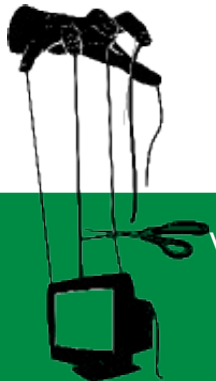
Verschlüsselung 2Go

Praxisworkshop

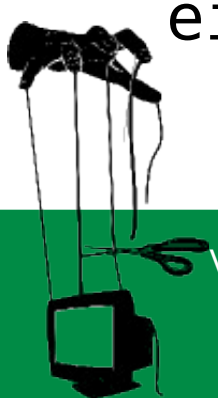


Schön, dass ihr da seid!

- Bevor es los geht noch ein kurzer Hinweis:
- Alle heute vorgestellten Programme, sowie Anleitungen und weiterführende Links findet ihr unter

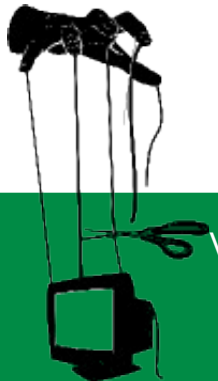
http://wiki.vorratsdatenspeicherung.de/Ortsgruppen/Muenster/Verschluesselung2Go

- Alle Programme gibt es heute auch zum Mitnehmen (Installation, USB-Stick oder CD) – fragt uns einfach



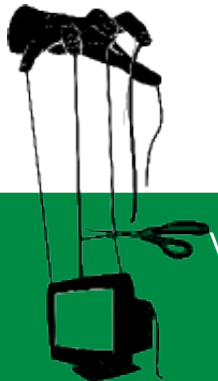
Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches



Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches



Warum eigentlich?

AK VORRAT

- Digitale Kommunikation ist alltäglich

GMX MAIL · MESSAGE · MORE

WEB.DE

skype

YAHOO!

Google Deutschland

msn

myspace .com

facebook

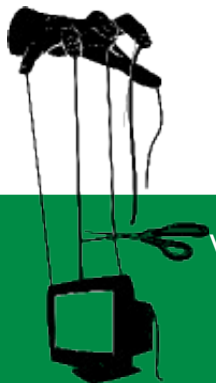
flickr

meinVZ

WordPress

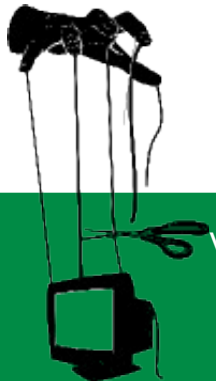
last·fm the social music revolution

twitter



Warum eigentlich?

- Riesige Mengen (persönlicher) Informationen stehen zum (gewollten) Zugriff bereit
- Daten ermöglichen Profilbildung (Freunde, Interessen, Aktivitäten, …)
- Interesse an euren Daten haben:
  - Staat
  - Wirtschaft
  - Privatpersonen



ALUMINIUM Baseballschläger 30' American Baseball

von Outdoor 4 You - Shop

(3 Kundenrezensionen) Mehr zu diesem Artikel

Preis: EUR 17,58

Auf Lager.
Verkauf und Versand durch **NORMANI**.

3 neu ab EUR 17,58

Marken-Uhren mit Tiefpreis-Garantie finden Sie im Uhren-Shop bei Amazon.de/Uhren.

Größeres Bild

Für Kunden: Stellen Sie Ihre eigenen Bilder ein.

Produktmerkmale

- Baseballschläger aus Aluminium
- mit rutschfestem Griff
- Absoluter Hammerpreis

Kunden, die diesen Artikel gekauft haben, kauften auch

Überlebensmesser, PVC-Scheide, Leichtmetallgriff

(2) EUR 11,49

Leder Quarzsandhandschuhe schwarz S-XXL

(4)
EUR 14,90 - EUR 17,95

Balaclava 3-Loch

(4) EUR 3,50

Wilson Baseball-Handschuh A300 NYY - RH

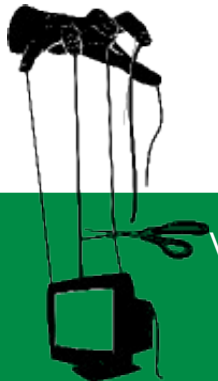
(1) EUR 20,99

Motivation

- Ziel: Kommunizieren, ohne dass Dritte unerwünscht mithören, -lesen, -schneiden, …

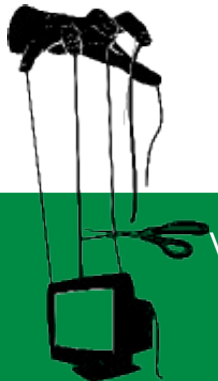
- Ansatz:
  - Inhalte unlesbar machen → Verschlüsselung
  - Kommunikation verschleiern → u.a. Verschlüsselung

Dazu nun ein paar Grundlagen...



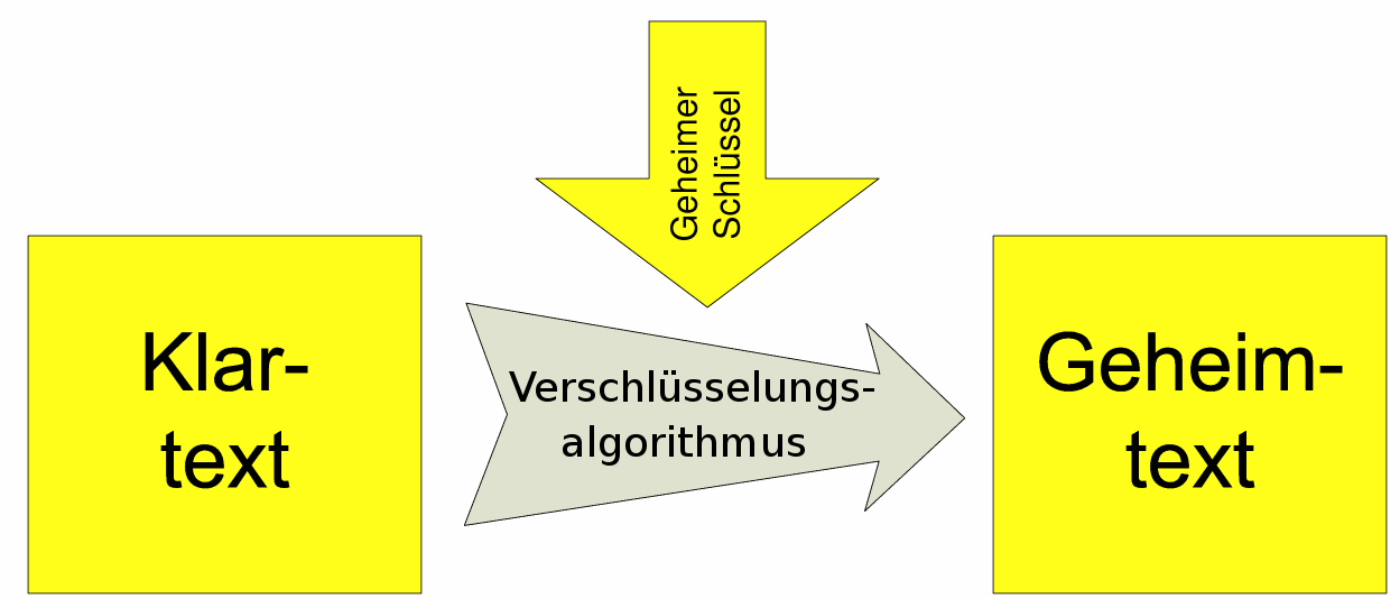
Agenda

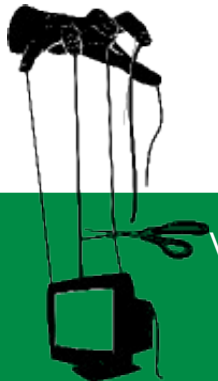
- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches



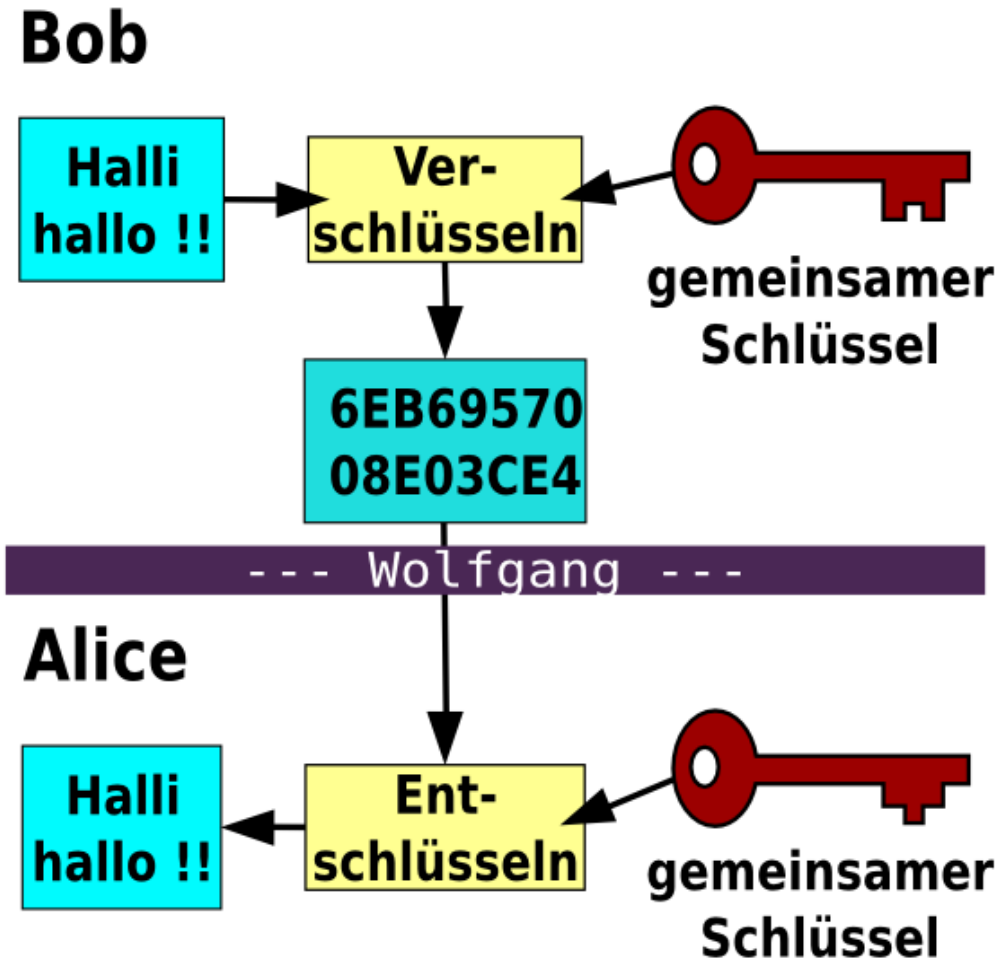
Verschlüsselung

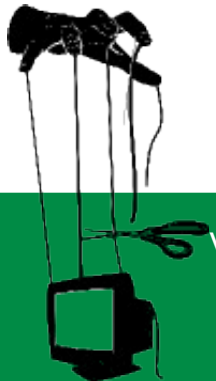
Der Vorgang eine klar lesbaren Information (Klartext) mit Hilfe eine Verschlüsselungsverfahren (Algorithmus) in eine „unleserliche“, nicht interpretierbare Zeichenfolge (Geheimtext) umwandeln.





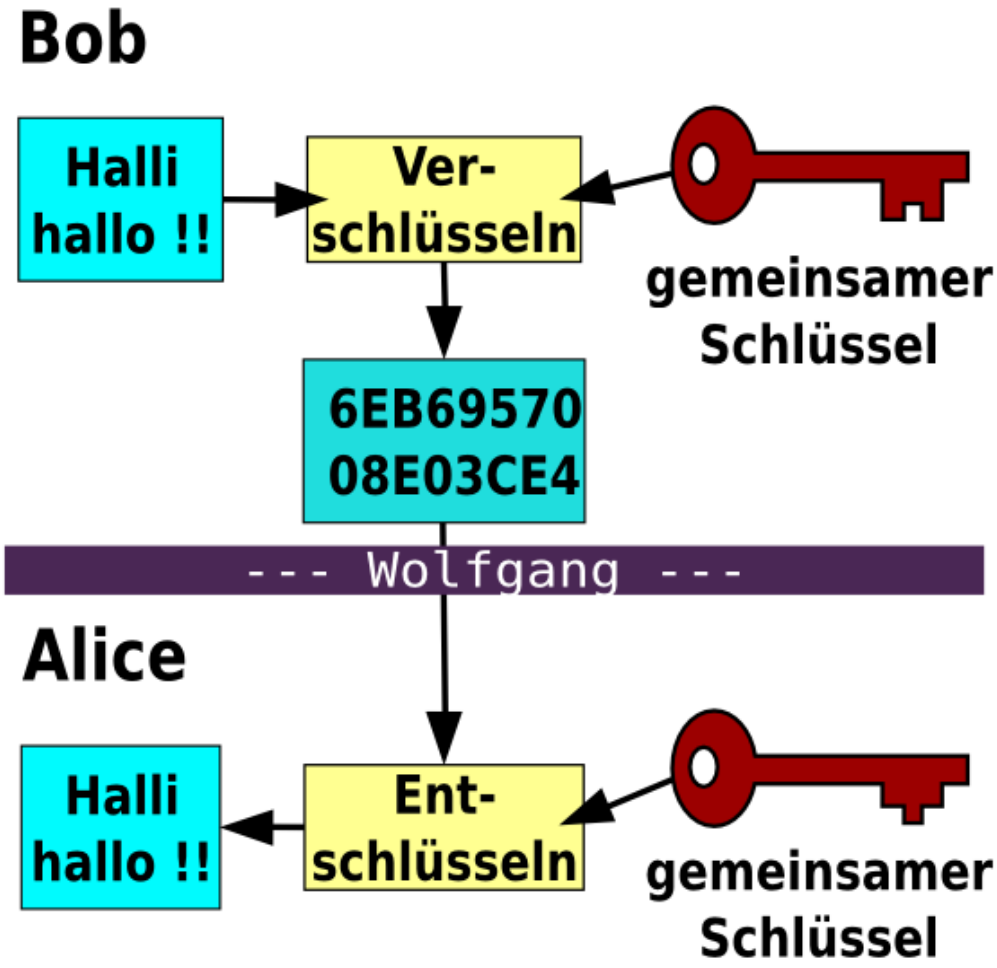
Symmetrische Verschlüsselung





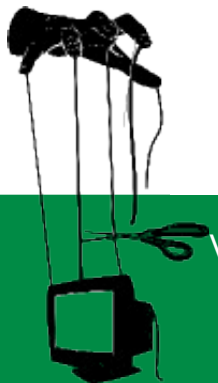
Verschlüsselung2Go

Symmetrische Verschlüsselung



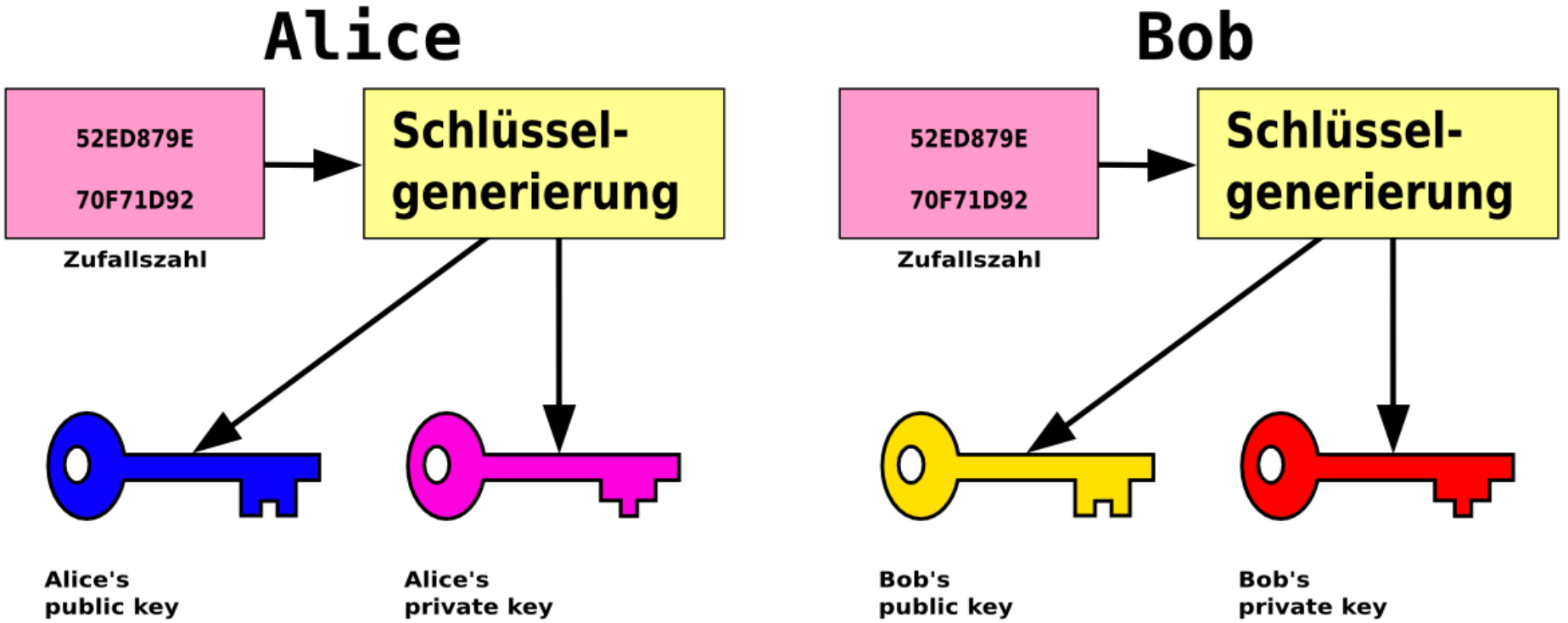
- Sehr starke Verschlüsselung
- Der Schlüssel muss über einen sicheren Kanal übertragen werden
- Viele Schlüssel benötigt

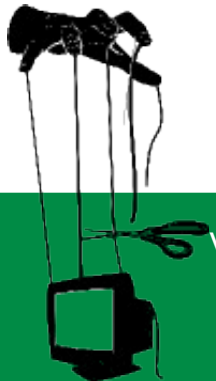
$$\frac{n \cdot (n - \backslash)}{2}$$



Verschlüsselung2Go

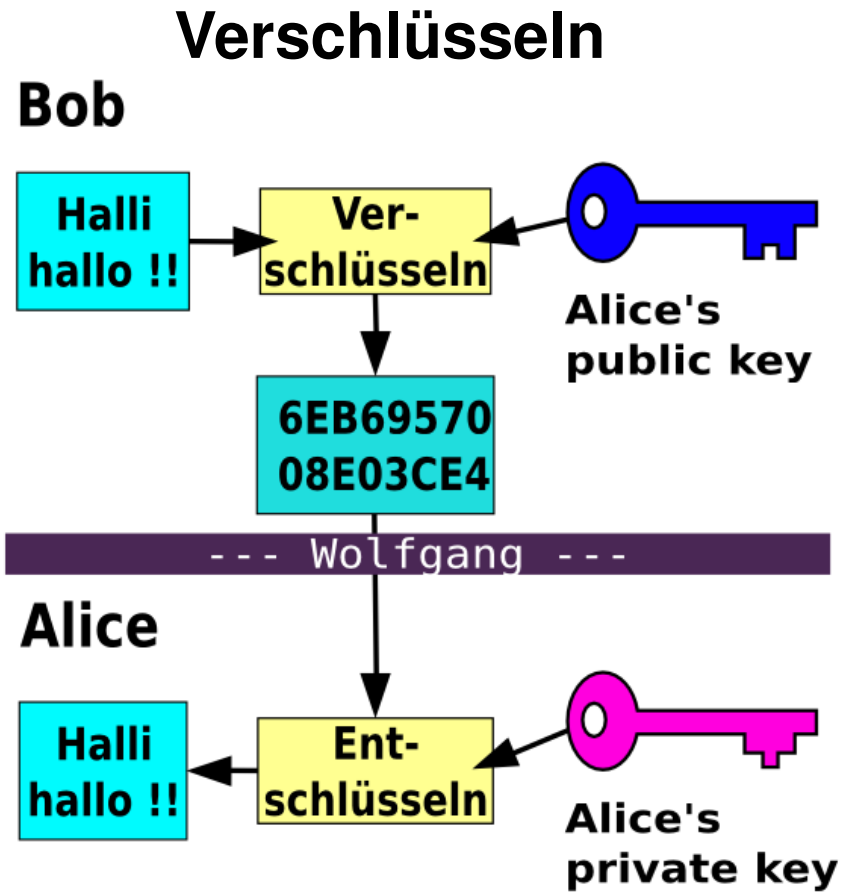
Asymmetrische Verschlüsselung

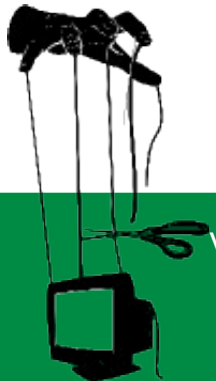




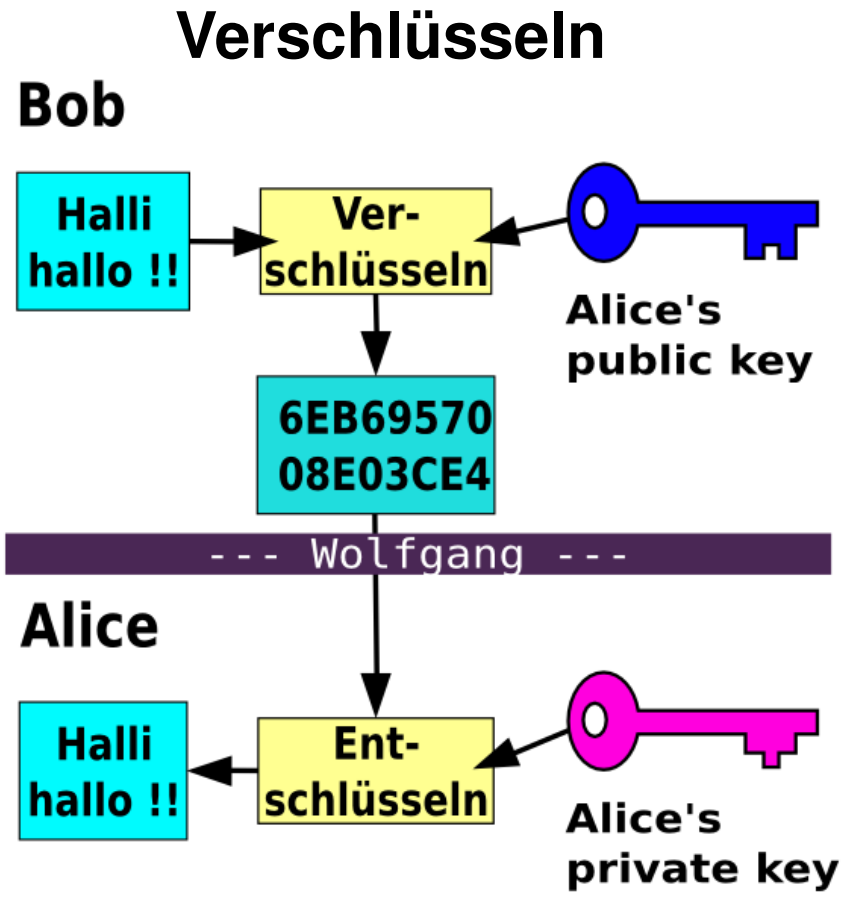
Verschlüsselung2Go

Asymmetrische Verschlüsselung





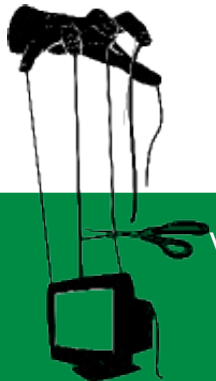
Asymmetrische Verschlüsselung



- Prinzip:

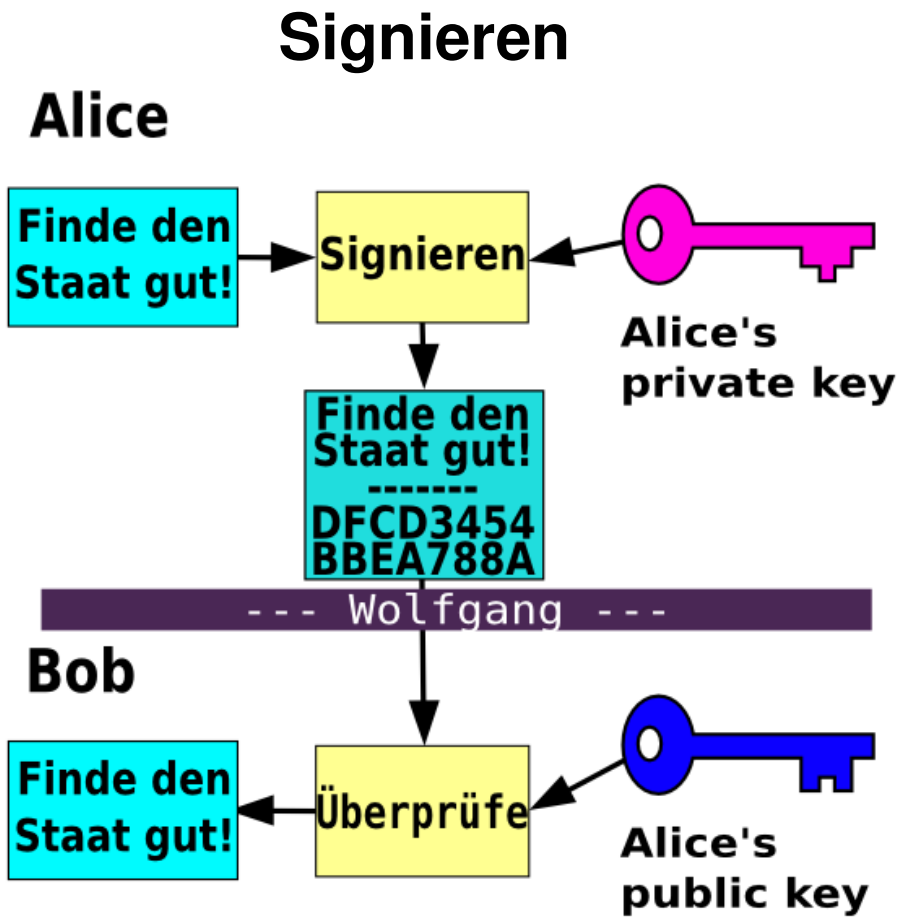
  17 * 23 = 391

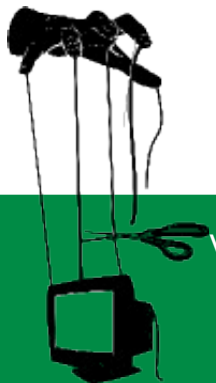
  391 = ???
- Komplexe (lange) Schlüssel benötigt
- Verfahren ist langsamer



Verschlüsselung2Go

Asymmetrische Verschlüsselung



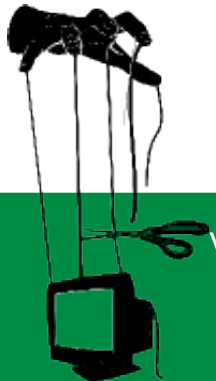


Verschlüsselung2Go

Verschlüsselung

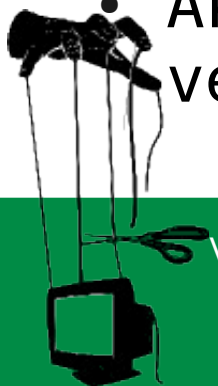
- Kerckhoffs' Prinzip:
  - Nachricht nicht entschlüsselbar ohne gültigen Schlüssel
  - Schlüsselsystem muß bekannt sein (Security by Obscurity)
  - Schlüssel muß leicht zu merken und auswechselbar sein
  - Chiffrierapparat und Dokumente müssen transportierbar sein
  - Das System muß einfach sein (ohne Expertenhilfe)

Mehr unter: http://www.cryptool.de



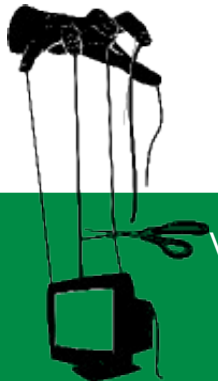
Portable Anwendungen

- Anwendungen, die ohne Installation laufen
- Können auf externen Datenträgern mitgenommen werden (Daten kommen mit)
- Keine Admin-Rechte für Benutzung notwendig
  - Können also auch in der Uni, bei der Arbeit genutzt werden
- Aktuell vor allem für Windows-Systeme verbreitet

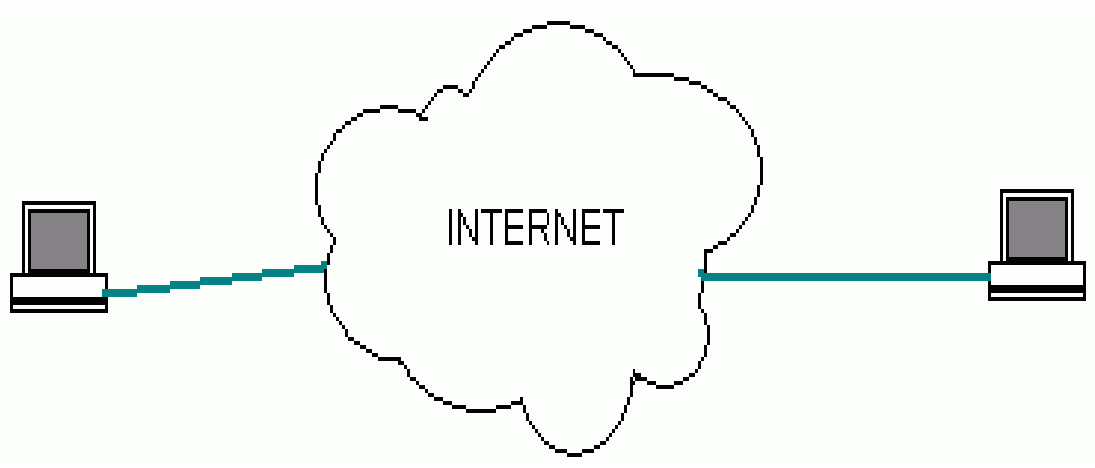


Agenda

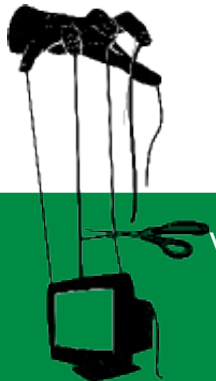
- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches



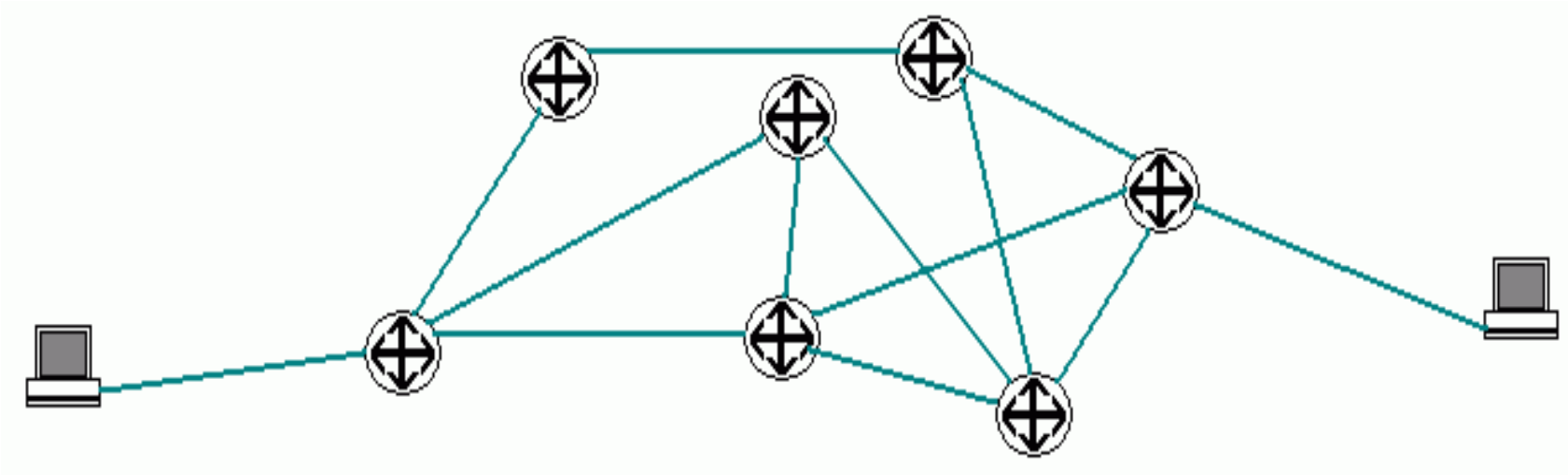
Surfen

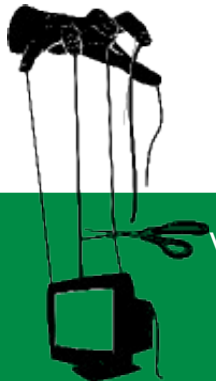


Wie es ungefähr funktioniert ...

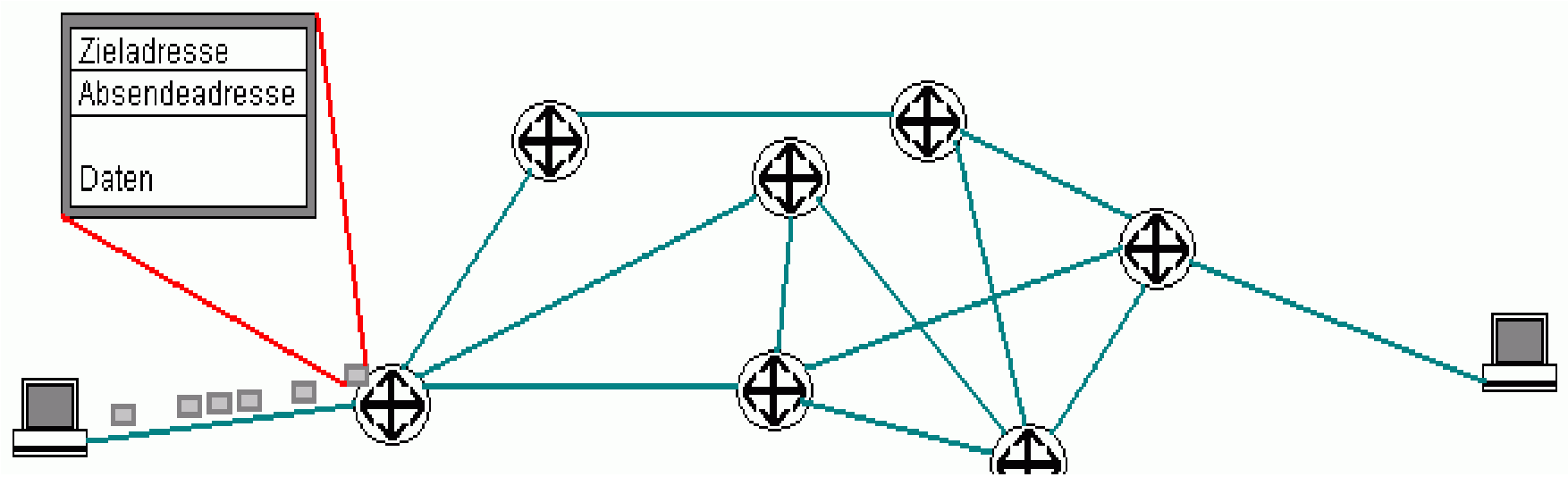


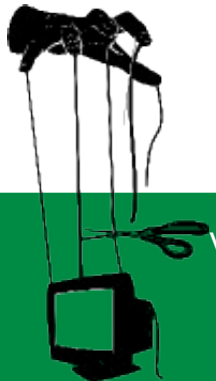
Surfen



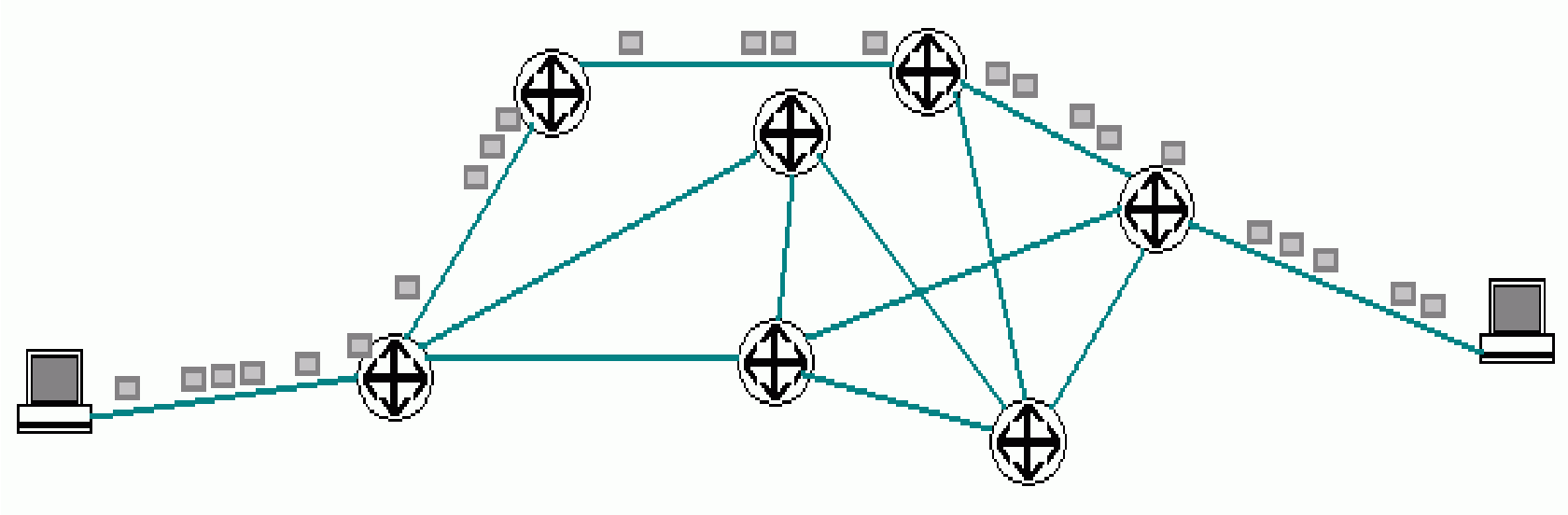


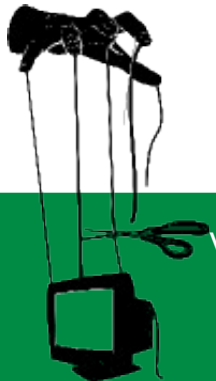
Surfen



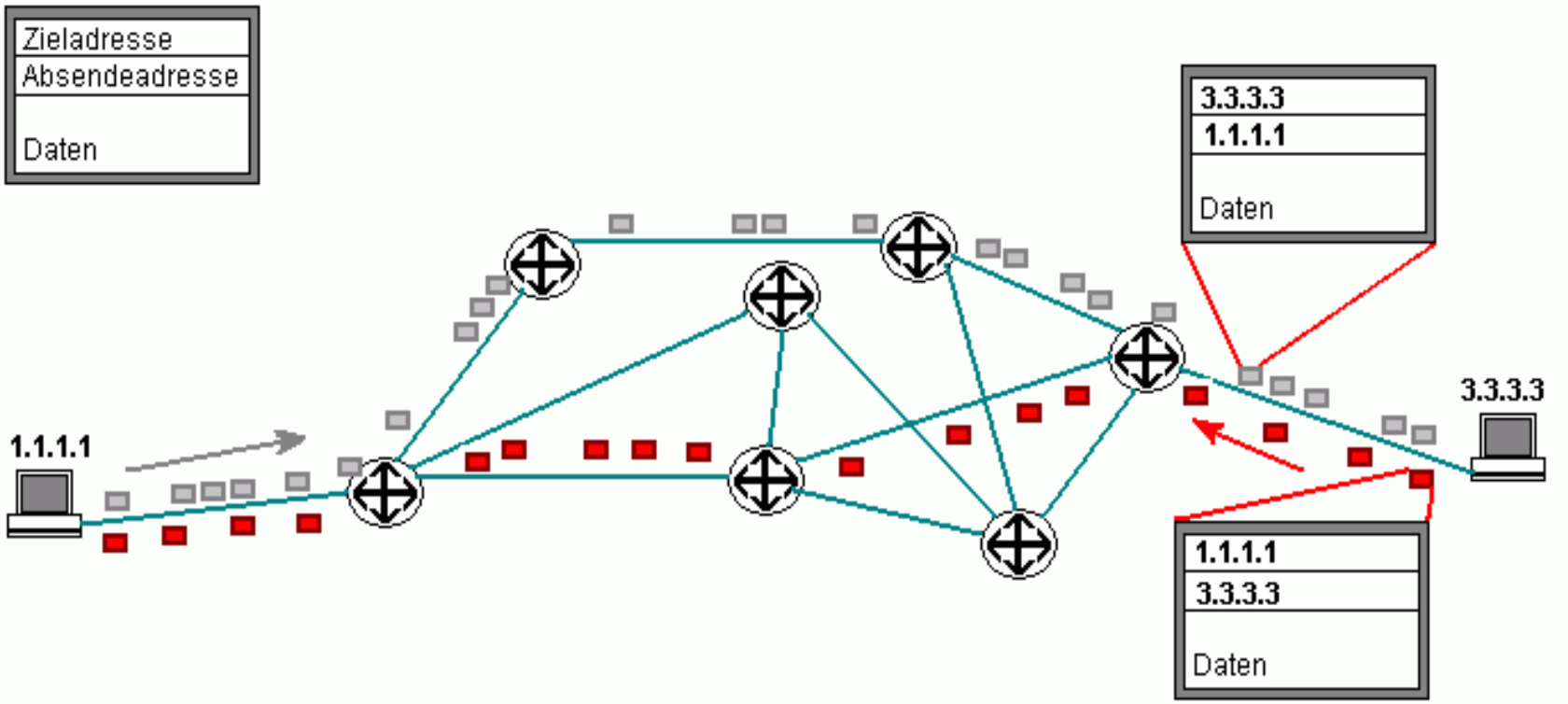


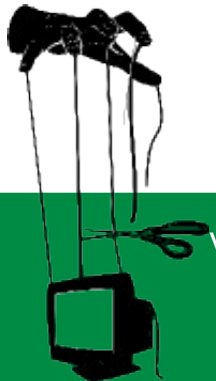
Surfen





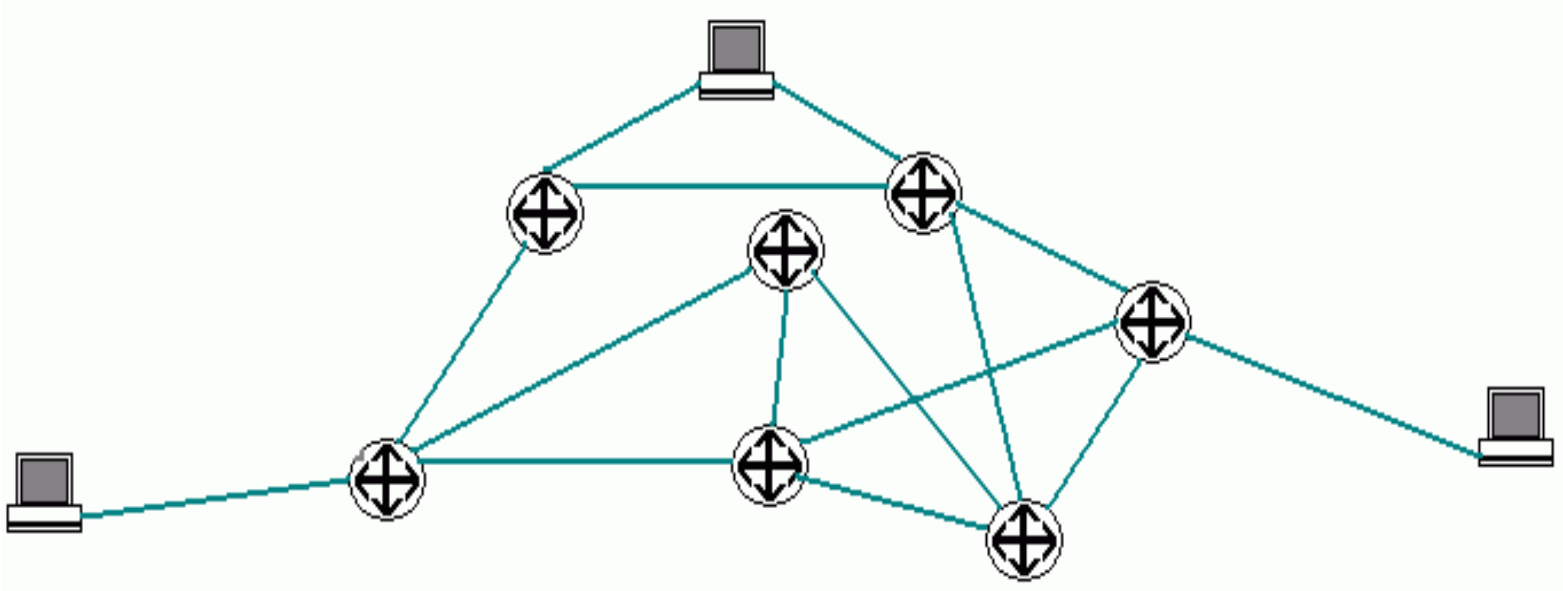
Surfen

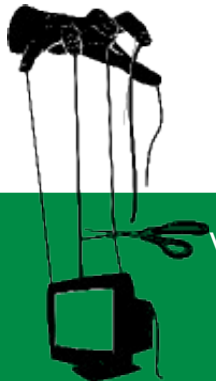




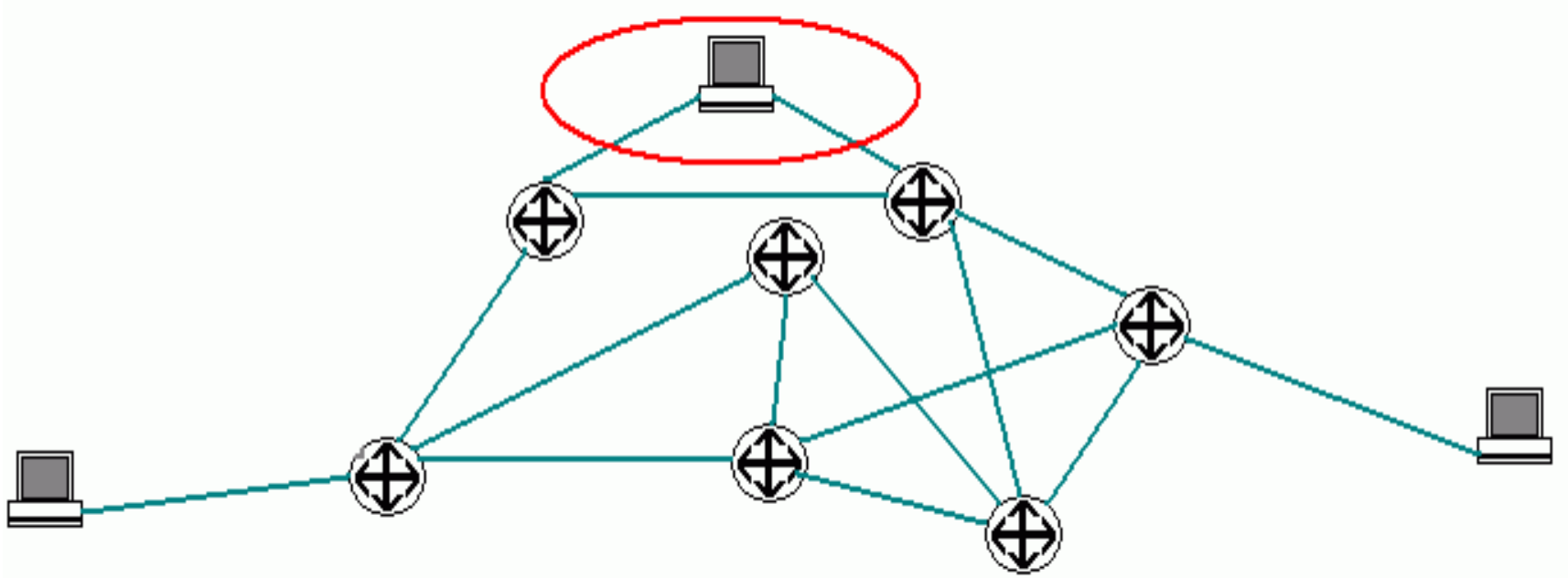
Verschlüsselung2Go

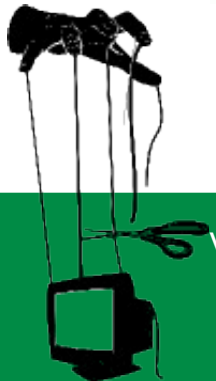
Surfen





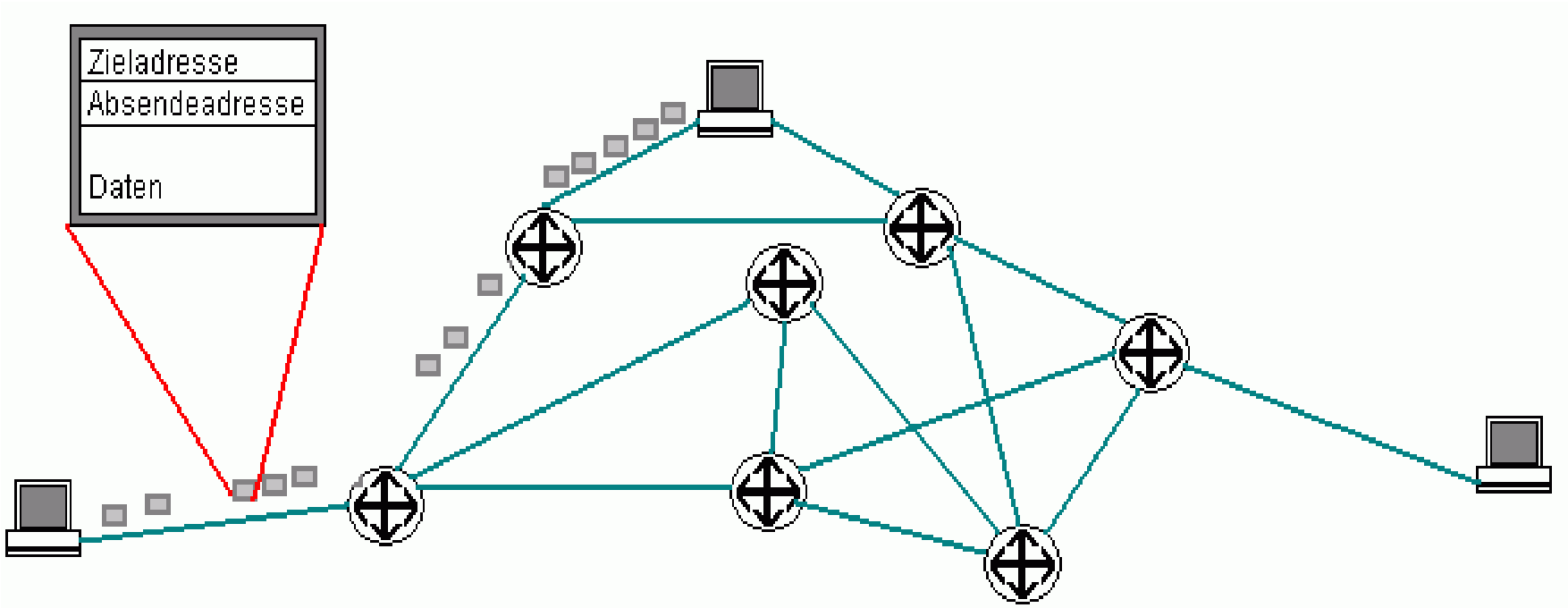
Surfen

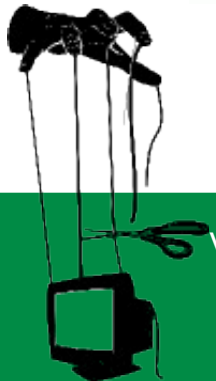




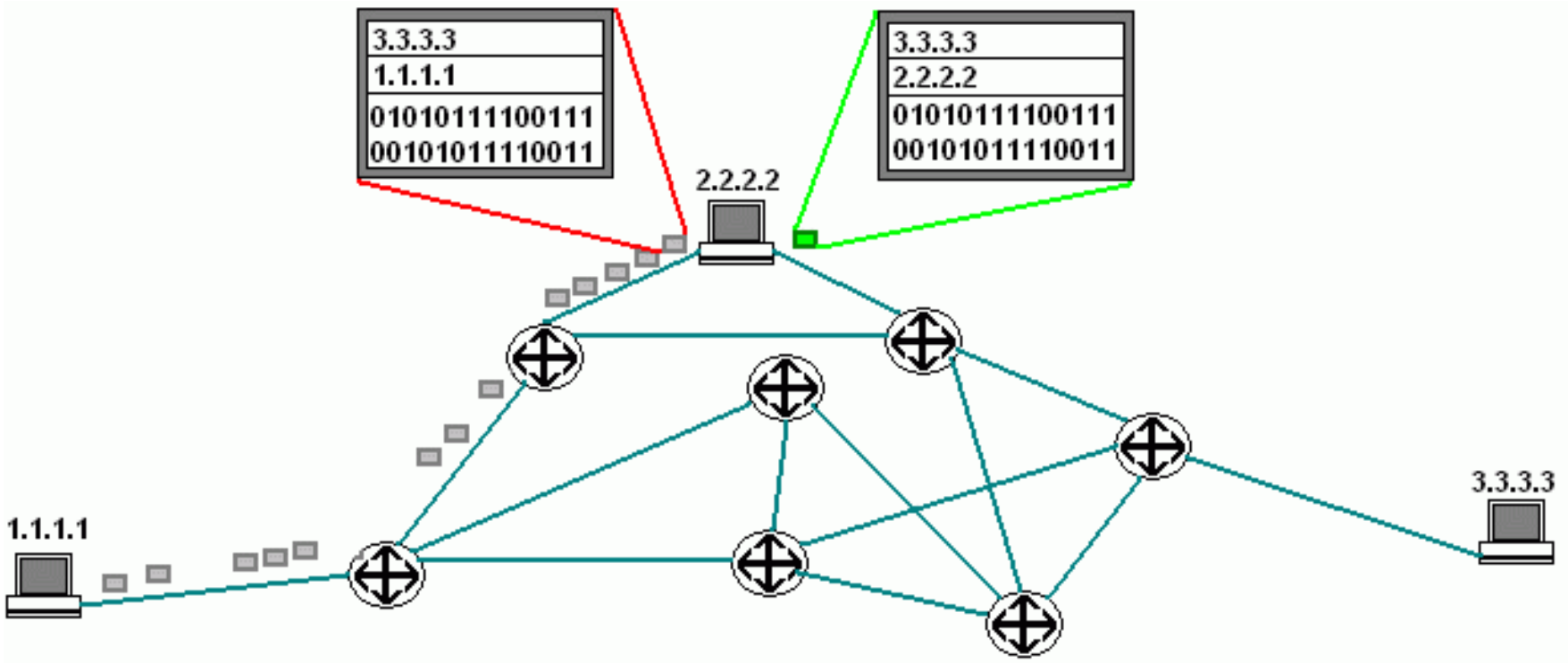
Verschlüsselung2Go

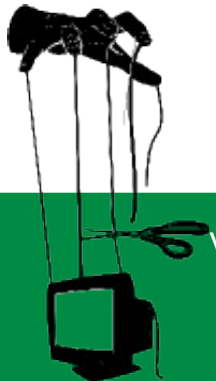
Surfen





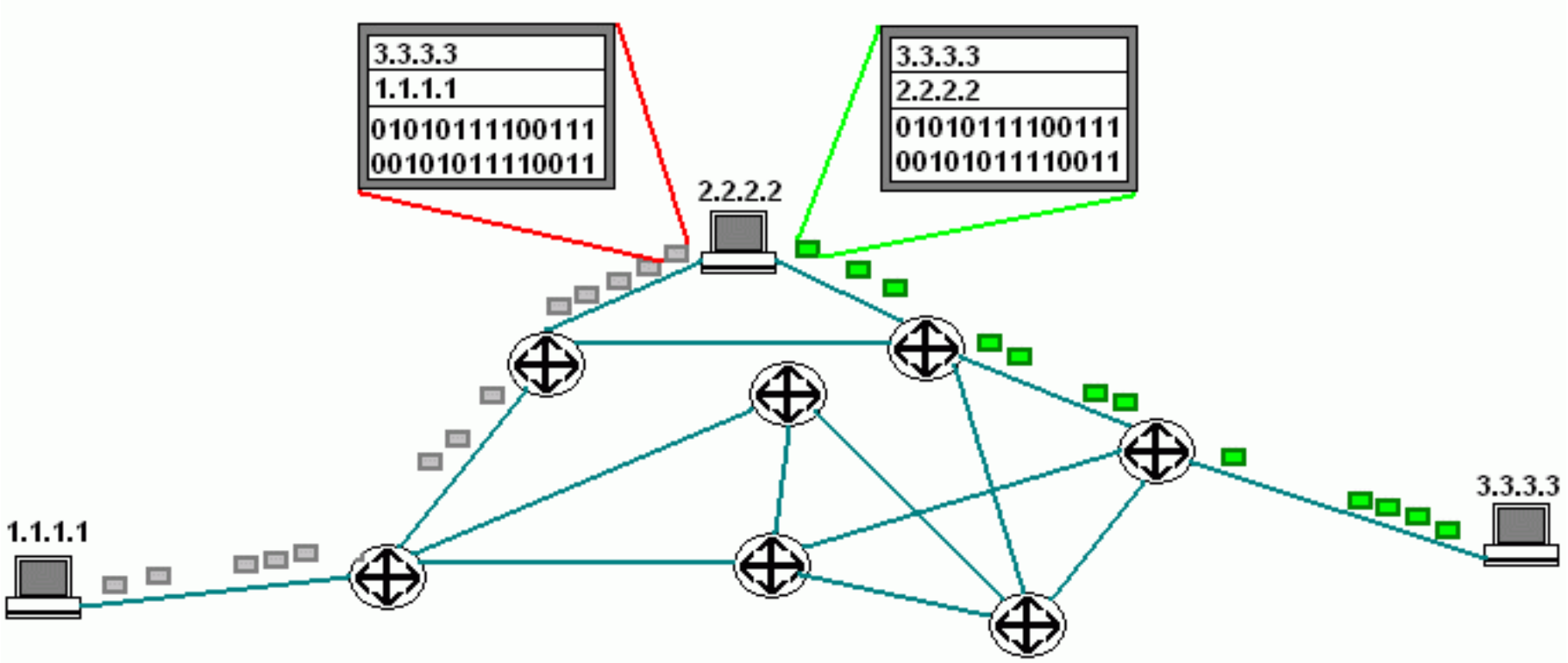
Surfen

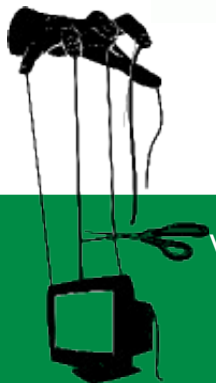




Verschlüsselung2Go

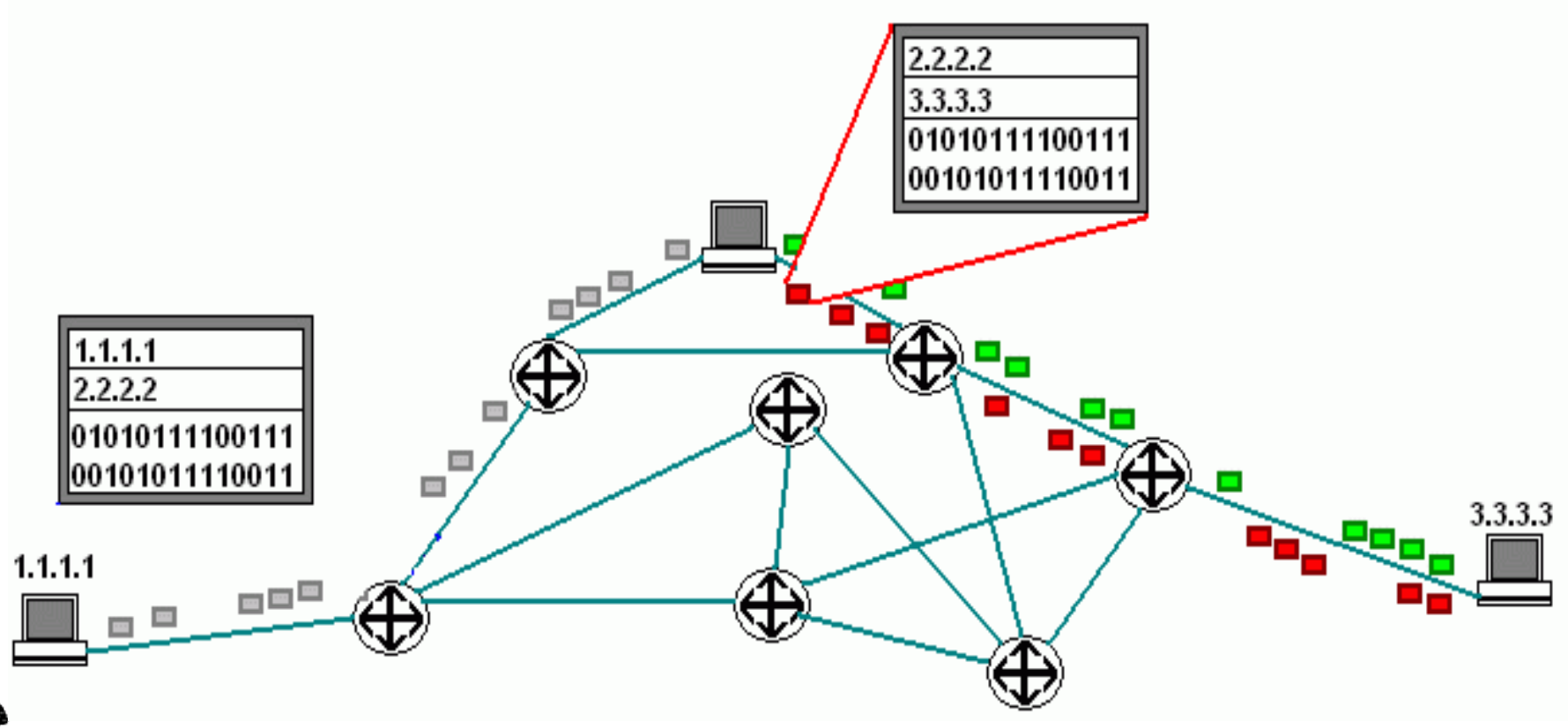
Surfen

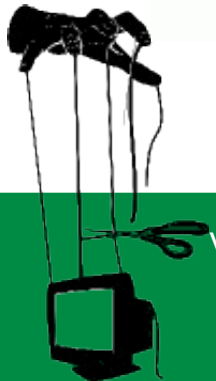




Verschlüsselung2Go

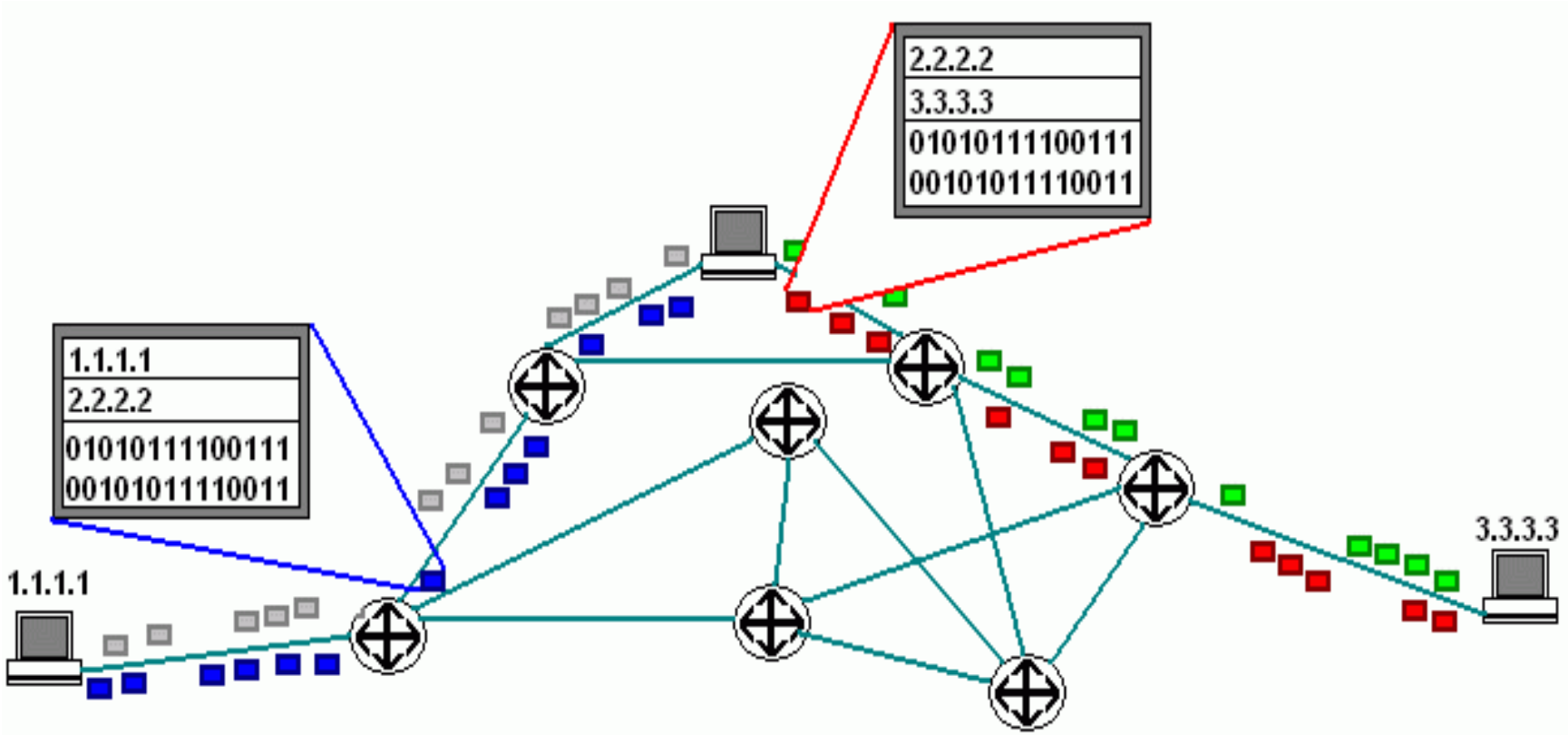
Surfen

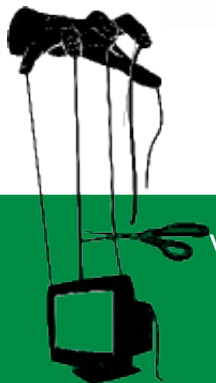




Verschlüsselung2Go

Surfen

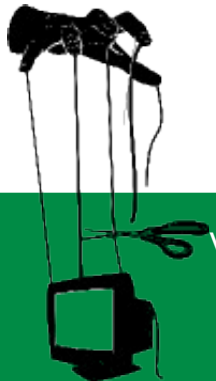




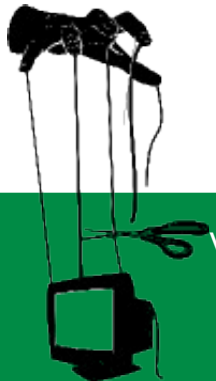
Verschlüsselung2Go

TOR

- The Onion Router
  - Derzeit meistgenutztes Anonymisierungstool
  - Weiterleitung von Daten über mehrere Proxies (Onion Router)
  - Verschlüsselung der Routerkommunikation
  - OpenSource
  - Dezentrale Organisation der Router
  - Infos: torproject.org



Praxis: Surfen mit TOR + Firefox

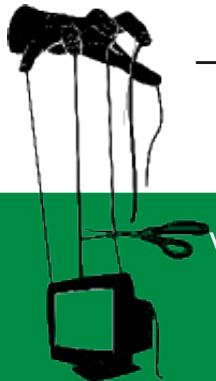


HTTPS

- HyperText Transfer Protocol Secure
  - Sichere Übertragung von Daten im WWW durch Verschlüsselung der Kommunikationsinhalte zwischen zwei Parteien
  - Sichere Authentifizierung von Webseiten

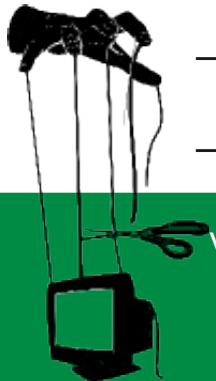
  --> u.a. Schutz vor Abhören der Verbindung

- Funktionsweise
  - Verwendung von asymmetrischer Verschlüsselung zur Authentifizierung
  - Austausch eines gemeinsamen symmetrischen Schlüssels



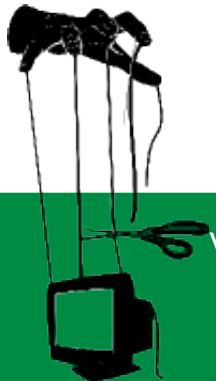
HTTPS

- Authentifizierung
  - Herstellung von Vertrauen über Zertifikate
- Schlüsseltausch
  - Client generiert zufälligen Sitzungsschlüssel und sendet diesen verschlüsselt an die Webseite
- Kommunikation
  - Beide Seiten verschlüsseln alle Inhalte mit dem gemeinsamen Schlüssel
  - Keine zusätzliche Soft-/Hardware notwendig
  - Aber: Nicht immer unterstützt



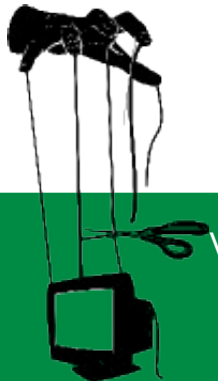
Praxis: Surfen mit HTTPS

AK VORRAT



Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches

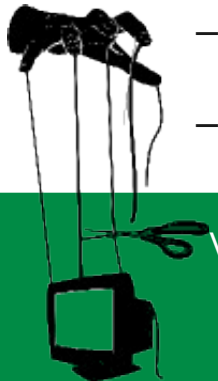


E-Mail

- Motivation
  - Absender/Adressen sind leicht fälschbar
  - Inhalte von Dritten lesbar („Postkarte“)

  --> Verschlüsselung der Inhalte:
    - Authentifizierung
    - Sicherstellung der Integrität von Nachrichten
    - Schutz der Nachrichteninhalte

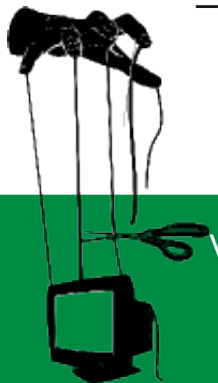
- Pretty Good Privacy (PGP)
  - Asymmetrische Verschlüsselung von E-Mails
  - De facto-Standard, OpenSource-Software



PGP

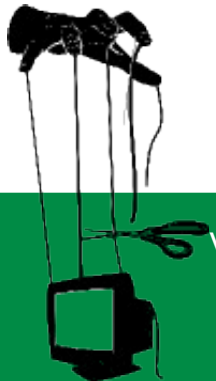
- Prinzip
  - Asymmetrische Verschlüsselung: Jeder Nutzer besitzt ein eigenes Schlüsselpaar (privat/öffentlich)
  - Nachrichten werden mit öffentlichem Schlüssel verschlüsselt und können nur mit privatem Schlüssel + privatem Kennwort geöffnet werden

- Schwachstelle
  - Verteilung der Schlüssel, schwache Passwörter
  - Ausweg: Web of Trust (Private Treffen/ KeySign-Parties)



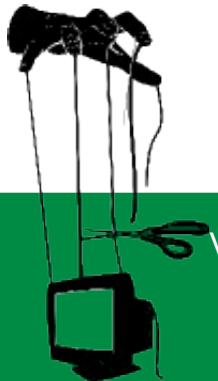
Praxis: E-Mails mit Thunderbird & Enigmail

AK VORRAT

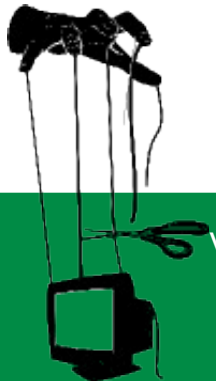


Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches

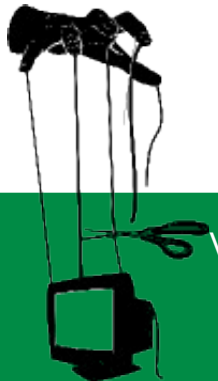


Instant Messaging



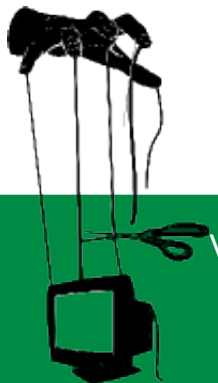
Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches



Sys

- Bisher: Ab … sendet wurden, al … ind
- Jetzt: Abs … igenen Rechner
- Risiken:
  - Viren …
  - Schad …
  - Direk … er, …)
  - → Ver …



Verschlüsselung2Go

Bundeskriminalamt

Ihr Bundeskriminalamt kommt zum :

○	**Festplatten kopieren**	**Ermöglichen Sie bitte den Zutritt zu den Arbeitsräumen und zu Ihrem Computer sowie dessen Hardware**
○	**Trojaner installieren**	**Ermöglichen Sie bitte den Zutritt zu den Arbeitsräumen und zu Ihrem Computer. Entfernen Sie bitte den Passwort-Schutz**
○	**sonstiges**	

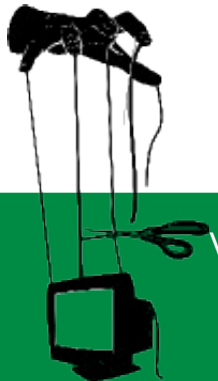
am : ___ . ___ . 20___ ___ : ___ Uhr

! Bitte verlassen Sie Ihre Wohnräume zum angegebenen Zeitpunkt ! Lassen Sie die Tür einen Spalt geöffnet.

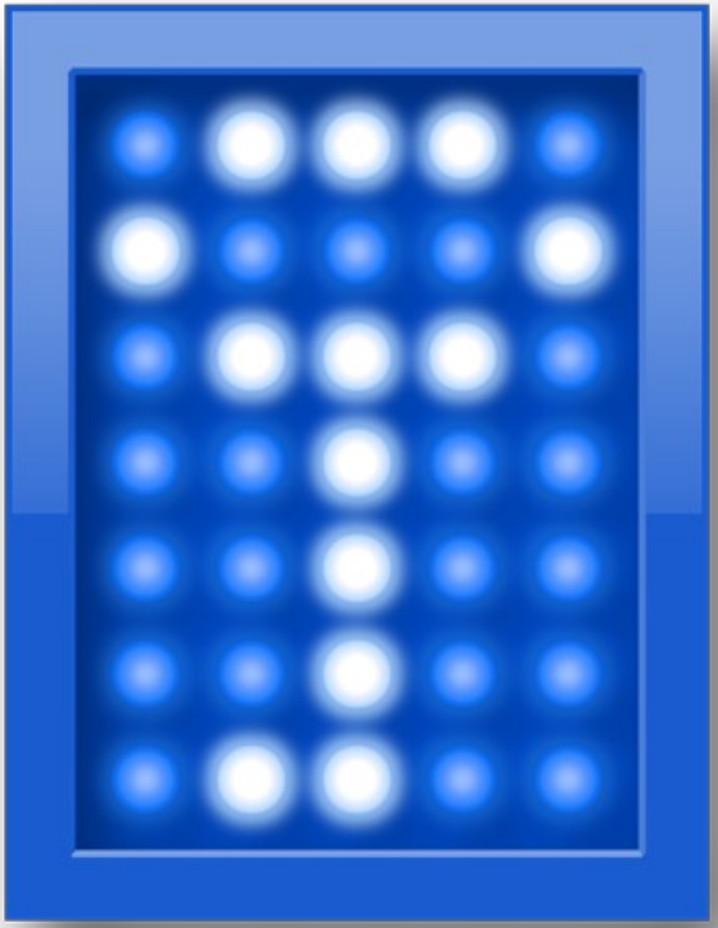
Mit freundlichen Grüßen
Ihr Bundeskriminalamt

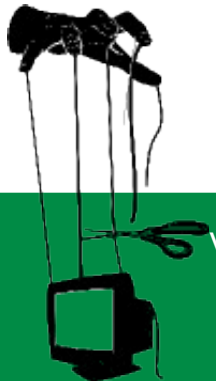
System & Dateien verschlüsseln

- Grundprinzip: Container („Truhe“) erstellen, in dem Daten (symmetrisch) verschlüsselt abgelegt werden
- Container können Dateien, Verzeichnisse oder ganze Festplatten sein
- Zugriff auf die Daten nur bei Kenntnis des Geheimnisses
  - Passwort, Schlüsseldatei, Fingerabdruck...



Praxis: Dateien mit Truecrypt verschlüsseln

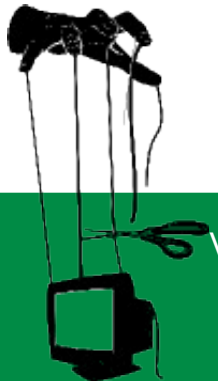




Verschlüsselung2Go

Live Systeme

- Portables System
  - Bietet Funktionen eines (Linux)-Betriebssystems
  - Lauffähig ohne Installation
  - Per DVD,CD oder USB-Stick nutzbar
  - Daten auf externen Datenträgern ablegbar
- Ermöglichen sicheres Arbeiten auf „fremden“ Rechnern
  - In der Uni, bei der Arbeit, im Internetcafe, …



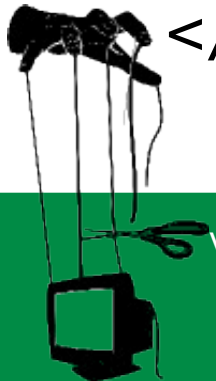
Live Systeme

<Werbung>

Es wird bald eine Live-CD vom AStA geben, die Programme zur sicheren Kommunikation und vieles mehr beinhaltet.

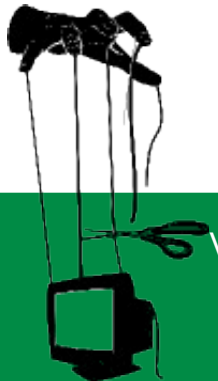
Achtet auf Ankündigungen → asta.ms

</Werbung>



Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches

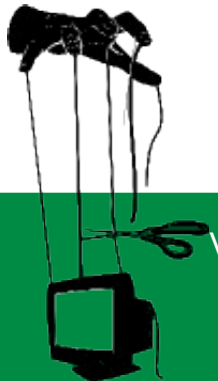


Rechtliches

- Die gute Nachricht:

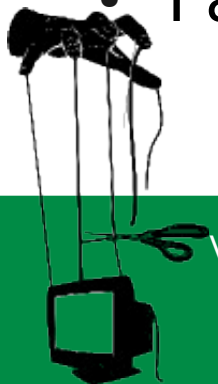
  Es gibt kein Vermummungsverbot im Netz
  Verschlüsselung ist legal

- Aber: Kriminalisierung wird versucht
  - Konspiratives Verhalten
  - Verdunkelungsgefahr
  - Verzögerung von Verfahren



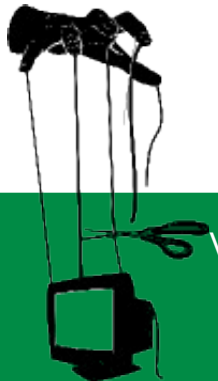
Agenda

- Motivation
- Grundlagen
- Surfen
- E-Mail
- Instant Messaging
- Systeme & Dateien
- Rechtliches
- Fazit



Fazit

- Mit Verschlüsselung könnt ihr viele täglich genutzte Dienste sicher nutzen
- Aber: Sie ersetzte kein umsichtiges Verhalten
  - Schwache Passwörter
  - Unverschlüsselte Kommunikation
  - Nicht aktuelle Systeme
- Je mehr verschlüsselt wird, desto besser
  - Aufwand bei der Auswertung (9 Zeichen ~ 10 Mio $)
  - Schutz von anderen (Anonymity loves company)

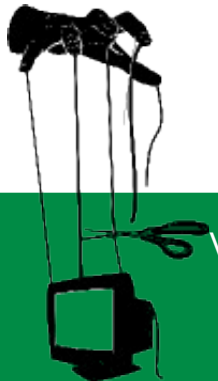


Fragen & Diskussion

Danke für die Aufmerksamkeit!

Links und Infos unter:

http://wiki.vorratsdatenspeicherung.de/Ortsgruppen/Münster



Digitales Zeitalter

AK VORRAT

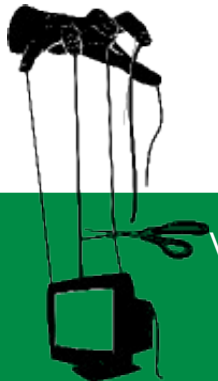
Nächste Veranstaltungen:

11.11. What the fuck is Wiki? 19:30 Uhr F24

21.11. Praxisworkshop Mediawiki, 16 Uhr
Institut für Soziologie, R501

25.11. Wikiwars, 19:30 Uhr F24

02.12. Videoüberwachung im öffentlichen Raum
19:30 Uhr F24



Verschlüsselung2Go