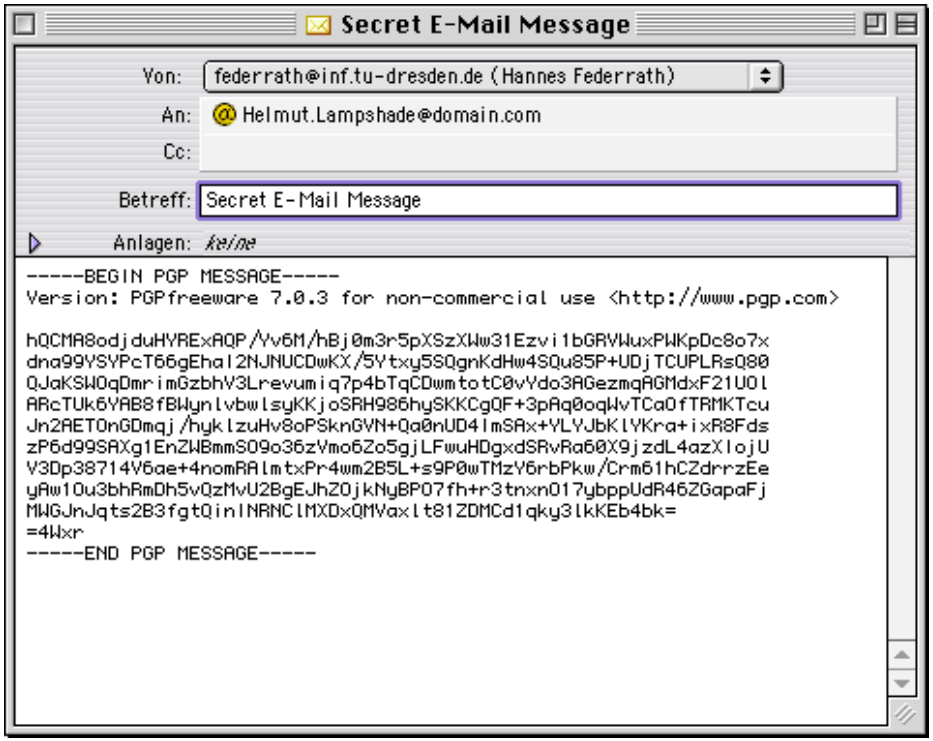
```
wwwtcs.inf.tu-dresden.de>tail access_log
amadeus.inf.tu-dresden.de - - [15/Oct/1997:11:50:01] "GET
/lvbeschr/winter/TechnDS.html HTTP/1.0" - "http://wwwtcs.inf.tu-
dresden.de/IKT/" "Mozilla/3.01 (X11; I; SunOS 5.5.1 sun4u)"
```

Finger: Die Ermittlung eines Rechnerbenutzers ist kein Problem

```
ithif19 logs 17 >finger @amadeus.inf.tu-dresden.de
[amadeus.inf.tu-dresden.de]
Login       Name                TTY         Idle    When
feder    Hannes Federrath       console             Wed 11:56
```

Hilft Verschlüsselung?

- Verschlüsseln hilft gegen Ausspähen der *Inhalte*



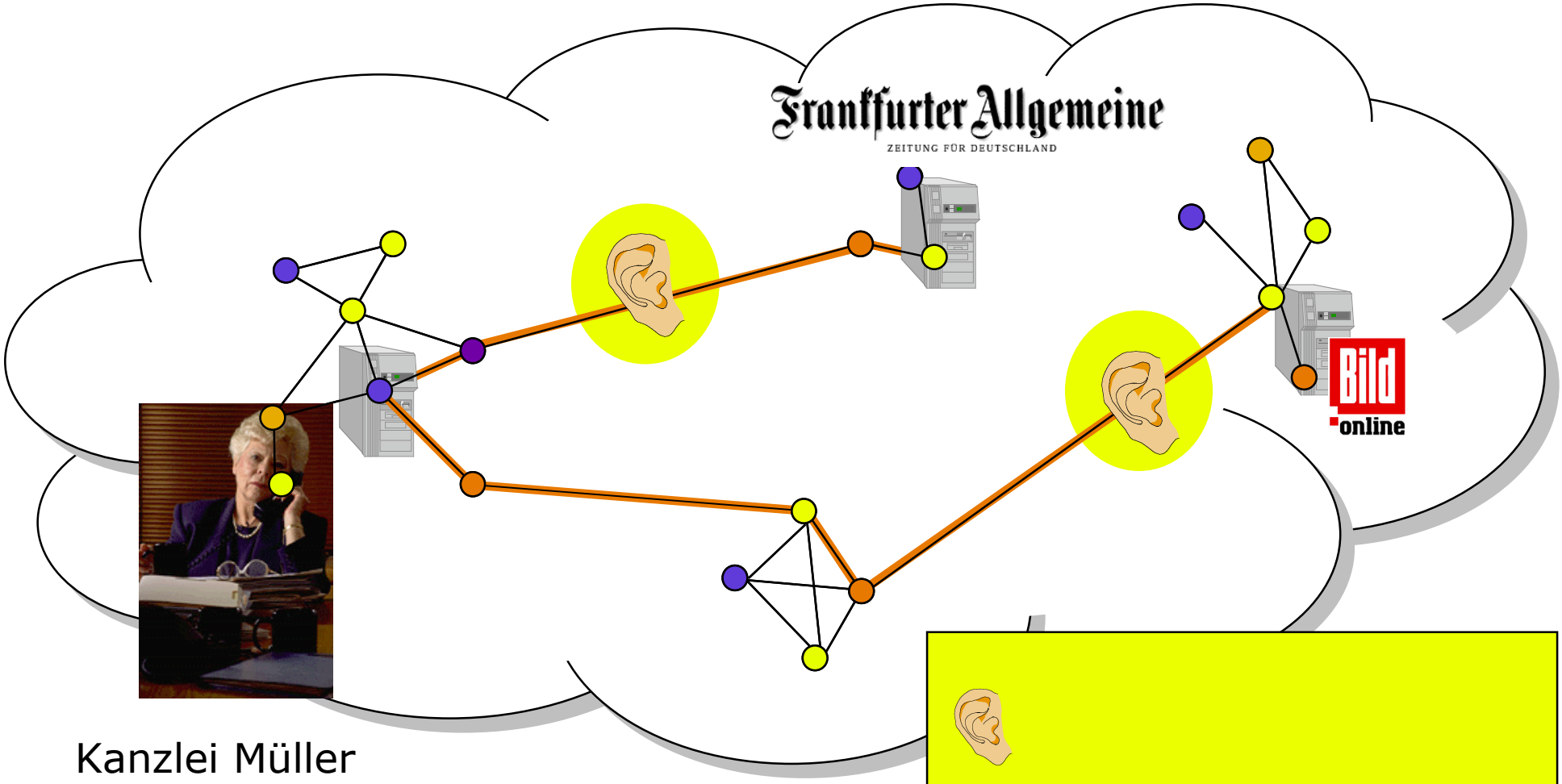
Trotzdem PGP verwenden!

Pretty Good Privacy

http://www.pgp.com

Verschlüsseln hilft überhaupt nichts gegen Beobachtung von Kommunikationsbeziehungen

> Warum genügt Verschlüsselung nicht?



Kanzlei Müller
spezialisiert auf
Firmenfusionen

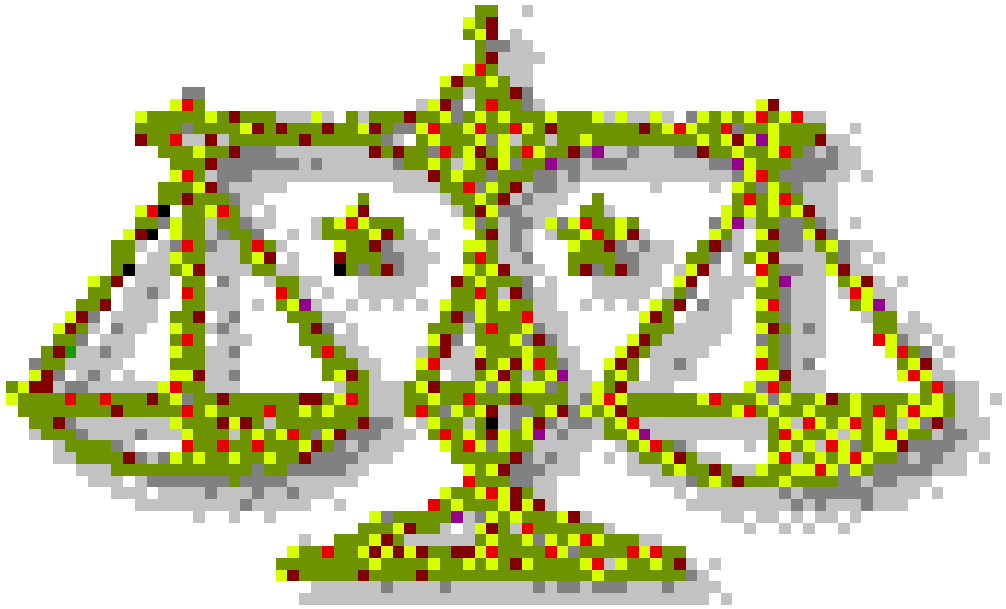
Beobachtung von
Kommunikationsereignissen
lässt auf Inhalte Schließen

Vertraulichkeit; hier: Vertraulichkeit der Verkehrsdaten

- **Unbeobachtbarkeit**
  - Schutz von Sender und/oder Empfänger gegenüber allen Unbeteiligten (inkl. Netzbetreiber)
    - Niemand kann Kommunikationsbeziehungen verfolgen.
    - Unbeobachtbares Senden und/oder Empfangen von Nachrichten
- **Anonymität**
  - Schutz der Identität zusätzlich auch gegenüber dem Kommunikationspartner
    - Anonymität als *Sender* von Nachrichten
    - Anonymität als *Empfänger* von Nachrichten
- **Unverkettbarkeit**
  - Ereignisse werden vom Angreifer bzgl. des Senders und/oder Empfängers als unabhängig erkannt

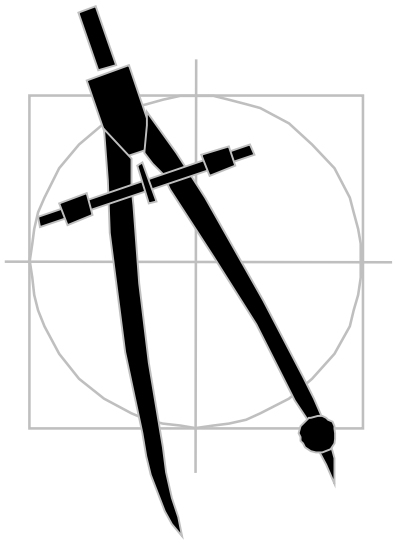
> Juristische Sicht

- Teledienstedatenschutzgesetz (TDDSG)
  - §3(4): Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.
  - §4(1): Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.



> Technischer Datenschutz

- Technischer Datenschutz
  - Systeme so konstruieren, dass unnötige Daten vermieden und nicht miteinander verkettet werden können.
- Zu verschleiern sind:
  - Adressen:
    - Sender, Empfänger, Kommunikationsbeziehung
  - Zeitliche Korrelationen:
    - Zeitpunkte, Dauer
  - Übertragenes Datenvolumen und inhaltliche Korrelationen
  - Orte:
    - Aufenthaltsorte, Bewegungsspuren

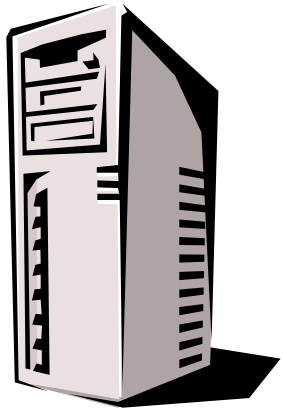


Funktionsweise von Cookies

Erster Besuch:

1. GET www.amazon.de

2. Set cookie id=12241235564



3. ggf. Warnung

4. Speichern auf Festplatte

Folgende Besuche:

GET www.amazon.de
cookie id=12241235564

- wird nur an zugehörigen Server zurückgesendet
- hat ein vom Server definiertes Verfallsdatum
- wird auch bei Abruf eingebetteter Objekte gesendet (z. B. Bilder)

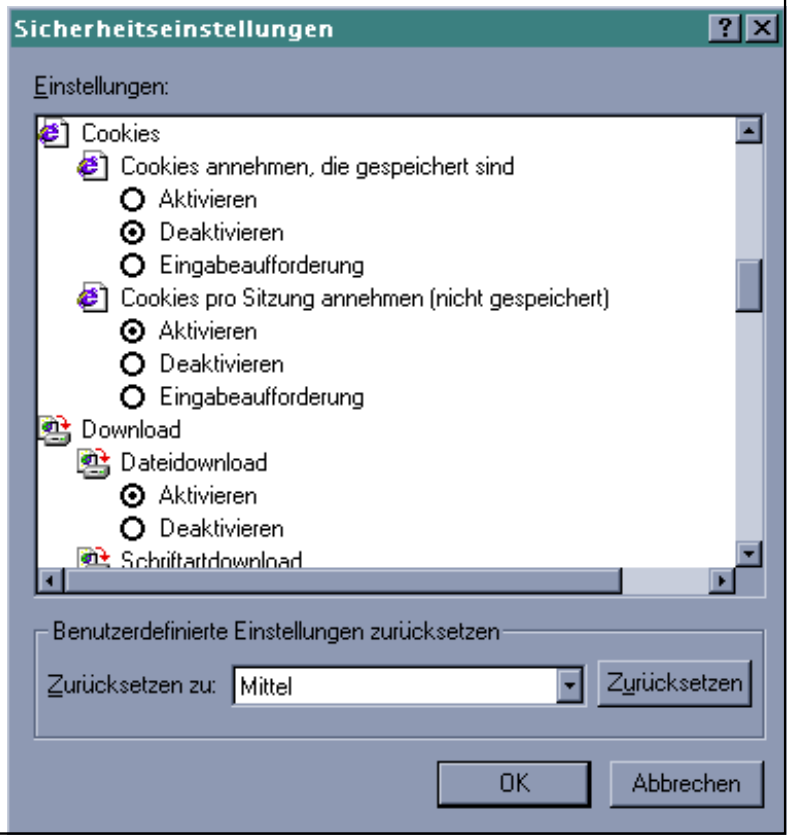
Ungefährliche Kekse ?

- Löschen nicht die Festplatte
- Übertragen keinen Viren
- Verraten keine lokal gespeicherten Daten
  - Passwörter, geheime Schlüssel usw.
- Webserver erkennt Nutzer bei jedem Besuchen seiner Seite wieder
  - Positiv:
    - personalisierte Webseiten
  - Negativ:
    - Erstellung von Nutzerprofilen

Gefährliche Kekse !

- Werberinge (z.B. Doubleclick.com):
  - Plazieren Banner auf Seiten vieler Anbieter
  - Alle Banner werden von zentralem Server geladen, Cookie wird gesendet
  - Werbeserver erhält globales Nutzungsprofil
  - Alle Server könnten Informationen erfahren, die man an einen gesendet hat.

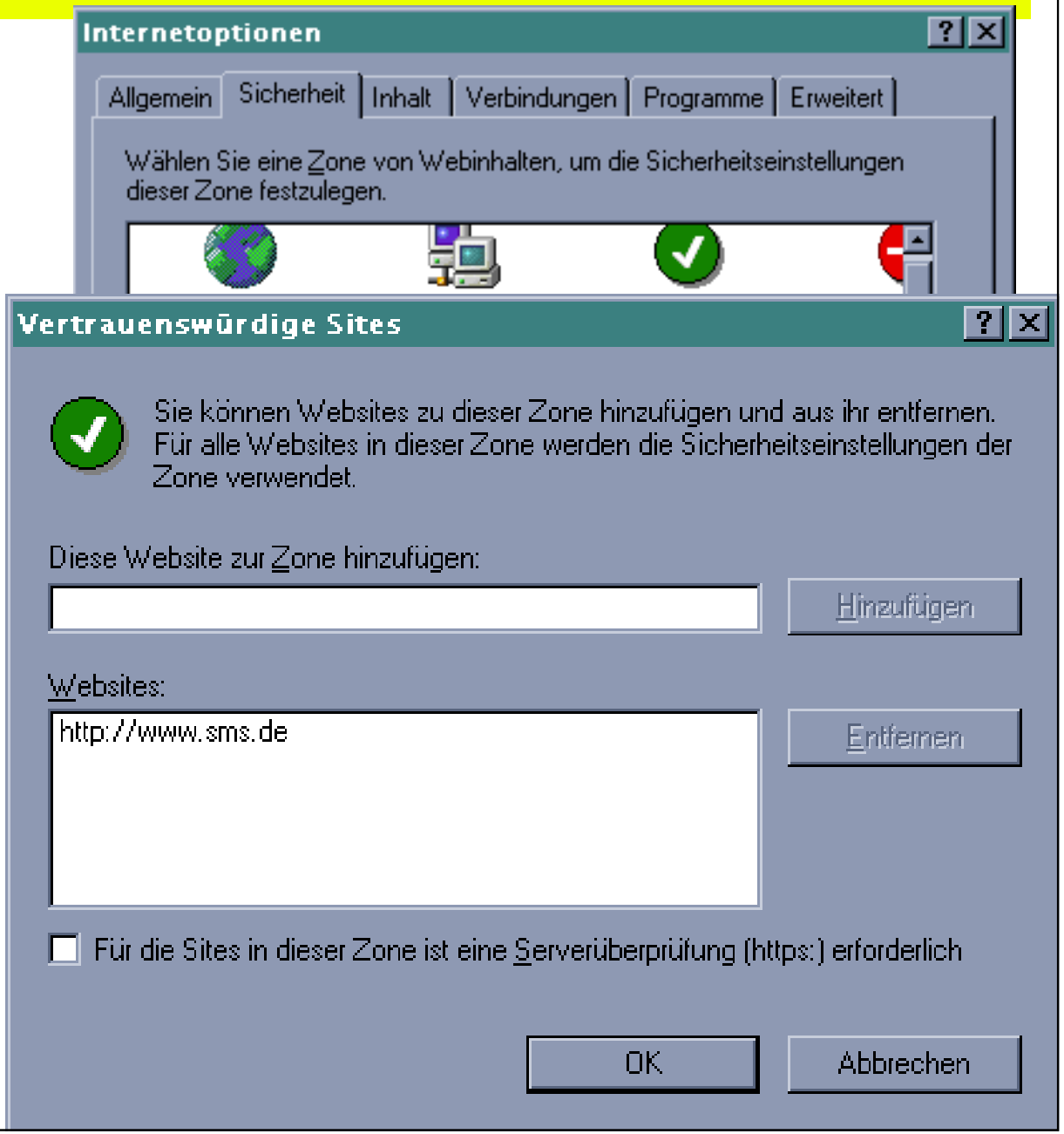
- Gegenmaßnahmen
  - Cookies deaktivieren
  - Problem:
    - Viele Angebote nur mit Cookies verfügbar
    - nützliche Anwendungen für Cookies



Gegenmaßnahmen

Cookies

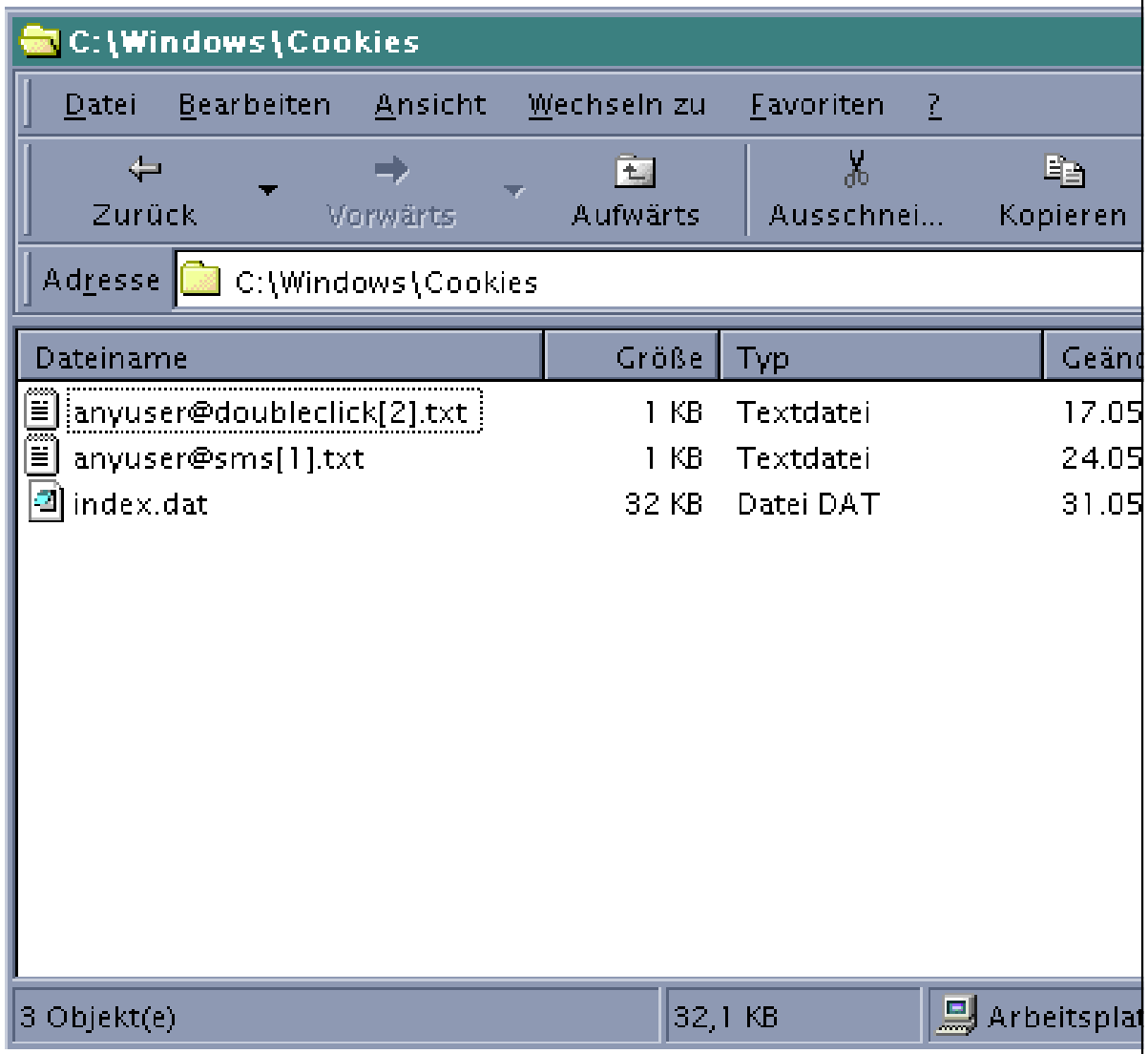
- ⌘ nur bei ausgewählten Seiten speichern
- ⌘ regelmäßig löschen
- ⌘ regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- ⌘ nur bei ausgewählten Seiten speichern
- ⌘ regelmäßig löschen
- ⌘ regelmäßig weltweit austauschen

CookieCooker
cookie.inf.tu-dresden.de

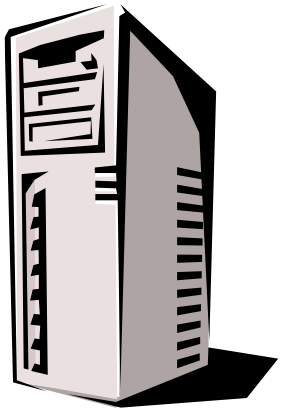
Überwachung auch ohne Cookies

- IP-Nummern

Adresse:
123.86.9.5

GET www.amazon.de
To: 195.66.15.4
From: 123.86.9.5

HTTP ...
To: 123.86.9.5
From: 195.66.15.4



Adresse:
195.66.15.4

Einschränkung:

Zuweisung dynamischer IP-Nummern bei Einwahlzugang

Überwachung auch ohne Cookies

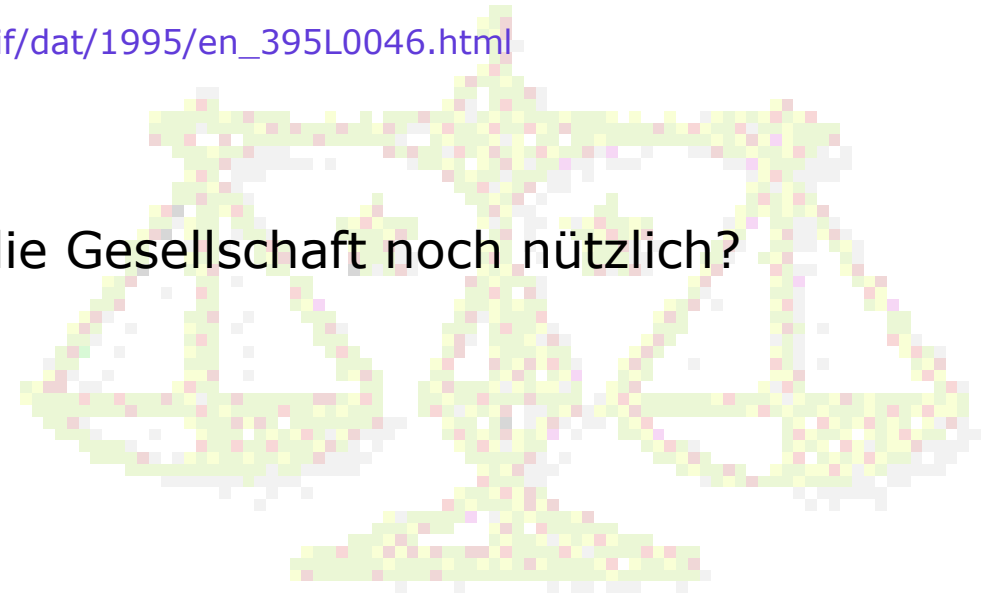
- Überwachung durch Internet Service Provider

Beispiel:

http://www.predictivenetworks.com/

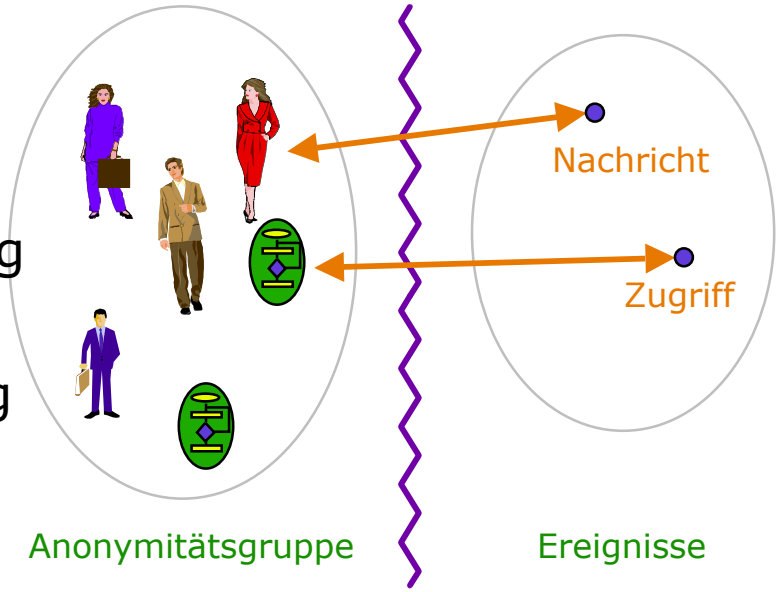
> Politisches und gesellschaftliches Umfeld

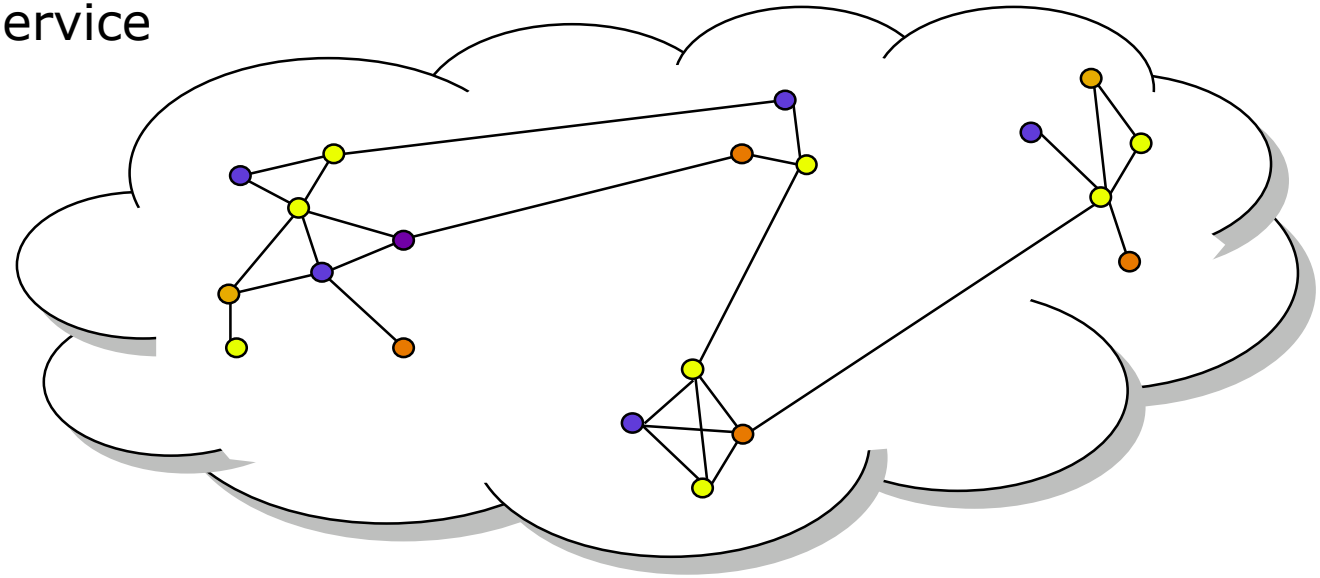
- Telekommunikationsüberwachung
  - Telekommunikationsüberwachungsverordnung (TKÜV)
    - http://www.bmwi.de/Homepage/download/telekommunikation_post/TKUEV-Entwurf.pdf
  - Cybercrime Convention
    - http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm
- Datenschutzgesetze
  - Neues Bundesdatenschutzgesetz (BDSG)
    - http://www.bfd.bund.de/information/bdsg_hinweis.html
  - EU-Datenschutzrichtlinie
    - http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html
- Offene Frage
  - Wieviel Privatheit ist für die Gesellschaft noch nützlich?



> Verfahren zur unbeobachtbaren Kommunikation

- Wer ist zu schützen?
  - Schutz des Senders
  - Schutz des Empfängers
  - Schutz der Kommunikationsbeziehung
- Grundkonzepte:
  - Verteilung mit impliziter Adressierung
  - Dummy traffic
  - Proxies
  - DC-Netz
  - Blind-Message-Service
  - Mix-Netz
  - Steganographie

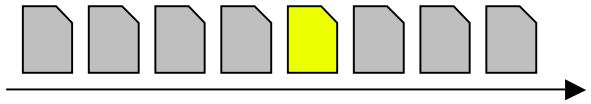




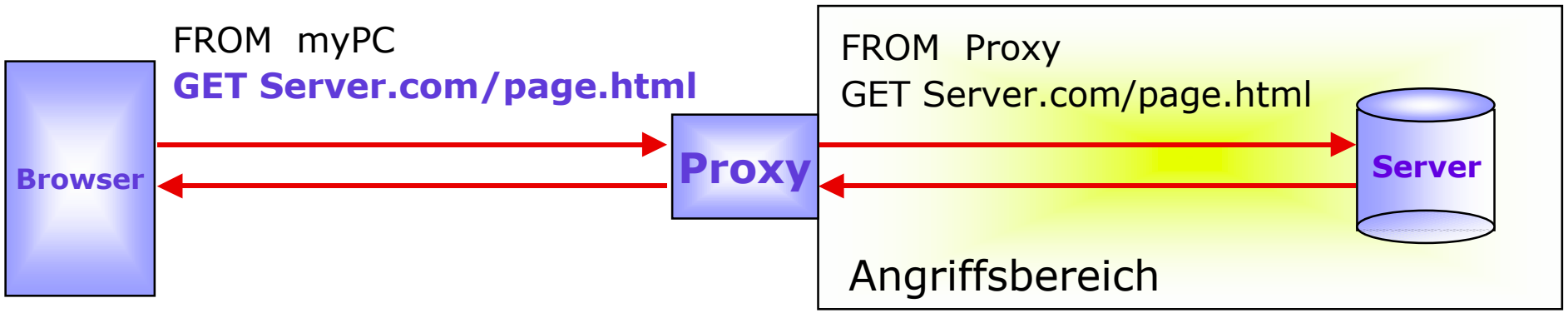
> Grunsätzliche Techniken (1)

- **Verteilung** (Broadcast) + implizite Adressierung
  - Schutz des Empfängers; alle erhalten alles
  - lokale Auswahl

- **Dummy Traffic:** Senden bedeutungsloser Nachrichten
  - Schutz des Senders



- **Proxies** zwischenschalten
  - Server erfährt nichts über Client, Proxy kann mitlesen

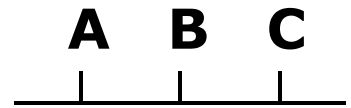


> Grundsätzliche Techniken (2)

- **DC-Netz:** kombiniert u.a. Broadcast, Kryptographie und Dummy Traffic
  - Schutz des Senders
- **Blind-Message-Service:** Unbeobachtbare Abfrage aus von unabhängigen Betreibern replizierten Datenbanken
  - Schutz des Clients
- **MIX-Netz:** kombiniert u.a. hintereinander geschaltete Proxies von unabhängigen Betreibern, Kryptographie und Dummy Traffic
  - Schutz der Kommunikationsbeziehung
  - Effizient in Vermittlungsnetzen
- **Steganographie**
  - Verbergen einer Nachricht in einer anderen

> DC-Netz

Chaum, 1988



Broadcastnetz

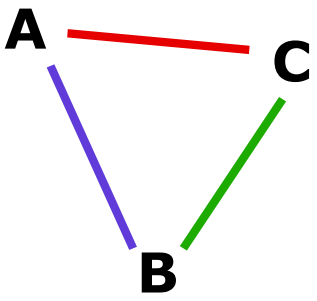
Echte Nachricht von A	00110101
Schlüssel mit B	00101011
Schlüssel mit C	00110110
Summe	00101000

A sendet 00101000

Leere Nachricht von B	00000000
Schlüssel mit A	00101011
Schlüssel mit C	01101111
Summe	01000100

B sendet 01000100

Schlüsselgraph



Leere Nachricht von C	00000000
Schlüssel mit A	00110110
Schlüssel mit B	01101111
Summe	01011001

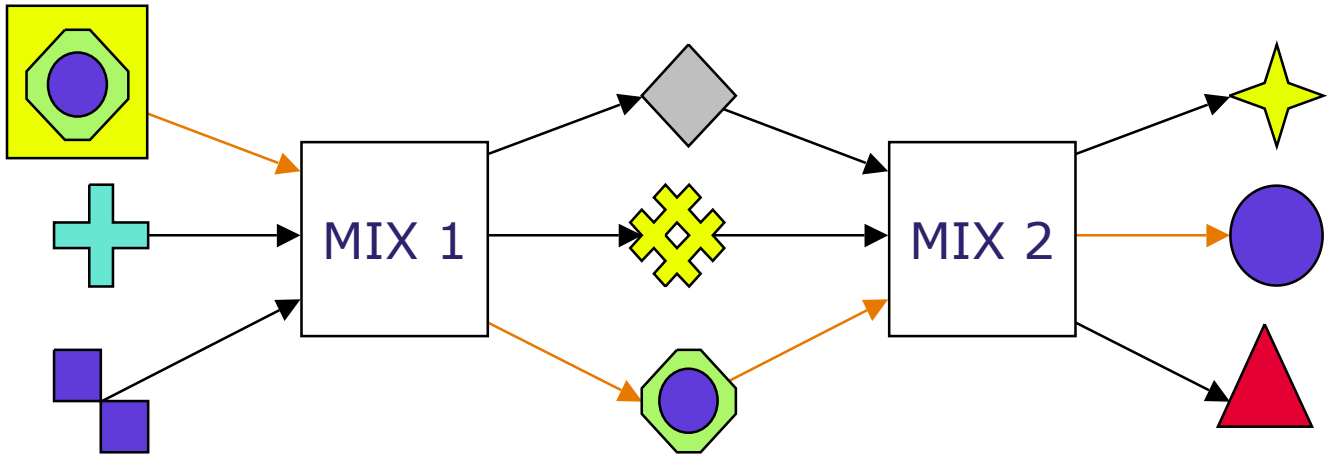
C sendet 01011001

Summe = Echte Nachricht von A 00110101

Mix-Netz

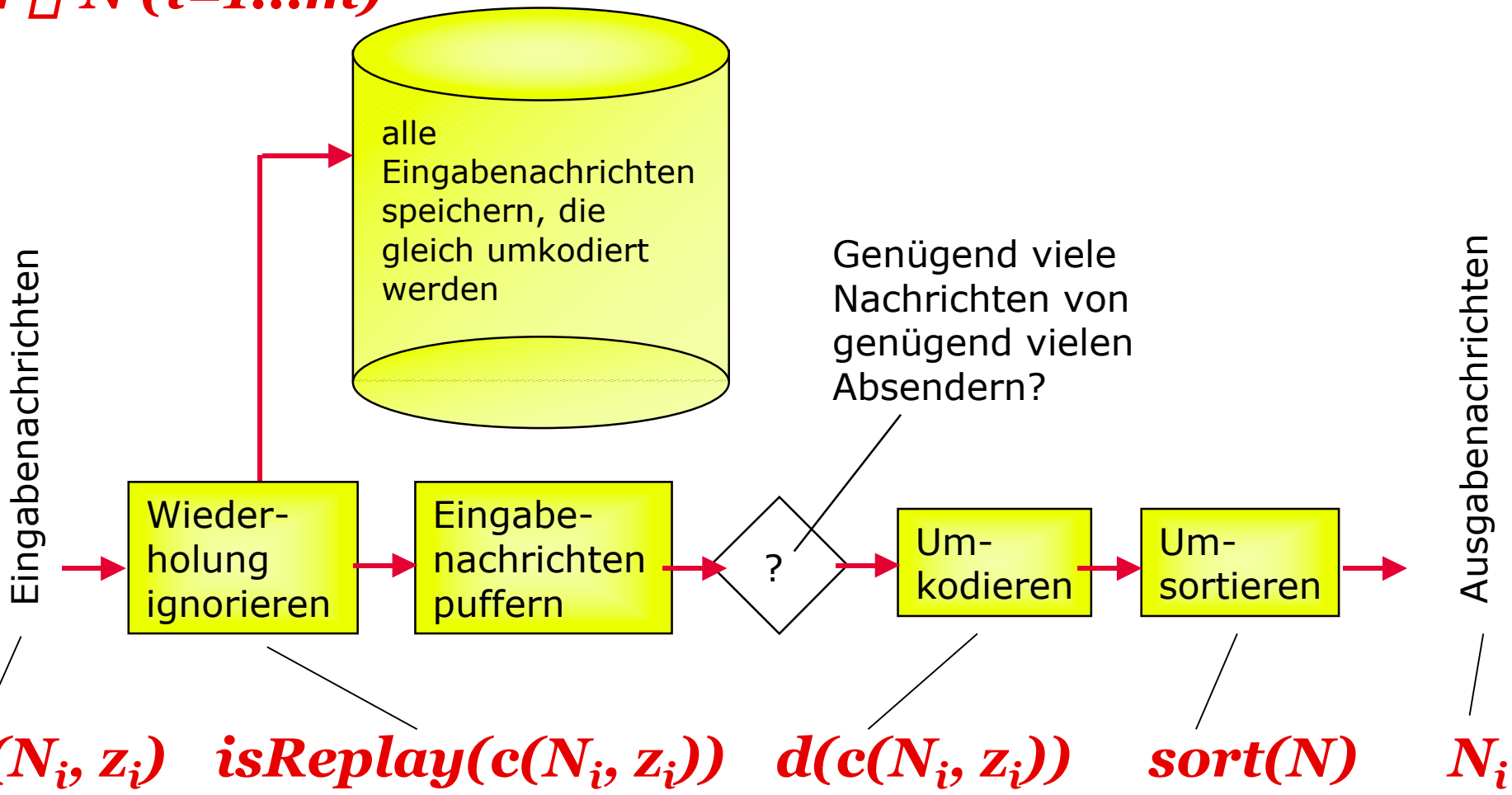
Chaum, 1981

- Grundidee:
  - Nachrichten in einem »Schub«
    - sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix verwenden.
  - Wenigstens ein Mix darf nicht angreifen.
- Schutzziel:
  - Unverkettbarkeit von Sender und Empfänger
  - Schutz der Kommunikationsbeziehung
  - Zuordnung zwischen E- und A-Nachrichten wird verborgen



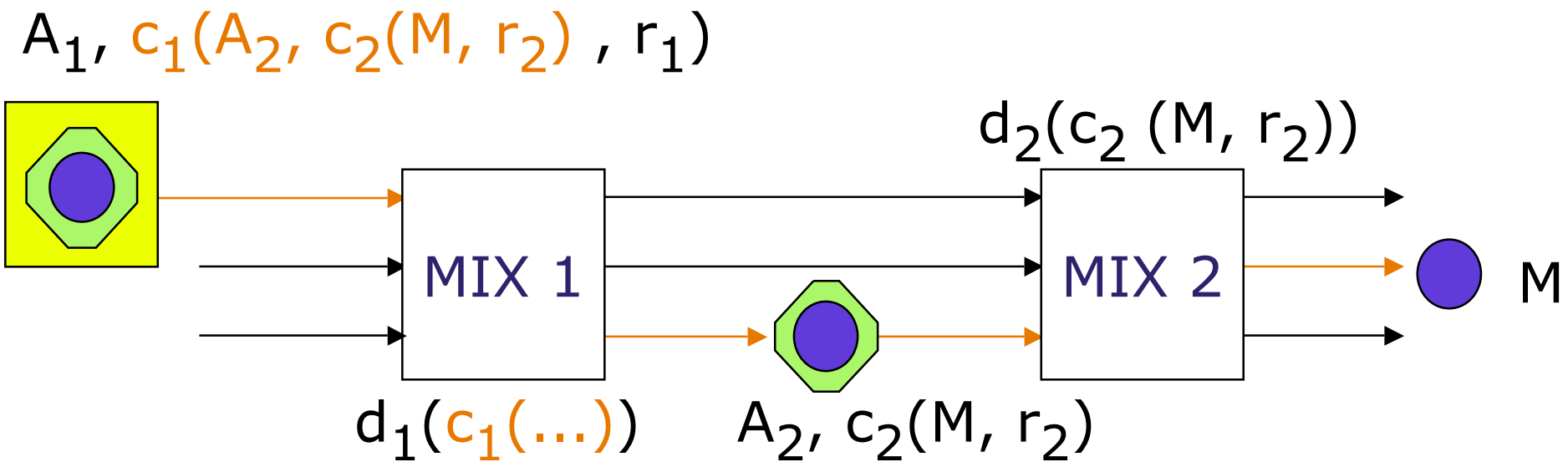
> Blockschaltbild eines Mix

$N = \{N_1, N_2, \ldots, N_m\}$
$N \not\sqsubset N \ (i=1\ldots m)$



Kryptographische Operationen eines Mix

- Verwendet **asymmetrisches Konzelationssystem**
  - $c_i(...)$ Verschlüsselungsfunktion für Mix i
    - Jeder kann den öffentlichen Schlüssel c_i verwenden
  - $d_i(...)$ private Entschlüsselung von Mix i
    - Nur Mix i kann entschlüsseln
  - A_i Adresse von Mix i
  - r_i Zufallszahl (verbleibt im Mix, wird »weggeworfen«)
  - M (verschlüsselte) Nachricht für Empfänger (inkl. seiner Adresse)

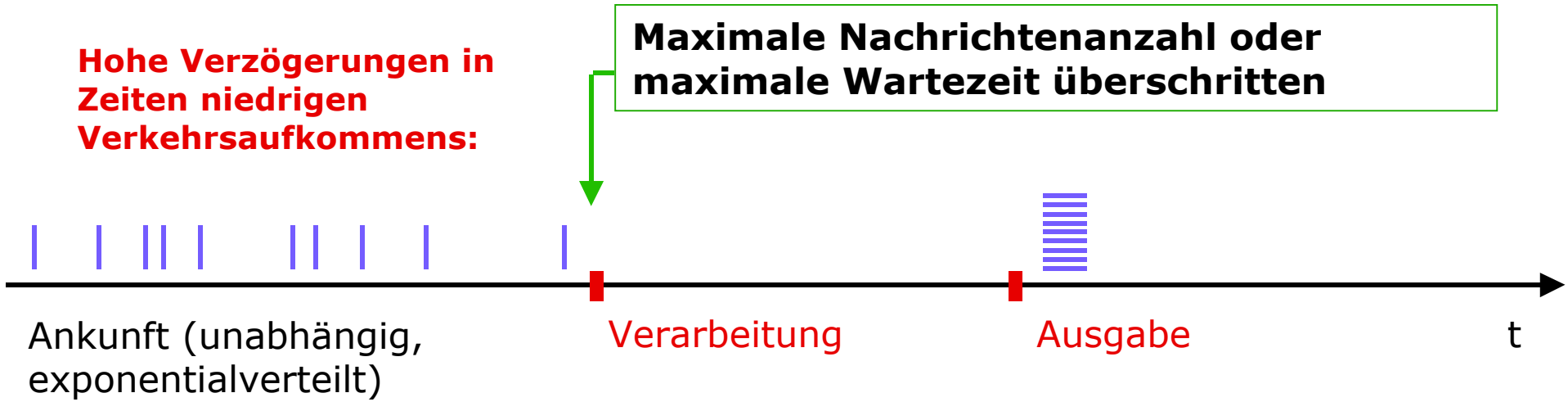


> Mixe: Warum mehr als ein Mix?

- Schutzziel: Auch Mix soll nicht beobachten können
  - Ein einzelner Mix kennt jedoch E-A-Zuordnung
- Verwende mindestens zwei Mixe
  - erster Mix kennt Sender
  - letzter Mix kennt Empfänger
- Allgemein:
  - Verwende so viele Mixe, dass sich in der Mix-Kette wenigstens ein Dir vertrauenswürdiger Mix befindet
- Praxis:
  - Je mehr Mixe verwendet werden, umso häufiger muß umkodiert werden und es steigt die Verzögerungszeit.
  - Es genügt, wenn ein einziger Mix tatsächlich vertrauenswürdig ist.
  - Lieber sorgfältig wenige Mixe auswählen.
  - Derzeit verwendet man wenigstens drei, besser fünf Mixe, aber das ist rein subjektiv.

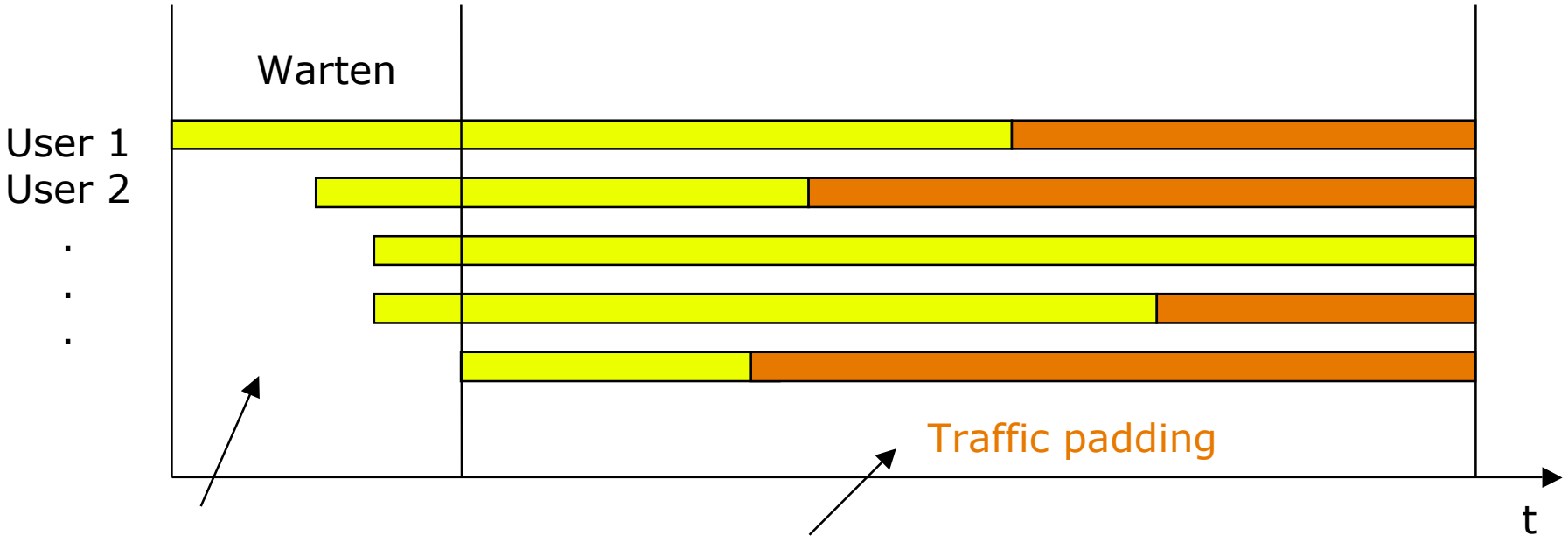
> Echtzeitkommunikation und Mixe

- Mixe sind gut geeignet für wenig zeitkritische Dienste:
  - E-Mail
- Für Echtzeitkommunikation (http, ftp) sind Modifikationen nötig:
  - Nachrichten sammeln führt zu starken Verzögerungen, da der Mix die meiste Zeit auf andere Nachrichten wartet
  - Nachrichtenlängen und Kommunikationsdauer variieren bei verbindungsorientierten Diensten stark
- Veränderungen nötig



> Traffic padding

- Ziel: Verbergen, wann eine Kommunikation beginnt und endet
- Problem: Niemand weiß, wann der letzte Nutzer seine Kommunikation beenden möchte



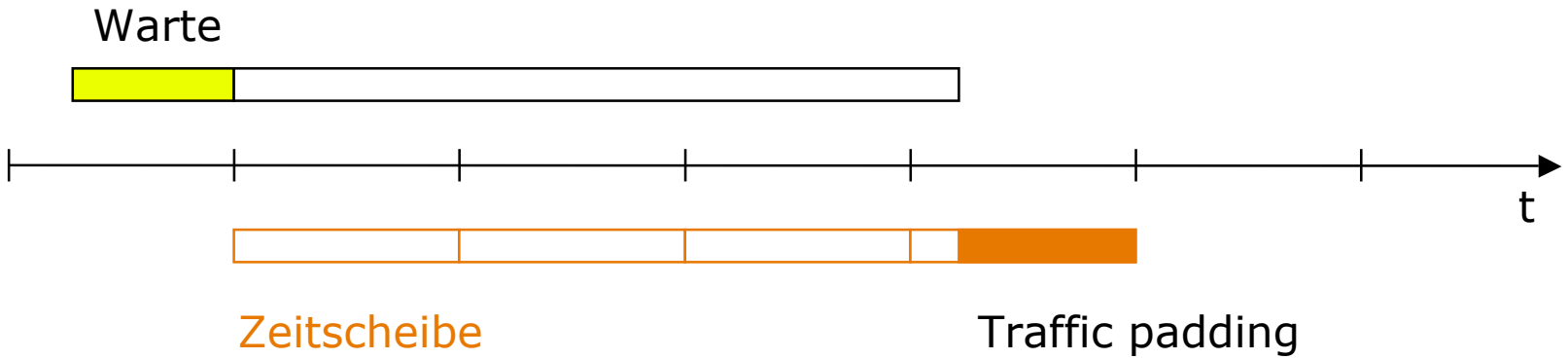
1. Warten, bis genügend Benutzer kommunizieren wollen (Bilden der Anonymitätsgruppe)
   Beispiel: 5 Nutzer

2. Nach Kommunikationsende senden die Nutzer solange Zufallszahlen, bis der letzte Nutzer seine Kommunikation beendet.

3. Problem: Niemand weiß, wann der letzte Nutzer seine Kommunikation beenden möchte, da niemand echte Nachrichten von Traffic padding unterscheiden kann.

> Zeitscheiben und Traffic padding

- Lösung: Zerlegen der Kommunikation in kleine Scheiben, genannt Zeitscheiben oder Volumenscheiben
  - Unbeobachtbarkeit innerhalb der Gruppe aller Nachrichten einer Zeitscheibe
  - Längere Kommunikationsverbindungen setzen sich aus mehreren Zeitscheiben zusammen
  - Zeitscheiben sind nicht verkettbar für Angreifer



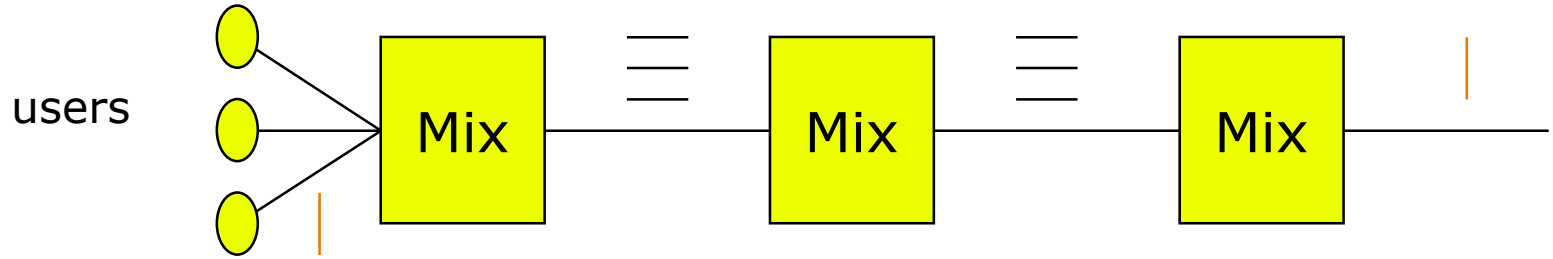
> Dummy traffic

- Ziel: Verkehrsaufkommen in Situationen niedrigen Verkehrs künstlich erhöhen, um Anonymitätsgruppe zu vergrößern

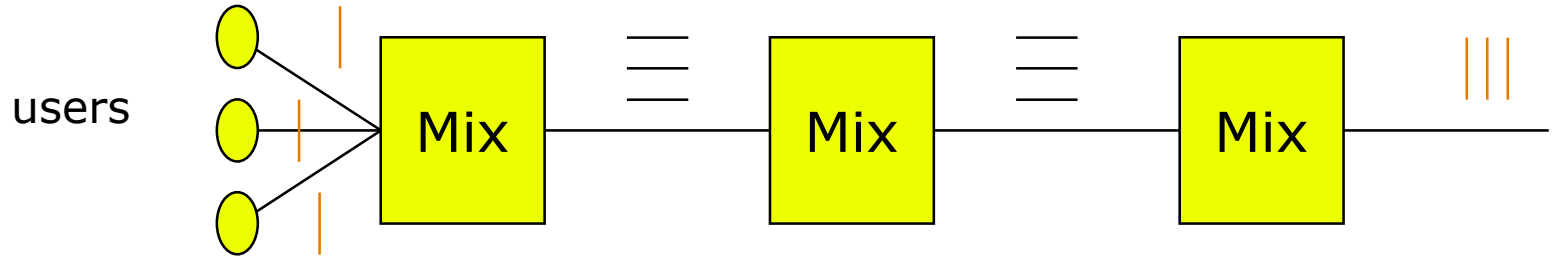
- Manchmal wird der Schub nicht voll, weil zu wenige Teilnehmer Nachrichten senden möchten
- Auswege:
  - Warten, bis weitere Nachrichten eintreffen (führt zu weiteren Verzögerungen)
  - Akzeptieren, dass Anonymitätsgruppe klein bleibt
  - Nutzer, die nichts zu senden haben, senden bedeutungslose Nachrichten
- **Def.: Dummy traffic**. Ein Nutzer sendet ständig Daten. Wenn er keine (verschlüsselten) Nachrichten zu senden hat, sendet er Zufallszahlen, die nicht unterscheidbar sind von echten verschlüsselten Nachrichten.

>> Dummy traffic

- Dummy traffic nur zwischen Mixen reicht nicht aus



- Dummy traffic muss Ende-zu-Ende generiert werden



> Praxis: Anonymisierung im Internet

- Anonymisierung von Electronic-Mail:
  - Typ-0-Remailer: anon.penet.fi
    - Header entfernen und anonym/pseudonym weiterleiten
    - Reply möglich, da der echte Absender gespeichert und durch ein Transaktionspseudonym ersetzt wurde
    - Verkettbarkeit über Länge und zeitliche Korrelation
  - Typ-1-Remailer: Cyperpunk-Remailer
    - wie Typ-0, zusätzlich Angabe über Verzögerungszeit bzw. Sendezeit, Kaskadierung
    - PGP-verschlüsselte Mails werden vom Remailer entschlüsselt
    - Verkettbarkeit über Länge, bei niedrigem Verkehrsaufkommen auch über zeitliche Korrelation
  - Typ-2-Remailer: Mixmaster (Cottrel, 1995)
    - sammeln von Nachrichten
    - Mix-Modell im Pool-Mode
    - alle Nachrichten haben gleiche Länge

> Anonymisierung von Verbindungen (HTTP, FTP)

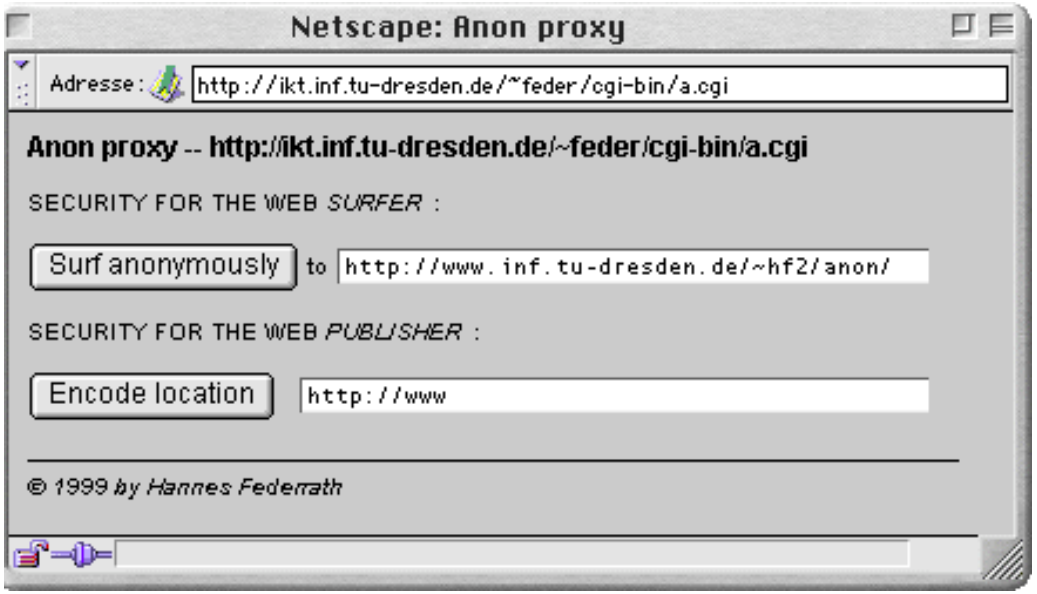
⌘ Client-Anonymität

- Einfache Proxies (teilweise mit Filterfunktion: Cookies, JavaScript, active content)
  - Anonymizer.com (Lance Cottrel)
  - Aixs.net
  - ProxyMate.com (Lucent Personal Web Assistant, Bell Labs)
  - Rewebber.com (Andreas Rieke, Thomas Demuth, FernUni Hagen)
  - Jeder entsprechend konfigurierte Web-Proxy

- Verkehrsanalysen berücksichtigende Verfahren
  - Onion-Routing (Naval Research Center)
  - Crowds (Mike Reiter, Avi Rubin AT&T)
  - Freedom (Ian Goldberg, Zero-Knowledge Inc.)
  - WebIncognito (Privada)
  - Web-Mixe/JAP (TU Dresden)

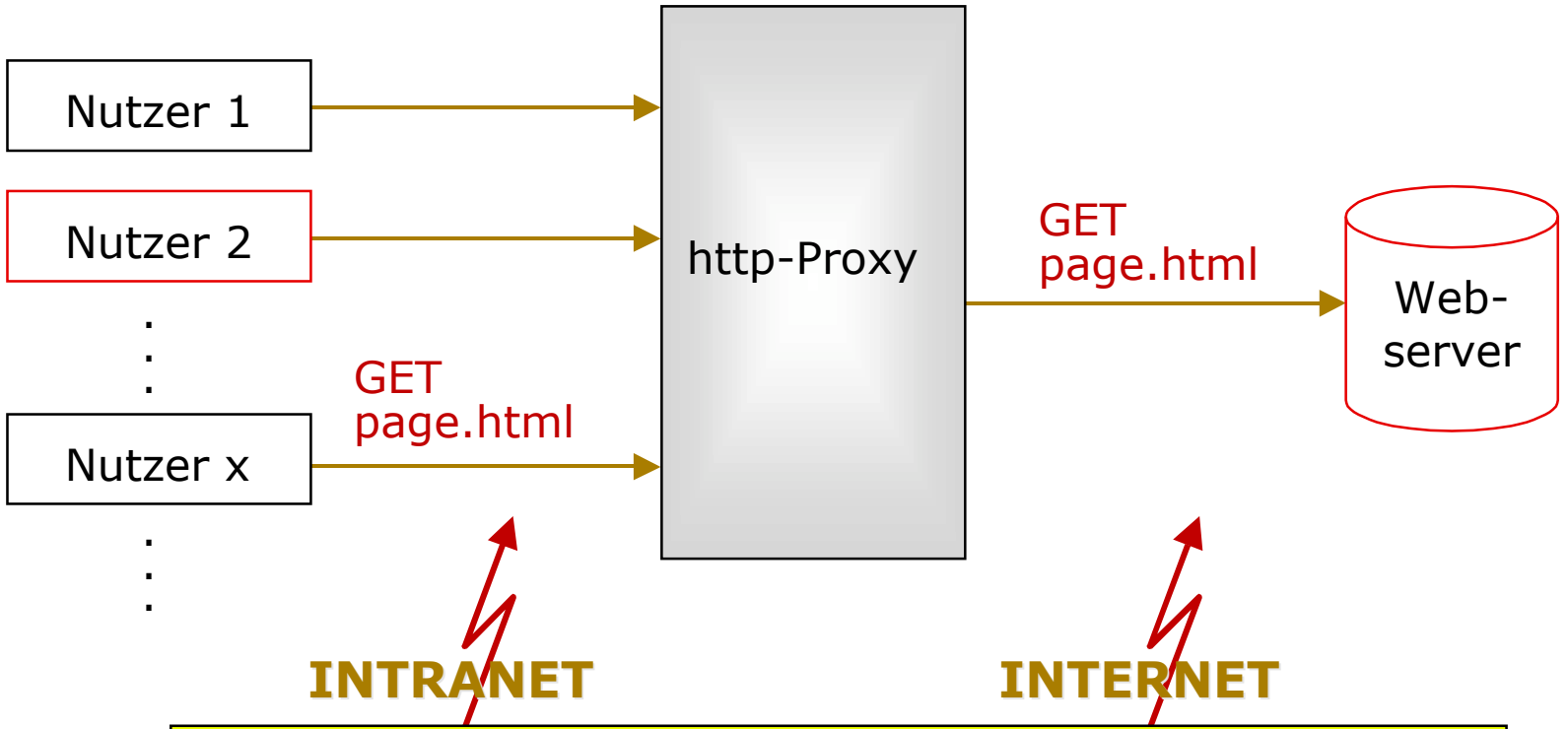
> Einfache Proxies

- Server besitzt keinerlei Information über den wirklichen Absender eines Requests
- **Kein Schutz gegen den Betreiber des Proxy**
- **Kein Schutz gegen Verkehrsanalysen**



- **Arbeitsprinzipien für Webzugriff:**
  1. **Formularbasiert**
     - URL eingeben
     - Proxy stellt Anfrage und versieht eingebettete URLs mit einem Präfix
  2. **Browserkonfiguration ändern**
     - »use proxy«

>> Einfache Proxies

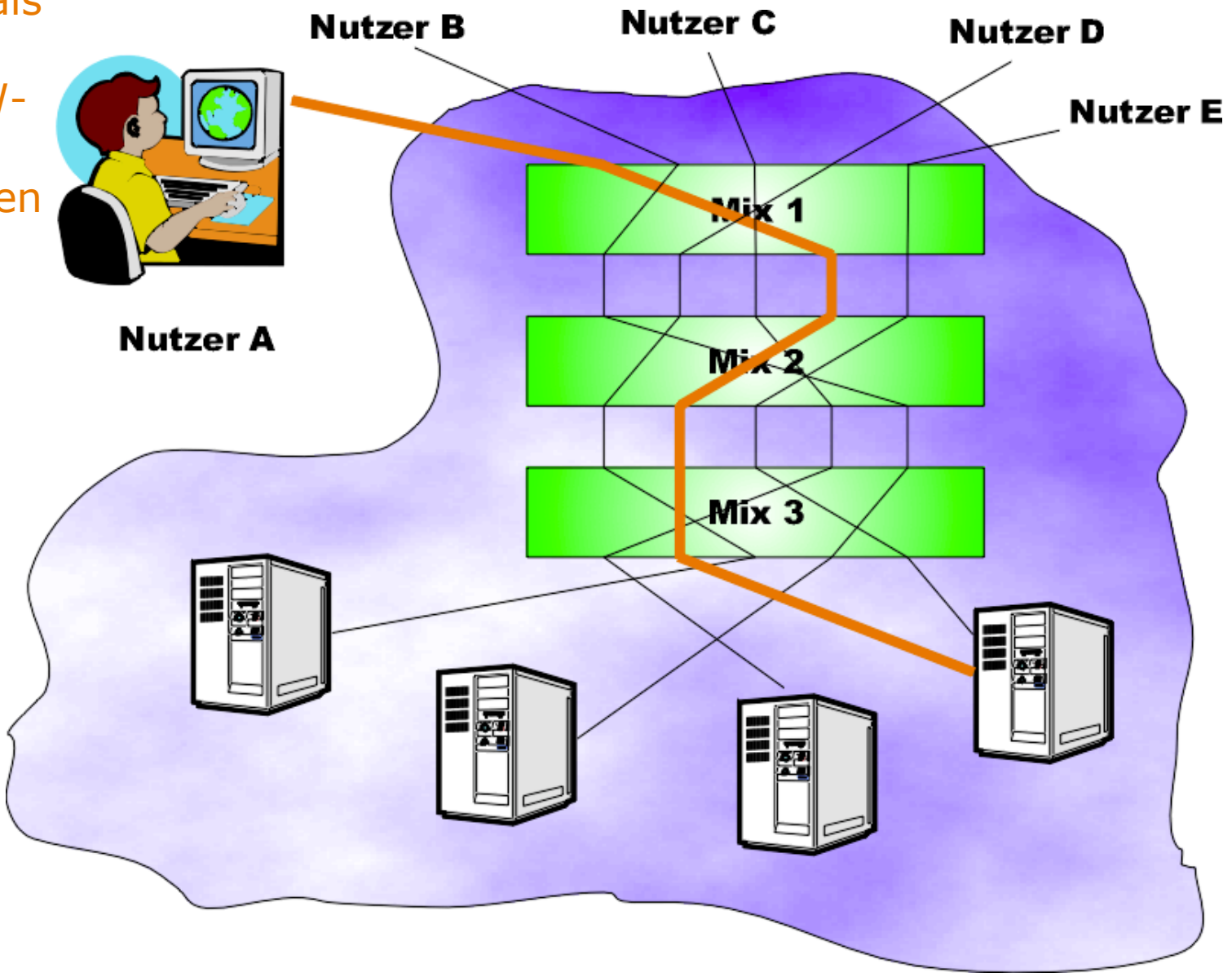


- Beobachtung und Verkettung ist möglich
  - zeitliche Verkettung
  - Verkettung über Inhalte (Aussehen, Länge)

Verschlüsselung zwischen Browser und Proxy verhindert Korrelation über »Aussehen«, aber nicht über Nachrichtenlänge und Zeit und hilft nichts gegen den Proxy.

JAP/WebMixe

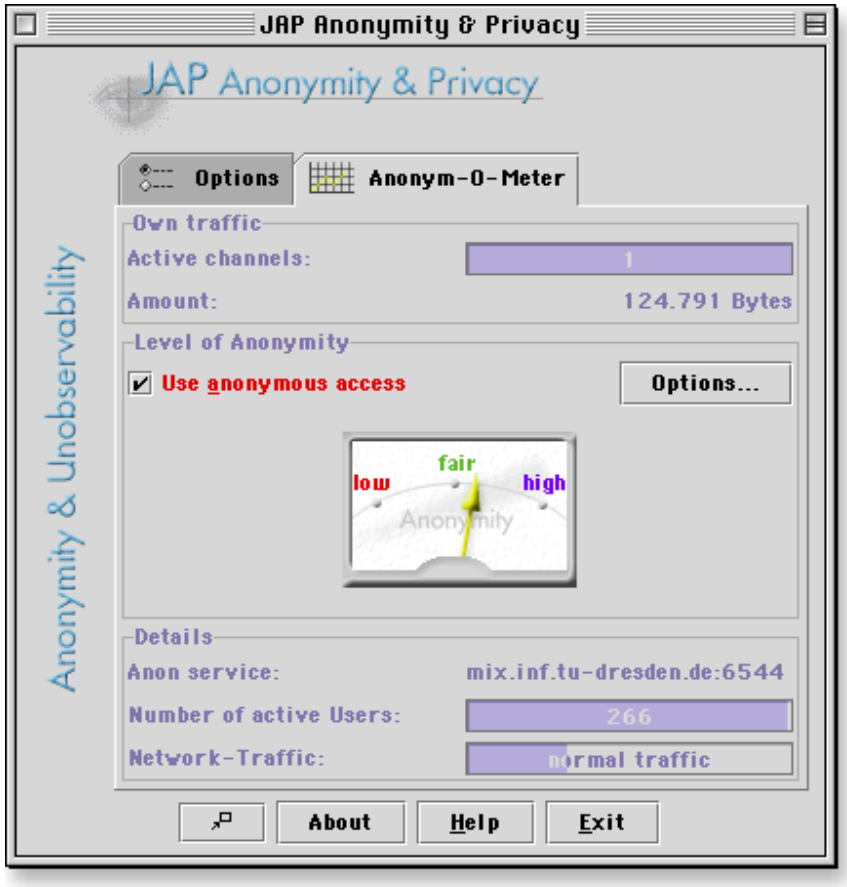
- JAP wird als Proxy für den WWW-Browser eingetragen



Technische Daten, Nutzerzahlen

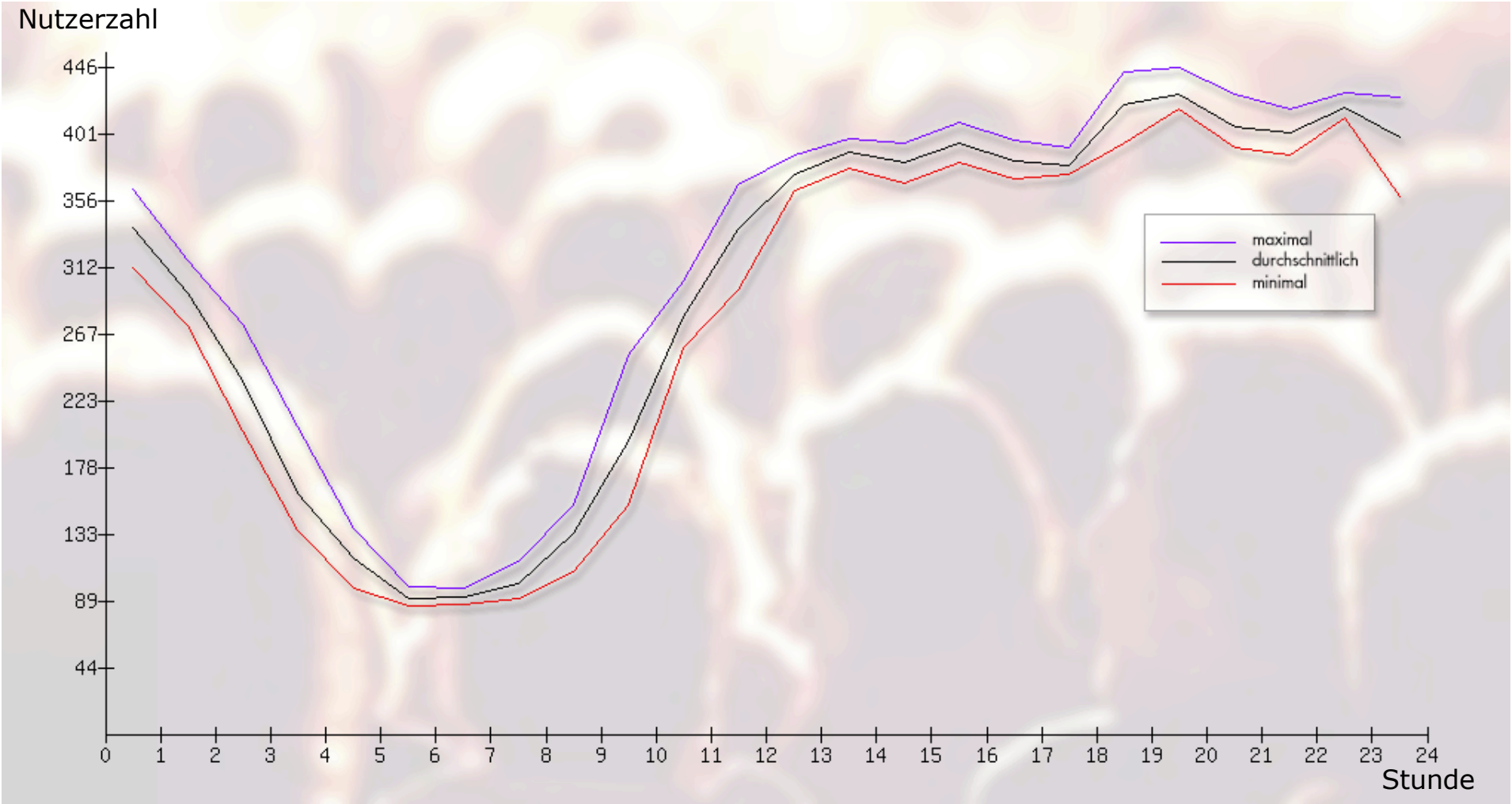
JAP.inf.tu-dresden.de

- Entwicklung eines praktisch nutzbaren Systems zum unbeobachtbaren Surfen im Internet
  - Schutz von personenbezogenen Daten bei der Benutzung des Internet
  - Verhinderung von »Profiling« und kommerzieller Nutzung
- Implementierung bestehend aus:
  - Java Client Programm »JAP«
  - Mix-Server (C++)
  - Info-Service (Java)
- Schätzung:
  - insgesamt ca. 18000 Nutzer
- Netzwerkverkehr ist zur Zeit der Hauptengpass:
  - ca. 1000 Gigabyte pro Monat
  - bei bis zu 650 Nutzern gleichzeitig online
  - zu Spitzenzeiten etwa 2000 Transaktionen (URLs) pro Minute
- 3 Mix-Kaskaden im Betrieb



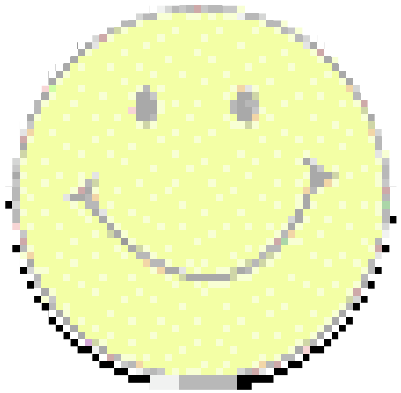
Nutzung

⌘ Typischer Verlauf der Nutzerzahl eines Tages



Positive Erfahrungen

- Vorstellung auf der CeBit 2001 und 2002
  - Im Gegensatz zu 1997 wird heute nicht mehr gefragt, wogegen man sich eigentlich schützen soll.
- Größeres Interesse am Datenschutz und im Bewusstsein um Bedrohungen
  - Hohe Bereitschaft praktikable Lösungen zum Selbstdatenschutz einzusetzen
- Kommerzielles Interesse
  - Vermarktung als Dienstleistung geplant



Negative Erfahrungen

- Sehr schwer vermittelbar, warum ein System sicher bzw. unsicher ist
  - Verbreitete Vorstellung: ständig wechselnde IP-Adresse = hohe Anonymität
- Mißbrauchsfälle aufgetreten
  - Dienst zur Zeit auf Web-Zugriffe beschränkt, obwohl allgemeiner anonymer TCP/IP möglich wäre
  - Nach juristischer Prüfung ist der Dienst legal, jedoch Überlegungen zur Deanonymisierung
  - Neue Forschungsfrage: Wie kann begründete Deanonymisierung ohne Massenüberwachung durchgeführt werden?
- Länder (Saudi Arabien) haben Zugang zum Dienst gesperrt
  - Forschungsfrage: Anonymisieren des Anonymisierungsdienstes

JAP Website

JAP Anonymity & Privacy

ANONYMITY IS NOT A CRIME

Kostenloser Download von JAP

http://jap.inf.tu-dresden.de

Weitere Informationen zur Anonymität im Internet

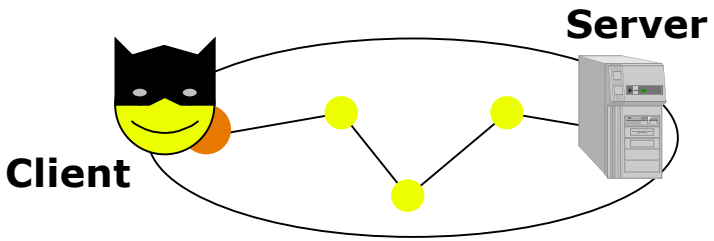
http://www.inf.tu-dresden.de/~hf2/anon/

> Empfehlungen für sicheres Surfen

WORLD WIDE WEB

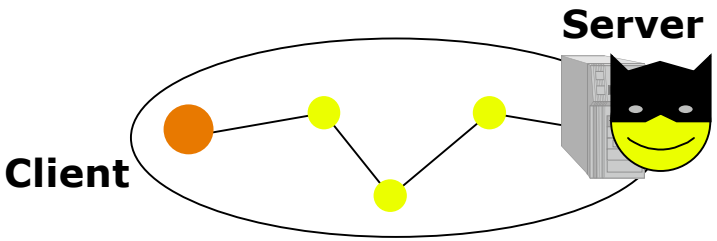
Client-Anonymität

Anonymes Abrufen fremder Inhalte



Server-Anonymität

Anonymes Publizieren von Inhalten



> Empfehlungen für sicheres Surfen

WORLD WIDE WEB

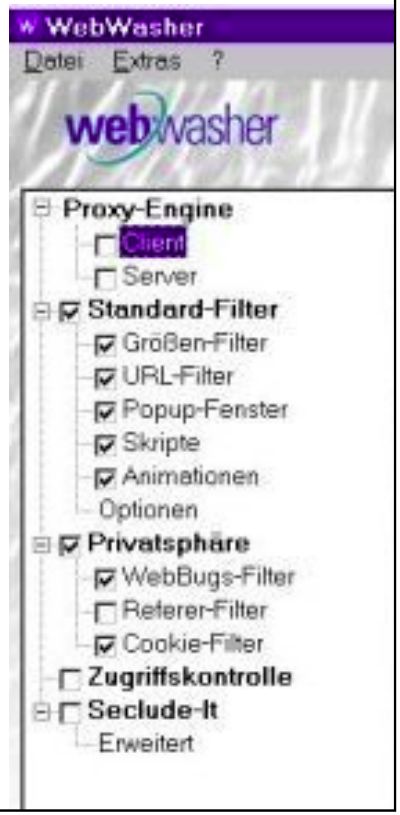
Client-Anonymität

Anonymes Abrufen fremder Inhalte

Server-Anonymität

Anonymes Publizieren von Inhalten

- **Cookies** und andere Verkettungsmerkmale **deaktivieren**
  - Web Server kann alle Benutzeraktivitäten *verketten*
  - Zusätzlicher Filter nützlich
    - http://www.webwasher.com/
    - http://www.junkbusters.com/ijb.html
  - Ebenfalls filtern: »Web Bugs« (transparente 1x1-Grafiken)
- **Java** und JavaScript **im Browser deaktivieren**
  - IP-Adresse kann abgefragt und übermittelt werden
    - Teilnehmer u.U. *identifizierbar* durch Server
- **ActiveX** und andere **aktive Inhalte deaktivieren**
  - Unberechtigter Zugriff auf Systemressourcen (Festplatte etc.) möglich
- **Profil der Dienstnutzung kann zur Beobachtung führen**
  - Online-/Offline-Phasen
  - Gleicher Nutzer besucht gleiche Webseite häufiger
    - Aktionen *verkettbar*



GET http://anon.nowhere.com/
>please type in your name
>set cookie

>>> E-Commerce und Pseudonymität

E-Commerce
- Aufbau eines E-Shopping-Systems

Pseudonymität
- Verfahren für Pseudonyme Transaktionen

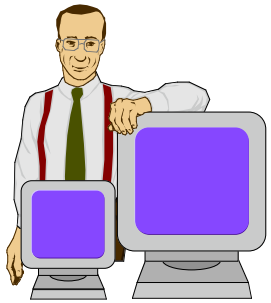
Pseudonyme
- Skalierbarkeit bzgl. des Schutzes

Anwendungen
- Pseudonyme Bestellungen
- Nym-Erzeugung in Freedom

> Aufbau eines E-Shopping Systems

Kunde K

Shopadministation, Händler



Storefront-Requests

Backoffice-Requests

Internet

Intranet

Storefront | Backoffice

Webadapter

Application Server

Catalog-Server

Transaction-Server

Daten-bank

Erweiterungsmodule

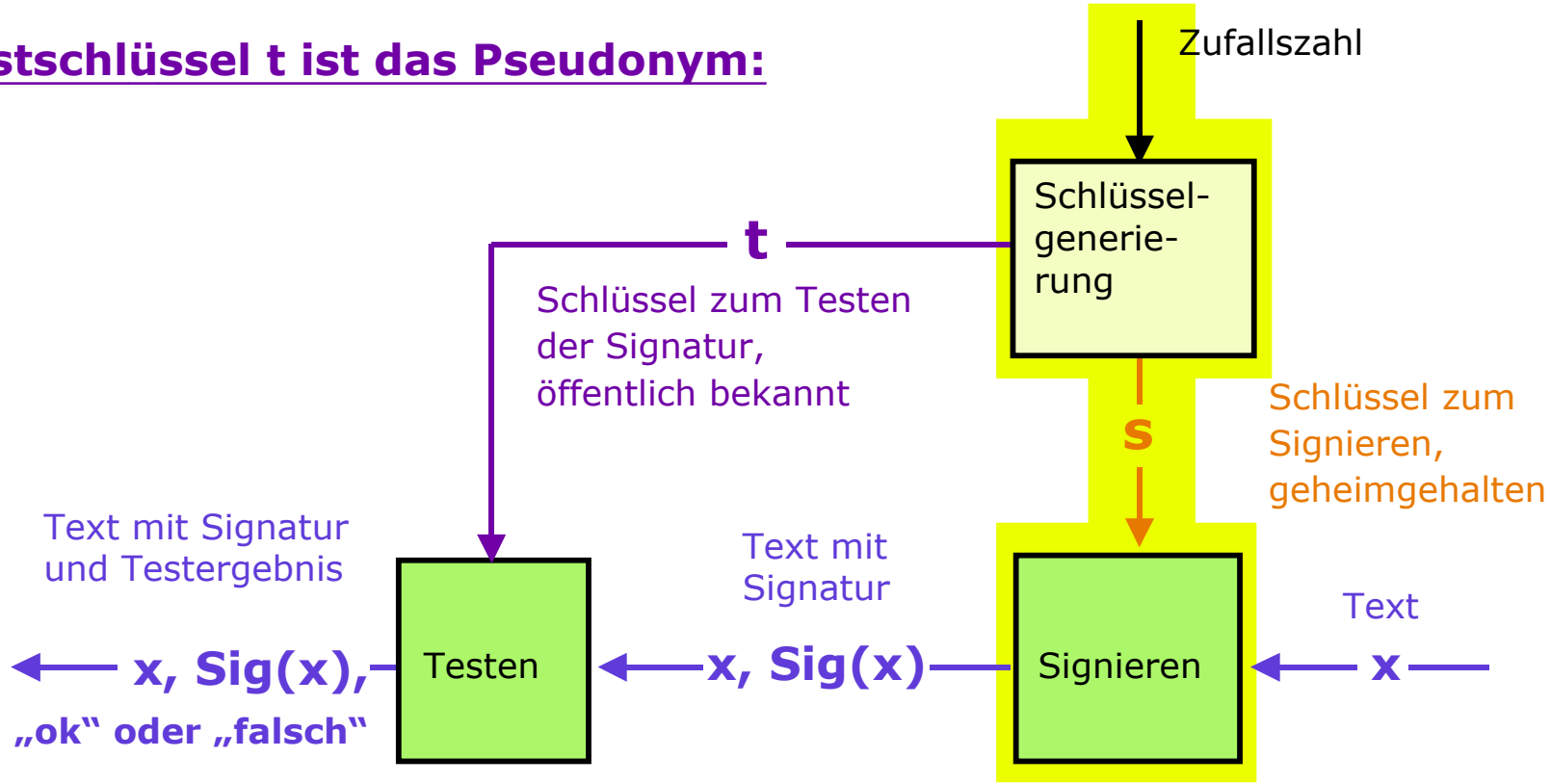
> Pseudonyme: Implementierungen

- Pseudonym-Arten
  - Vom Teilnehmer selbst gewählte Zeichenketten, die keinen Bezug zu seiner Identität besitzen
  - Große Zufallszahlen (etwa 45 Dezimalstellen)
  - Öffentliche Testschlüssel eines Signatursystems
- Pseudonyme zur Bestätigung von Eigenschaften
  - Einfaches »qualifizierendes Zertifikat«
  - Blenden des Pseudonyms vor dem Zertifizieren
  - Secret-key Zertifikate

```
BEGIN ZERTIFIKAT
Pseudonym: 3045263427234662342498724137 5
Öffentlicher Testschlüssel des Pseudonyms:
h833hd38dddajscbicme098342k236egfkw74h5445
84hdbscldmrtpofjrkt0jshuedagaszw12geb3u4b=
Bestätigte Eigenschaften:
Der Inhaber ist über 18 Jahre alt.
Der Inhaber ist deutscher Staatsbürger.
Datum: 19.03.2000
Gültig bis: 18.03.2001
Aussteller: Einwohnermeldeamt Dresden
Signatur des Ausstellers:
23j423vdsaz345kj435ekji3u4z2983734ijo23i72
kj867wdbez2o074j5lkdmcdkki1237t3rgbdvbwdj=
END ZERTIFIKAT
```

Signatursystem für Pseudonmität verwenden

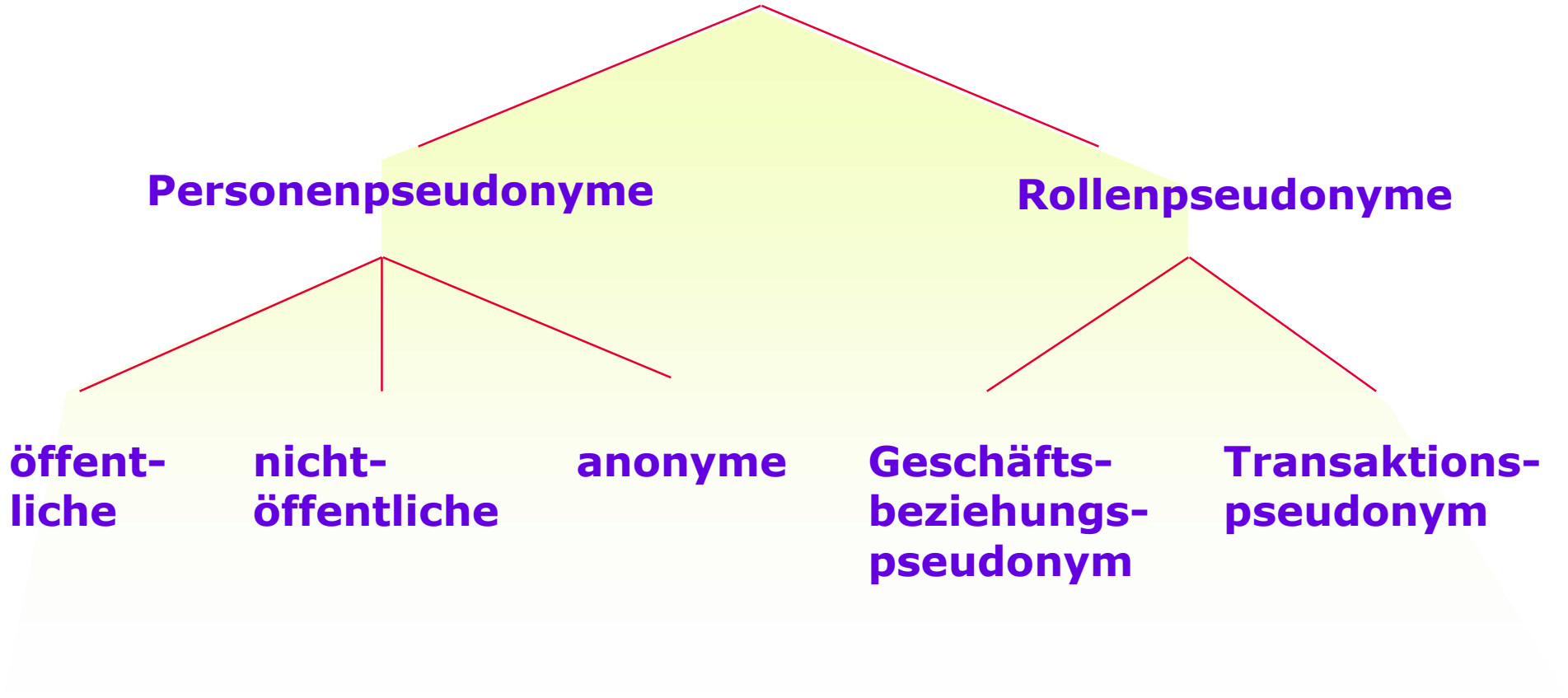
Testschlüssel t ist das Pseudonym:



Bereits heute realisierbar mit PGP:

Pretty Good Privacy (PGP): http://www.pgpi.org/

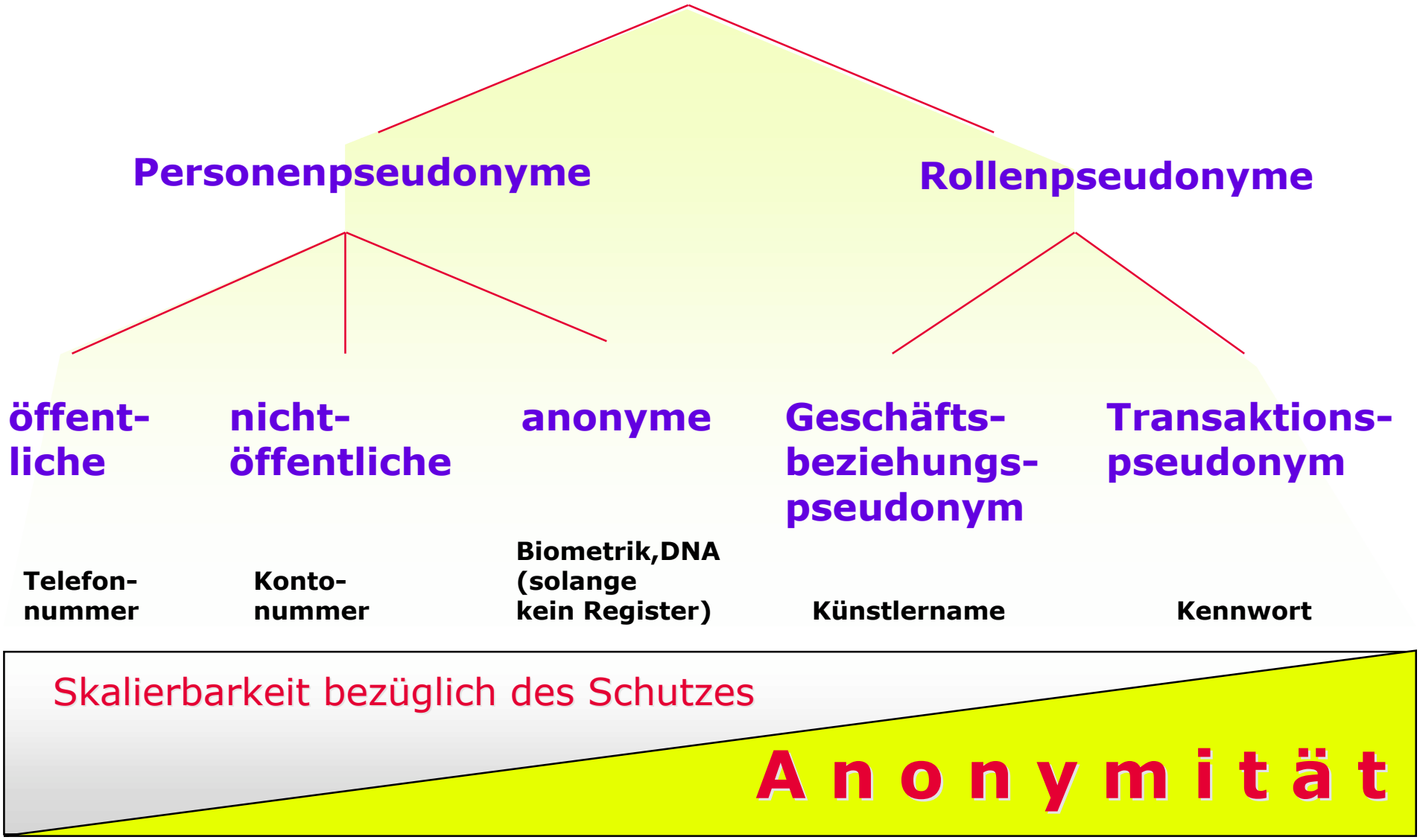
> Pseudonyme: Systematik



Skalierbarkeit bezüglich des Schutzes

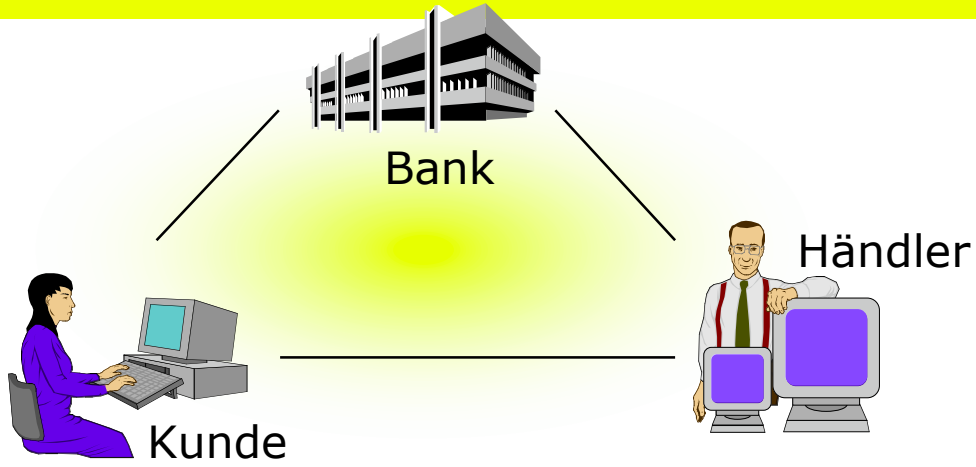
Anonymität

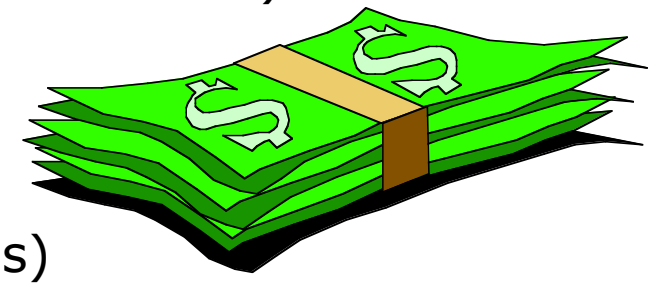
>> Pseudonyme: Beispiele



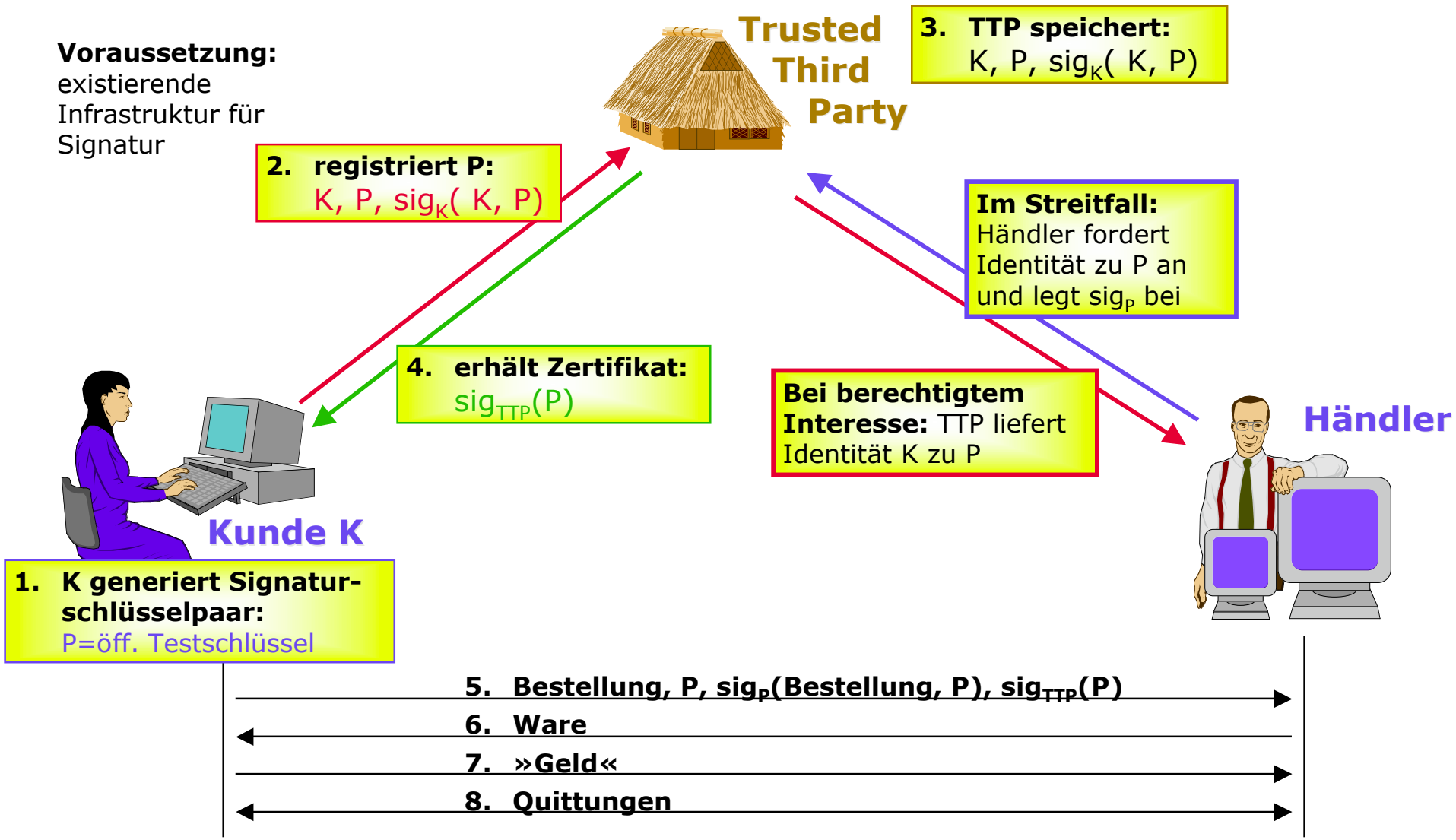
> Verfahren für pseudonyme Transaktionen

- Wer ist zu schützen?
  - Kunde
  - Händler
  - Bank
  - …
- Grundkonzepte:
  - Pseudonymität, d.h. dig. Signaturen relativ zu Pseudonym
    = öffentl. Testschlüssel
    - Identifizierung im Betrugsfall (Zertifizierungsinstanz, die Identität kennt):
      nicht kontrollierbar
    - Geldhinterlegung für Haftung (aktiver Treuhänder):
      kontrollierbar
  - Werteaustauschprotokolle
  - Digitale Zahlungssysteme
  - Umrechenbare Beglaubigungen (Credentials)





> Pseudonyme Bestellung von (digitalen) Waren



»Nym«-Erzeugung in Freedom