

# Kryptographie im Alltag



Thalunil ([thalunil@kallisti.de](mailto:thalunil@kallisti.de))

derPeter ([peterhasse@gmx.de](mailto:peterhasse@gmx.de))

## Inhalt

- Glossar & Begrifflichkeiten
- Geschichtliches
- Kryptografische Grundlagen
  - Symmetrische Chiffres
  - Asymmetrische Chiffres
- Werkzeuge
- SSL Hierarchieebene
  - Blick aus 10.000km Höhe
  - Davorstehend: Interna von SSL
- GnuPG
- DECT
- Instant Messaging

### Kryptologie

Wissenschaft der Verschlüsselung von Informationen und der technischen Verfahren der Informationssicherheit

in der Neuzeit: digitale Signaturen, Hashfunktionen, elektronisches Geld

—▶ Oberklasse von: Kryptografie und Kryptanalyse

### Kryptographie

(griechisch: *kryptós*, „verborgen“, und *gráphein*, „schreiben“)

Wissenschaft der Verschlüsselung von Informationen ( „Geheimschriften“),

Schutz von Daten durch deren Transformation, in der Regel unter Einbeziehung von geheimen Schlüsseln.

### Kryptographie

(griechisch: *kryptós*, „verborgen“, und *gráphein*, „schreiben“)

Wissenschaft der Verschlüsselung von Informationen ( „Geheimschriften“),

Schutz von Daten durch deren Transformation, in der Regel unter Einbeziehung von geheimen Schlüsseln.

Security of the weakest link

## **Kryptanalyse**

Informationsgewinnung eines kryptografischen Produkts ohne  
Kenntnis des geheimen Schlüssels

Moderne Disziplin, heute: Informationsgewinnung || Nachweis  
der kryptografischen Sicherheit durch Analyse

## Glossar & Begrifflichkeiten der Thematik

### **Klartext:**

originärer, zu schützende Nachricht

### **Geheim Schlüssel:**

Geheim, Kenntnisnahme schwer möglich (secretkey)

### **Chiffre:**

Resultat der Operation Klartext X Geheimchlüssel

## Glossar & Begrifflichkeiten der Thematik

### **Klartext:**

originärer, zu schützende Nachricht

### **Geheim Schlüssel:**

Geheim, Kenntnisnahme schwer möglich (secretkey)

### **Chiffre:**

Resultat der Operation Klartext X Geheimchlüssel

### **Alice/Bob/Eve: (die Mitspieler)**

Alice = Komm.- Partner A

Bob = Komm.- Partner B

Eve = Partei die Kenntnis von dem Chiffre erhält,  
Mitleser

## Glossar & Begrifflichkeiten der Thematik

### Prinzip von Kerckhoff

1883 „La Cryptographie militaire“ Abhandlung zur sicheren  
Kommunikation

[http://www.petitcolas.net/fabien/kerckhoffs/crypto\\_militaire\\_1.pdf](http://www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf)

## Glossar & Begrifflichkeiten der Thematik

### Prinzip von Kerckhoff

1883 „La Cryptographie militaire“ Abhandlung zur sicheren Kommunikation

[http://www.petitcolas.net/fabien/kerckhoffs/crypto\\_militaire\\_1.pdf](http://www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf)

### Eigenschaften:

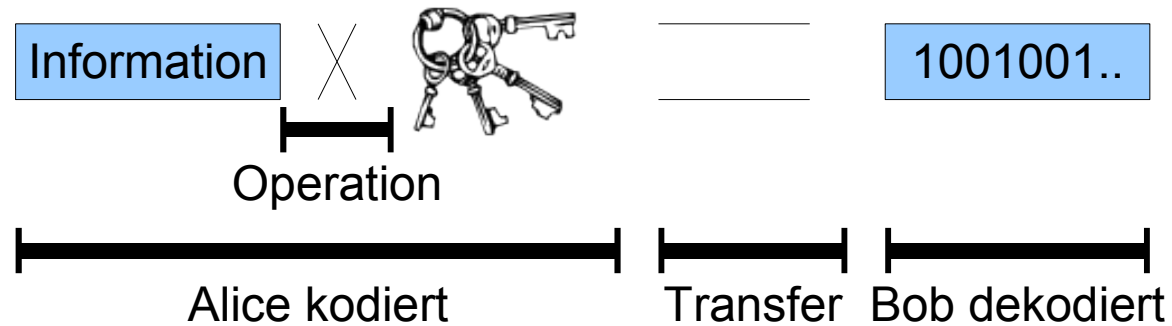
- Mathematische Herleitung des Klartextes aus dem Chifftrat darf nicht effizient möglich sein -> Langfristige Nutzung von Algorithmen und schwer änderbar (Praktischer Einsatz)
- Kein Schaden an A & B wenn Kryptosystem bekannt und öffentlich („Security by obscurity“)
- Gute Untersuchung des Kryptosystems („gut abgehangen“)

## Glossar & Begrifflichkeiten der Thematik

# Krypto Überblick

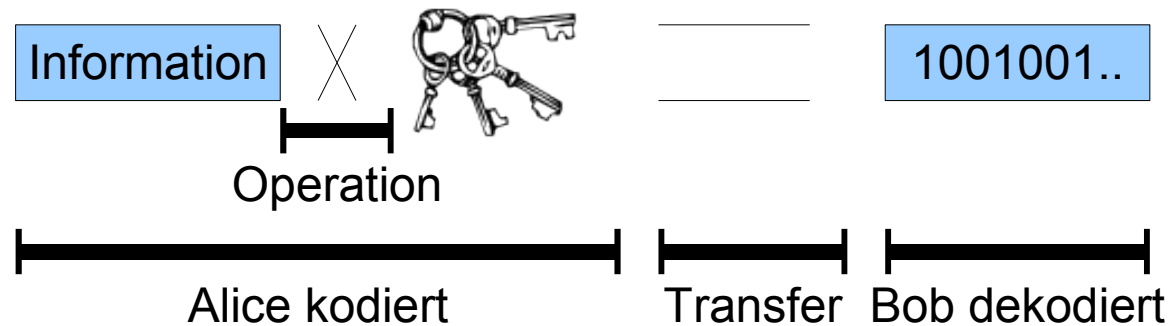
<b>Symmetrische Verschlüsselungen</b>	<b>Block</b>	<b>Strom</b>
DES (Data Encryption Standard)	X	
AES (Advanced Encryption Standard)	X	
IDEA (International Data Encryption Algorithm)	X	
Camellia	X	
Twofish	X	
Blowfish	X	
RC6	X	
Quick Stream Cipher		X
RC4		X
<b>Asymmetrische Verschlüsselungen</b>		
RSA		
Elgamal-Kryptosystem		
Schlüsselaustausch		
Diffie-Hellman-Algorithmus		
<b>Hash Funktionen</b>		

## Symmetrische Verschlüsselung



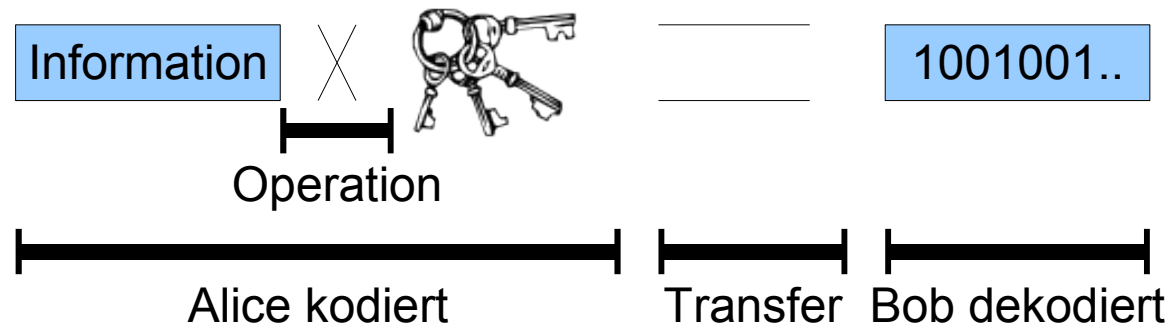
\* Vereinbarung eines geheimen Schlüssel zwischen den Parteien A + B

## Symmetrische Verschlüsselung



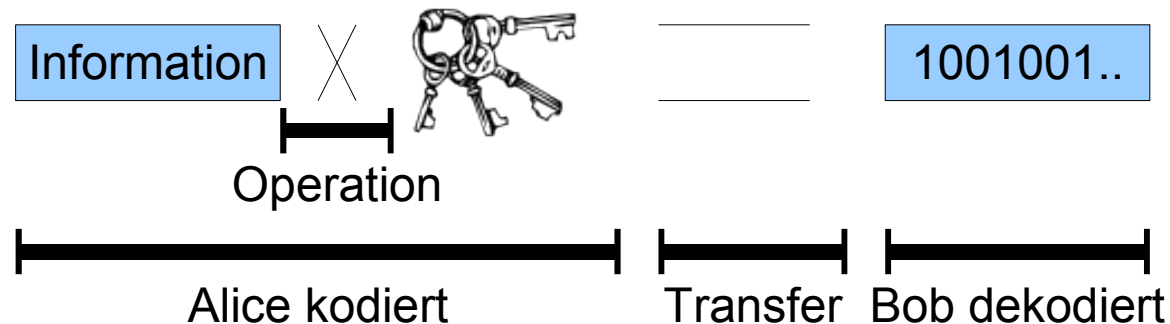
- \* Vereinbarung eines geheimen Schlüssel zwischen den Parteien A + B
- \* Nachricht kodiert mit geheimen Schlüssel (secretkey),  
Resultat: Transferbar über einen ungesicherten Kanal

## Symmetrische Verschlüsselung



- \* Vereinbarung eines geheimen Schlüssel zwischen den Parteien A + B
- \* Nachricht kodiert mit geheimen Schlüssel (secretkey),  
Resultat: Transferbar über einen ungesicherten Kanal
- \* Empfängerseite Bob dekodiert Chiffre mittels secretkey + Algorithmus

## Symmetrische Verschlüsselung



- \* Vereinbarung eines geheimen Schlüssel zwischen den Parteien A + B
- \* Nachricht kodiert mit geheimen Schlüssel (secretkey),  
Resultat: Transferbar über einen ungesicherten Kanal
- \* Empfängerseite Bob dekodiert Chiffre mittels secretkey + Algorithmus

Kodierung und Dekodierung mit gleichen Schlüssel (und nur mit ihm)  
Nachricht Sicher, solange secretkey nur A und B bekannt

**Auch dann: Kryptooperation öffentlich (Eve kennt den Algorithmus)**

## Symmetrische Verschlüsselung

Einfache Substitution (Ersetzung)

    feste Zuordnung von Klartext zu Chiffretext nach Vorgabe

    statistisch einfach angreifbar (Häufigkeitsanalyse, Paarbildung)

## Symmetrische Verschlüsselung

Einfache Substitution (Ersetzung)

feste Zuordnung von Klartext zu Chiffretext nach Vorgabe  
statistisch einfach angreifbar (Häufigkeitsanalyse, Paarbildung)

Homophone Substitution (mehrfache Klar-Chiffretext Abbildung)

zeichenweise Zuordnung von Klartext auf Chiffretext ist variabel

„c -> z; c -> k; c -> °“

Güte der Homophonität ist Abhängig von der Qualität des Chiffrierers

„Algorithmus und Chiffrierer sind bekannt und nicht geheimzuhalten“

Bei Vorhandensein von Klartext ist diese einfache, manuelle homophone  
Verschlüsselung NICHT qualitativ hochwertig.

## Symmetrische Verschlüsselung

Einfache Substitution (Ersetzung)

feste Zuordnung von Klartext zu Chiffretext nach Vorgabe  
statistisch einfach angreifbar (Häufigkeitsanalyse, Paarbildung)

Homophone Substitution (mehrfache Klar-Chiffretext Abbildung)

zeichenweise Zuordnung von Klartext auf Chiffretext ist variabel

„c -> z; c -> k; c -> °“

Güte der Homophonität ist Abhängig von der Qualität des Chiffrierers

„Algorithmus und Chiffrierer sind bekannt und nicht geheimzuhalten“

Bei Vorhandensein von Klartext ist diese einfache, manuelle homophone  
Verschlüsselung NICHT qualitativ hochwertig.

Transpositionschiffren

Positionsvertauschung nach Regelsatz

„SIMPLEMINDSWIN“ (Matrix 4)

SIMP

LEMI

NDSW

WIN = SLNWIEDIMMSNPIW

## Symmetrische Verschlüsselung

Einfache Substitution (Ersetzung)

feste Zuordnung von Klartext zu Chiffretext nach Vorgabe  
 statistisch einfach angreifbar (Häufigkeitsanalyse, Paarbildung)

Homophone Substitution (mehrfache Klar-Chiffretext Abbildung)

zeichenweise Zuordnung von Klartext auf Chiffretext ist variabel

„c -> z; c -> k; c -> °“

Güte der Homophonität ist Abhängig von der Qualität des Chiffrierers

„Algorithmus und Chiffrierer sind bekannt und nicht geheimzuhalten“

Bei Vorhandensein von Klartext ist diese einfache, manuelle homophone  
 Verschlüsselung NICHT qualitativ hochwertig.

## Transpositionschiffren

Positionsvertauschung nach Regelsatz

„SIMPLEMINDSWIN“ (Matrix 4)

SIMP

LEMI

NDSW

WIN = SLNWIEDIMMSNPIW

Zu simpel, ebenfalls statistisch angreifbar und computertechnisch einfach  
brechbar (Differentielle Kryptanalyse, SCHNEIER APPL-CRYPTO Seite 336]

## Symmetrische Verschlüsselung

Mehrfache Anwendung?

Nicht sinnvoll, da die Kombination von Substitutionen im Effekt nur eine Substitution ergibt: Eine Gruppe

## Symmetrische Verschlüsselung

Mehrfache Anwendung?

Nicht sinnvoll, da die Kombination von Substitutionen im Effekt nur eine Substitution ergibt: Eine Gruppe

Mischung von Transposition und Substitution

effektiv nicht besser als einzelne Anwendung: Häufigkeitsanalyse weiterhin möglich gegen die Substitution. Transposition auch aufdeckbar durch kleine Teile des Klartextes -> Gebrochen!

## Symmetrische Verschlüsselung

One-Time Pad / Einmalschlüssel / Wegwerf-Schlüssel

bisher: keine unknackbare Methode, hier die erste beweisbare Methode

Auswahl eines Schlüssel mit Länge(key)  $\geq$  Länge(klartext)

Polyalphabetische Chiffrierung

EIN AUSSERORDENTLICH LANGER UND VÖLLIG ZUFÄLLIGER SCHLÜSSEL  
DER KLARTEXT IST ETWAS KÜRZER

EIN AUSSERORDENTLICH LANGER U  
+ DER KLARTEXT IST ETWAS KÜRZER  
= HMEKFSJXVLKLWGXE ECZVURXDVL

## Symmetrische Verschlüsselung

One-Time Pad / Einmalschlüssel / Wegwerf-Schlüssel

bisher: keine unknackbare Methode, hier die erste beweisbare Methode

Auswahl eines Schlüssel mit Länge(key)  $\geq$  Länge(klartext)

Polyalphabetische Chiffrierung

EIN AUSSERORDENTLICH LANGER UND VÖLLIG ZUFÄLLIGER SCHLÜSSEL  
DER KLARTEXT IST ETWAS KÜRZER

EIN AUSSERORDENTLICH LANGER U  
+ DER KLARTEXT IST ETWAS KÜRZER  
= HMEKFSJXVLKLWGXECCZVURXDVL

Einwegschlüssel darf nur einmal verwendet werden

→ Zufälliger Schlüssel erzeugt keine Gesetzmäßigkeiten, Problem: Entropie in Rechner, Rechner haben immer einen Ablauf, eine Gesetzmäßigkeit

## **Asymmetrische Verschlüsselung**

Anders: Public-Key Verfahren

Erste Einführung 1976 durch Diffie und Hellmann

Qualitativ neuwertig: Lösung des Problems der Schlüsselverteilung

## Asymmetrische Verschlüsselung

Anders: Public-Key Verfahren

Erste Einführung 1976 durch Diffie und Hellmann

Qualitativ neuwertig: Lösung des Problems der Schlüsselverteilung

Asymmetrisch bedeutet hier: 2 Schlüsselteile (privater & öffentlicher Schlüssel)

Privater Schlüssel zum **VER**schlüsseln, Öffentlicher Schlüssel für die **ENT**schlüsselung

Chiffrier & Dechiffrieralgorithmus kann (muss aber nicht) identisch sein. Gleiche Eigenschaft wie bei den symmetrischen Methoden

## Asymmetrische Verschlüsselung

Anders: Public-Key Verfahren

Erste Einführung 1976 durch Diffie und Hellmann

Qualitativ neuwertig: Lösung des Problems der Schlüsselverteilung

Asymmetrisch bedeutet hier: 2 Schlüsselteile (privater & öffentlicher Schlüssel)

Privater Schlüssel zum **VER**schlüsseln, Öffentlicher Schlüssel für die **ENT**schlüsselung

Chiffrier & Dechiffrieralgorithmus kann (muss aber nicht) identisch sein. Gleiche Eigenschaft wie bei den symmetrischen Methoden

Öffentlicher Schlüssel ist ableitbar aus dem privaten.

**NICHT** aber die Ableitung des privaten aus dem öffentlichen

## Asymmetrische Verschlüsselung

Anders: Public-Key Verfahren

Erste Einführung 1976 durch Diffie und Hellmann

Qualitativ neuwertig: Lösung des Problems der Schlüsselverteilung

Asymmetrisch bedeutet hier: 2 Schlüsselteile (privater & öffentlicher Schlüssel)

Privater Schlüssel zum **VER**schlüsseln, Öffentlicher Schlüssel für die **ENT**schlüsselung

Chiffrier & Dechiffrieralgorithmus kann (muss aber nicht) identisch sein. Gleiche Eigenschaft wie bei den symmetrischen Methoden

Öffentlicher Schlüssel ist ableitbar aus dem privaten.

**NICHT** aber die Ableitung des privaten aus dem öffentlichen

Nachteilig (trotz der tollen Eigenschaften): Wenige praxistaugliche Algorithmen bekannt.  
Langsam und auch noch angreifbar mittels ausgewähltem Geheimtext.

## Asymmetrische Verschlüsselung

Anders: Public-Key Verfahren

Erste Einführung 1976 durch Diffie und Hellmann

Qualitativ neuwertig: Lösung des Problems der Schlüsselverteilung

Asymmetrisch bedeutet hier: 2 Schlüsselteile (privater & öffentlicher Schlüssel)

Privater Schlüssel zum **VER**schlüsseln, Öffentlicher Schlüssel für die **ENT**schlüsselung

Chiffrier & Dechiffrieralgorithmus kann (muss aber nicht) identisch sein. Gleiche Eigenschaft wie bei den symmetrischen Methoden

Öffentlicher Schlüssel ist ableitbar aus dem privaten.

NICHT aber die Ableitung des privaten aus dem öffentlichen

Nachteilig (trotz der tollen Eigenschaften): Wenige praxistaugliche Algorithmen bekannt. Langsam und auch noch angreifbar mittels ausgewähltem Geheimtext.

- ▶ Nutzung: Austausch von Sitzungsschlüssel zum Einsatz bei symmetrischen Verfahren

# SSL / TLS

- Secure Sockets Layer / Transport Layer Security
- Verschlüsselungsprotokoll zur Datenübertragung im Internet
- Aus OSI Sicht zwischen Schicht 4 und HTTP
- TLS 1.0 = SSL 3.1
- DES, SH1, MD5, Trippel DES, AES, MD5
- **HTTPS**, **SMTPS**,...
- Transparent -> kann für die meisten Protokolle genutzt werden
- Mehrere „Schichten“
  - Schicht 1
    - SSL Handshake Protokoll
    - SSL Change Cipher Spec. Protokoll
    - SSL Alert Protokoll
    - SSL Applikation Data Protocol
  - Schicht 2
    - SSL Record Protocol

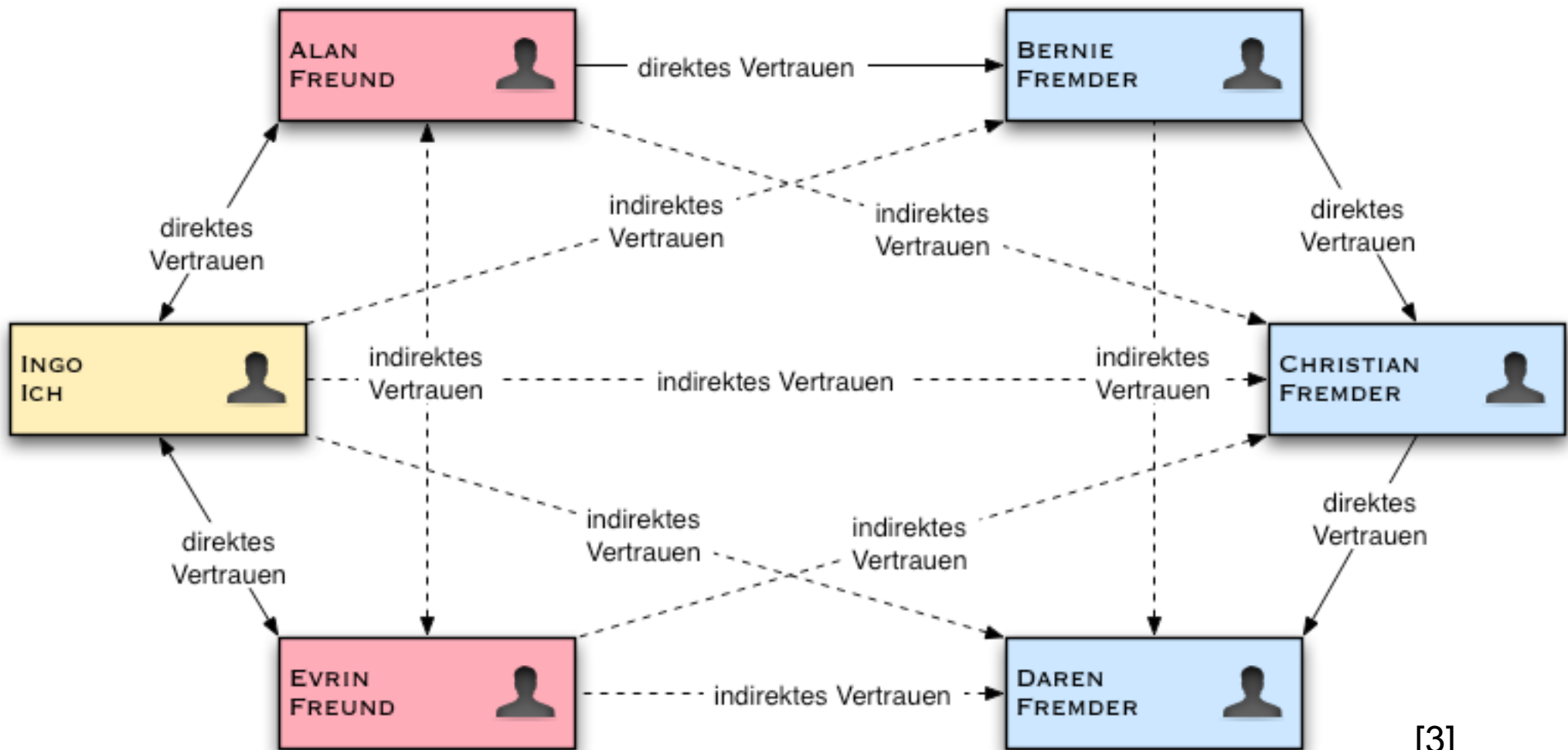
# SSL / TLS

- SSL Record Protokoll
  - Unterste Schicht
  - 2 Funktionen
    - Integritätssicherung
    - Ende-zu-Ende Verschlüsselung (Symmetrisch)
- SSL Handshake Protokoll
  - Authentifizieren der Teilnehmer
  - Aushandeln von Verschlüsselung und Schlüssel
- SSL Alert Protokoll
  - Austausch von „Alerts“ zwischen Server und Client

# Pretty Good Privacy (PGP)

- 1991 erste Version von Phil Zimmerman mit dem Ziel „Starke Verschlüsselung für die Bürger“
- Hybrid Verschlüsselung
  - Lineare Verschlüsselung für die Nachricht
  - Asymmetrische Verschlüsselung für die Schlüssel
- Verschiedene Verschlüsselungs Algorithmen nutzbar
- Keine zentrale CA -> Web of Trust
- Rechte an PGP wechselten häufig den Besitzer -> OpenPGP

# Web of trust



[3]

## Web of trust

Transitive Vertrauensbeziehungen:

Alice signiert den Schlüssel von Bob  
Bob signiert den Schlüssel von Carl  
somit vertraut Alice dem Schlüssel von Carl.

Anders ausgedrückt: Ich vertraue jedem, dem jemand vertraut, dem ich vertraue.  
Und umgekehrt: Jeder, der jemandem vertraut, der mir vertraut, vertraut auch mir.

[2]

Durch das Web of trust wird die Funktion einer PKI, die Zugehörigkeit eines Schlüssels zu einer realen Person herzustellen, übernommen.

## Web of trust

- Owner Trust
  - unkown (Benutzer über die man keine weiteren Informationen hat)
  - not trusted (Benutzer denen man nicht vertraut)
  - marginal (Benutzer denen nicht voll vertraut wird)
  - complete (Benutzer denen voll vertraut wird)
  - ultimate (Benutzer deren privater Schlüssel sich im Privaten Schlüsselbund befindet)
- Signatory Trust
  - Vertrauen wird vom „Signierer“ abgeleitet
  - Vertrauen gegenüber einer Signatur und nicht Person
- Nachteile gegenüber PKI
  - „Key revocation“ nicht sofort allgemein verfügbar
  - Nicht rechtlich bindend
  - Analog zu „Sozialnetworks“ sind Beziehungen öffentlich einsehbar

## PGP

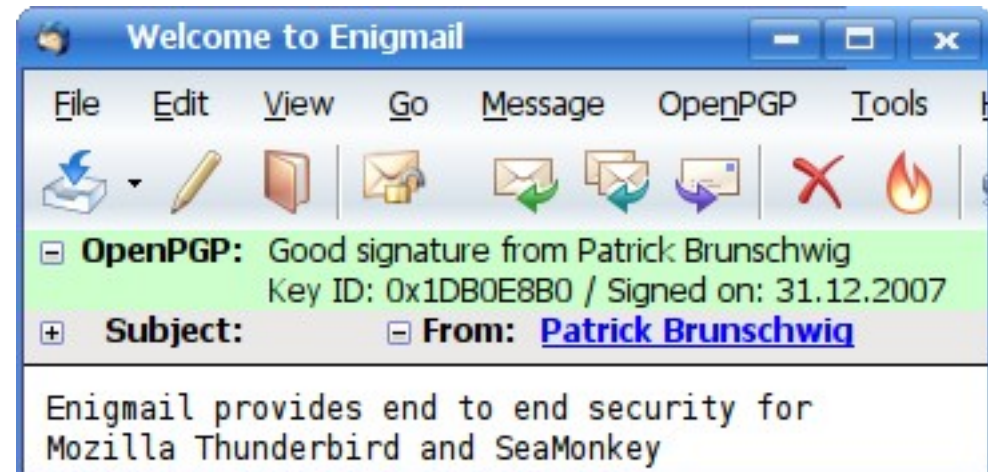


GnuPG oder GPG (GNU Privacy Guard)

- Freie Implementierung von OpenPGP nach RFC 4880
- Dient als „backend“ für viele Kryptools
- Default nur Patentfreie Algorithmen, GPL Software
- Für „alle“ Betriebssysteme verfügbar.

# Enigmail

- Mozilla Plugin  
(Thunderbird, seeMonkey...)
- Frontend für alle GnuPG Funktionen
- Frei und weitgehend für OS verfügbar



## Kryptographie „Hands on“

Enigmail – GPG

GSM – A8 (Schlüsselerzeugung) und A5 (Verschlüsselung)

DECT – DECT Standard Cipher

OTR – AES, DH, SHA-1

Email – SSL

HTTPS – SSL

OpenVPN – OpenSSL

WEP, WPA, WPA2

RFID Auto Schlüssel - ?

DRM

LUKS, BitLocker, FileFault, TrueCrypt ....

EC Karte – DES, TDES ..

.

Quellen:

<http://de.wikipedia.org/wiki/Kryptographie>

Kerckhoffs Prinzip [http://de.wikipedia.org/wiki/Auguste\\_Kerckhoffs](http://de.wikipedia.org/wiki/Auguste_Kerckhoffs)

Schneier Bruce: Angewandte Kryptographie, 1996, 800 Seiten, REFERENZ

Wobst Reinhard: Abenteuer Kryptologie, 1997, 360 Seiten, Bekömmlich

Ertl Wolfgang: Angewandte Kryptographie, 2001, 170 Seiten, Fachbuch

Schneier Bruce, Ferguson Niels: Practical Cryptography, 380 Seiten, Moderne Praxis

Viega John, Messier Matt, Chandra Pravir: Network Security with SSL, 350 Seiten, SSL

[http://de.wikipedia.org/wiki/Web\\_of\\_Trust](http://de.wikipedia.org/wiki/Web_of_Trust)