

# Mit Kryptographie die Welt retten

## Cypherpunk in Theorie und Praxis

Sebastian Beschke  
sebastian@sbeschke.de

Chaostreff Tübingen

01. 10. 2011

# Überblick

- 1 Einführung in die Kryptographie
- 2 Privatsphäre unter Beschuss
- 3 Die Anonymisierungssoftware Tor
- 4 Zusammenfassung

# Einführung in die Kryptographie

# Eine einfache Chiffre

FBSKHUSXQNV ZULWH FRGH

# Eine einfache Chiffre

FBSKHUSXQNV ZULWH FRGH  
cypherpunks write code

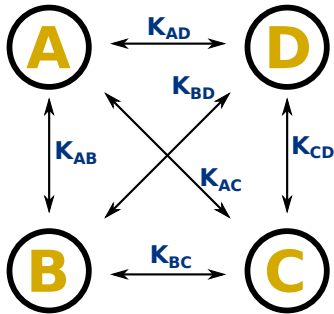
# Eine einfache Chiffre

FBSKHUSXQNV ZULWH FRGH  
cypherpunks write code

$K = 3$   
*Schlüssel*

# Symmetrische und Public-Key-Verschlüsselung

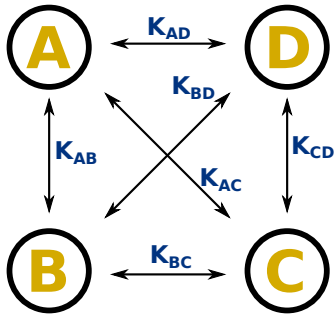
## Symmetrisches Verfahren:



$\Rightarrow \frac{n(n-1)}{2}$  Schlüssel

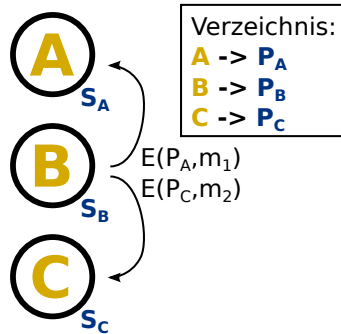
# Symmetrische und Public-Key-Verschlüsselung

## Symmetrisches Verfahren:



$\Rightarrow \frac{n(n-1)}{2}$  Schlüssel

## Public-Key-Verfahren:



$\Rightarrow 2n$  Schlüssel



# Hybride Verfahren

- Public-Key-Kryptographie ist aufwändig zu berechnen
- Daher oft hybrider Ansatz:
  - Austausch eines Schlüssels mittels Public-Key-Kryptographie
  - Anschließend symmetrische Verschlüsselung mit diesem Schlüssel
  - Der Schlüssel ist dann in der Regel kurzlebig

# Das RSA-Verfahren

- RSA ist eines der ältesten Public-Key-Verfahren (1978)
- Auch heute noch ein Standard-Verfahren
- Basiert auf der Modulo-Rechnung und dem Satz von Euler
- Deshalb jetzt ein wenig Mathe. . .

# Modulo-Rechnung

- Modulo-Rechnung ist das Rechnen mit Resten
- $4 \cdot 4 \equiv ? \pmod{5}$

# Modulo-Rechnung

- Modulo-Rechnung ist das Rechnen mit Resten
- $4 \cdot 4 \equiv ? \pmod{5}$
- $4 \cdot 4 = 16$

# Modulo-Rechnung

- Modulo-Rechnung ist das Rechnen mit Resten
- $4 \cdot 4 \equiv ? \pmod{5}$
- $4 \cdot 4 = 16$
- $16 : 5 = 3 \text{ Rest } 1$

# Modulo-Rechnung

- Modulo-Rechnung ist das Rechnen mit Resten
- $4 \cdot 4 \equiv ? \pmod{5}$
- $4 \cdot 4 = 16$
- $16 : 5 = 3 \text{ Rest } 1$
- Also  $4 \cdot 4 \equiv 1 \pmod{5}$

# Der Satz von Euler

## Definition (Die Eulersche $\varphi$ -Funktion)

$\varphi(n)$  = Anzahl der zu  $n$  teilerfremden Zahlen  $\leq n$

# Der Satz von Euler

## Definition (Die Eulersche $\varphi$ -Funktion)

$\varphi(n)$  = Anzahl der zu  $n$  teilerfremden Zahlen  $\leq n$

- Ist  $p$  eine Primzahl, so ist  $\varphi(p) = p - 1$
- Ist  $n = pq$ ,  $p, q$  prim, so ist  $\varphi(n) = (p - 1)(q - 1)$



# Der Satz von Euler

## Definition (Die Eulersche $\varphi$ -Funktion)

$\varphi(n)$  = Anzahl der zu  $n$  teilerfremden Zahlen  $\leq n$

- Ist  $p$  eine Primzahl, so ist  $\varphi(p) = p - 1$
- Ist  $n = pq$ ,  $p, q$  prim, so ist  $\varphi(n) = (p - 1)(q - 1)$

## Theorem (Der Satz von Euler)

Seien  $a$  und  $n$  teilerfremd. Dann gilt  $a^{\varphi(n)} \equiv 1 \pmod{n}$

# Verschlüsseln mit dem Satz von Euler

## Theorem (Der Satz von Euler)

*Seien  $a$  und  $n$  teilerfremd. Dann gilt  $a^{\varphi(n)} \equiv 1 \pmod{n}$*

- Sei  $n$  das Produkt zweier Primzahlen  $p, q$
- Angenommen, wir haben  $e, d$  mit  $ed = k \cdot \varphi(n) + 1$

# Verschlüsseln mit dem Satz von Euler

## Theorem (Der Satz von Euler)

*Seien  $a$  und  $n$  teilerfremd. Dann gilt  $a^{\varphi(n)} \equiv 1 \pmod{n}$*

- Sei  $n$  das Produkt zweier Primzahlen  $p, q$
- Angenommen, wir haben  $e, d$  mit  $ed = k \cdot \varphi(n) + 1$
- Sei  $m$  eine Nachricht.
- $c \equiv m^e \pmod{n}$  ist dann die verschlüsselte Nachricht.

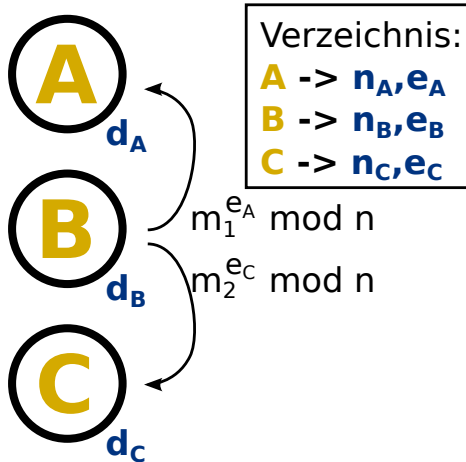
# Verschlüsseln mit dem Satz von Euler

## Theorem (Der Satz von Euler)

*Seien  $a$  und  $n$  teilerfremd. Dann gilt  $a^{\varphi(n)} \equiv 1 \pmod{n}$*

- Sei  $n$  das Produkt zweier Primzahlen  $p, q$
- Angenommen, wir haben  $e, d$  mit  $ed = k \cdot \varphi(n) + 1$
- Sei  $m$  eine Nachricht.
- $c \equiv m^e \pmod{n}$  ist dann die verschlüsselte Nachricht.
- Kennt man  $d$ , kann man sie entschlüsseln:  
$$c^d \equiv m^{ed} \equiv m^{k \cdot \varphi(n) + 1} \equiv m \cdot m^{k \cdot \varphi(n)} \equiv m \pmod{n}$$

# RSA-Verschlüsselung



# Sicherheit von RSA

- Ein Angreifer könnte  $\log_e m^e$  berechnen.
  - Das ist bei Modulorechnung sehr schwierig.

# Sicherheit von RSA

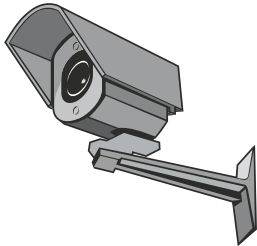
- Ein Angreifer könnte  $\log_e m^e$  berechnen.
    - Das ist bei Modulorechnung sehr schwierig.
  - Oder er könnte versuchen,  $d$  zu bestimmen.
    - Der Knackpunkt: Zur Bestimmung von  $d$  braucht man  $\varphi(n)$
    - Leicht zu bestimmen, wenn man  $p, q$  kennt:  
$$\varphi(n) = (p - 1)(q - 1).$$
    - Sonst aber sehr schwer zu bestimmen.
- ⇒  $d$  zu bestimmen, ist so schwer, wie die Primfaktorzerlegung von  $n$ .

# Privatsphäre unter Beschuss



# Die Rolle von Kryptographie

- Kryptographie: Metier von Geheimdiensten und Geheimniskrämern?
- Nicht im Informationszeitalter!



# Was heißt eigentlich „Privatsphäre“?

- Privatsphäre ist nicht nur Verschlüsselung:
  - Anonymität
  - Abstreitbarkeit
  - Authentifizierung

# Was heißt eigentlich „Privatsphäre“?

- Privatsphäre ist nicht nur Verschlüsselung:
  - Anonymität
  - Abstreitbarkeit
  - Authentifizierung
- Privatsphäre ist nicht Geheimnistuerei:
  - *Geheime* Informationen soll *niemand* erfahren
  - *Private* Informationen soll *nicht jeder* erfahren

*“Privacy is the power to selectively reveal oneself to the world.”*

Eric Hughes, A Cypherpunk's Manifesto

# Der Kampf um die Privatsphäre

- Privatsphäre ist ein wiederkehrendes Thema der politischen Debatte in Deutschland:
  - Klarnamenspflicht im Internet
  - Vorratsdatenspeicherung
  - Bundestrojaner
  - Zensur(sula)gesetz
  - Übermittlung von Fluggastdaten
  - usw. usf.

# Der Kampf um die Privatsphäre

- Privatsphäre ist ein wiederkehrendes Thema der politischen Debatte in Deutschland:
  - Klarnamenspflicht im Internet
  - Vorratsdatenspeicherung
  - Bundestrojaner
  - Zensur(sula)gesetz
  - Übermittlung von Fluggastdaten
  - usw. usf.
- oder auch kürzlich:

*„Eine anonyme Teilhabe am politischen Meinungs- und Willensbildungsprozess ist abzulehnen.“*

Positionspapier der CDU/CSU-Fraktion im Bundestag  
zum Thema „Freiheit des Internet“

# Diskrepanzen

- In der „realen Welt“ ist Privatsphäre oft der Standard.
  - Bargeld, Briefgeheimnis. . .
- In der digitalen Welt sieht das meistens anders aus:
  - Standardmäßig unverschlüsselte Übertragung von Webseiten, E-Mail, Chatnachrichten. . .
  - Internet-Verbindungen sind über den Provider zurückverfolgbar

# Das *Cypherpunk's Manifesto*

- Eine offene Gesellschaft braucht Privatsphäre
- Regierungen und Konzerne werden Privatsphäre nicht freiwillig schaffen
- Kryptographie ist das Mittel zur Wahrung der Privatsphäre
- Cypherpunks machen entsprechende Software

*"Cypherpunks write code."*

# Interessante Projekte

- Bitcoin (<http://bitcoin.org>)
- Freenet (<http://freenetproject.org>)
- Off-the-Record messaging  
(<http://www.cypherpunks.ca/otr/>)
- Tor (<https://www.torproject.org>)

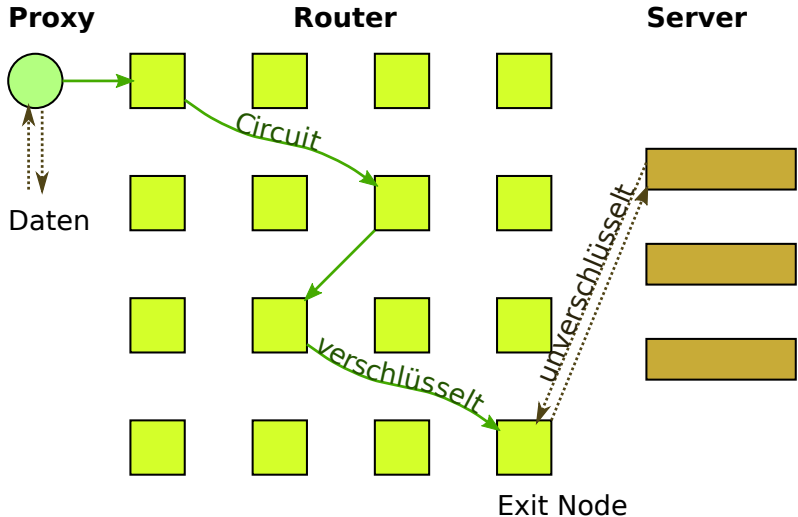


# Die Anonymisierungssoftware Tor

# Überblick über Tor

- Das Tor-Projekt. . .
  - Entstanden als Weiterentwicklung des “Onion Routing” -Projekts des US Naval Research Laboratory
  - Später finanziert durch die Electronic Frontier Foundation
  - Seit 2006 ist das “Tor Project” eine Nonprofit-Organisation in den USA
- Ziele von Tor
  - Verschleiern: Wer kommuniziert mit wem?
  - Umgehen von Zensurschranken
  - Anonymes Bereitstellen von Informationen

# Netzwerkstruktur von Tor



# Aufbau eines Circuit

**Proxy**



Kennt  $K_A$

Schlüsselaustausch von  $K_A$

**Router**



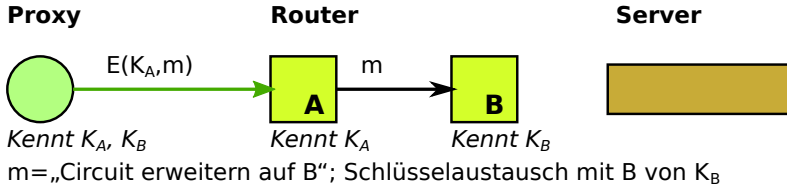
Kennt  $K_A$



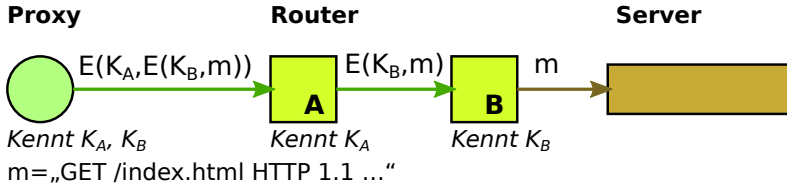
**Server**



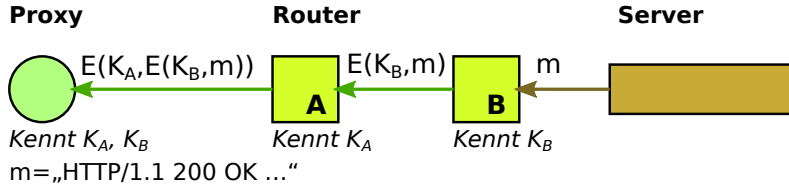
# Aufbau eines Circuit



# Weiterleiten von Daten



# Weiterleiten von Daten



# Anonymisierung

- Niemand erfährt, mit wem der Sender kommuniziert
  - Der Server denkt, die Anfrage käme vom Exit Node
  - Jeder Knoten im Circuit kennt nur seine Nachbarn
  - Nur der Exit Node kann das Ziel des Datenpakets sehen
- Aber:
  - Der Exit Node sieht den Datenverkehr im Klartext
  - Daher ist Ende-zu-Ende-Verschlüsselung zum Server sinnvoll
  - Trotzdem kann das Datenpaket identifizierende Daten beinhalten



# Zusammenfassung

# Zusammenfassung

- Der Schutz der Privatsphäre ist wichtig
- Geschickter Einsatz von Kryptographie kann hierbei helfen
- Es ist schwer, ein wasserdichtes Kryptosystem zu bauen
- Selbst ein wasserdichtes System kann durch Fehler auf anderen Ebenen außer Kraft gesetzt werden
- Aber: Die Grundprinzipien sind einfach zu verstehen – Jede/r kann mitdenken

## Quellen und Anhang

sebastian@sbeschke.de (OpenPGP: 0x78FE61BF)

- Die Vortragsmaterialien sind CC-BY-SA: Namensnennung, Weitergabe unter gleichen Bedingungen. Zu finden unter: <https://github.com/sbeschke/tor-presentation>
- Buchtipp: Steven Levy, Crypto - How the code rebels beat the government - saving privacy in the digital age
- Mehr Krypto-Hintergründe: (Englische) Wikipedia über die angesprochenen Themen
- Mehr über Anonymität:  
<http://freehaven.net/anonbib/date.html>
- Das Design von Tor: <https://svn.torproject.org/svn/projects/design-paper/tor-design.html>
- Mehr zum Chaostreff Tübingen:  
<http://chaostreff.klappezu.org>