Angewandte Kryptographie

Vortrag im Rahmen der Seminarreihe des CCC–Ulm

Dipl.–Ing. Marten Karl

Überblick

- Geschichtliches
- Kryptographische Verfahren
  - Symmetrische Verschlüsselung
  - Asymmetrische Verschlüsselung
- Begriffsklärungen
- Angriffsmöglichkeiten
- Anwendungen

Geschichtliches zu Geheimschriften

- Früheste Erwähnung bei Herodot, sie bezieht sich auf die Zeit um 500 vor Christus
- Geheimschriften gliedern sich in Steganographie und Kryptographie
- Es war immer ein Kampf zwischen den Verschlüsslern (Kryptographen) und den Entschlüsslern (Kryptologen)
- Einfachste Verschlüsselung

Cäsar-Verschlüsselung

- Jeder Buchstabe wird durch den Buchstaben ersetzt, der ihm um einen bestimmten Abstand nachfolgt
- Beispiel: (3) A⇒D, B⇒E, C⇒F, ..., Y⇒B, Z⇒C
  BEISPIEL⇒EHLVSLHO
- Es handelt sich um eine symmetrische Verschlüsselung

Vertrauen

- Algorithmen und Implementierungen sind für Einzelpersonen kaum zu prüfen.
- Wesentlich ist das Vertrauen in die eingesetzten Verfahren.
- „Nicht jede Open–Source–SW ist sicher, aber nur Open–Source–SW kann sicher sein!“
- Die vorgestellten Protokolle basieren auf bekannten und analysierten Algorithmen

Symmetrische Verschlüsselung

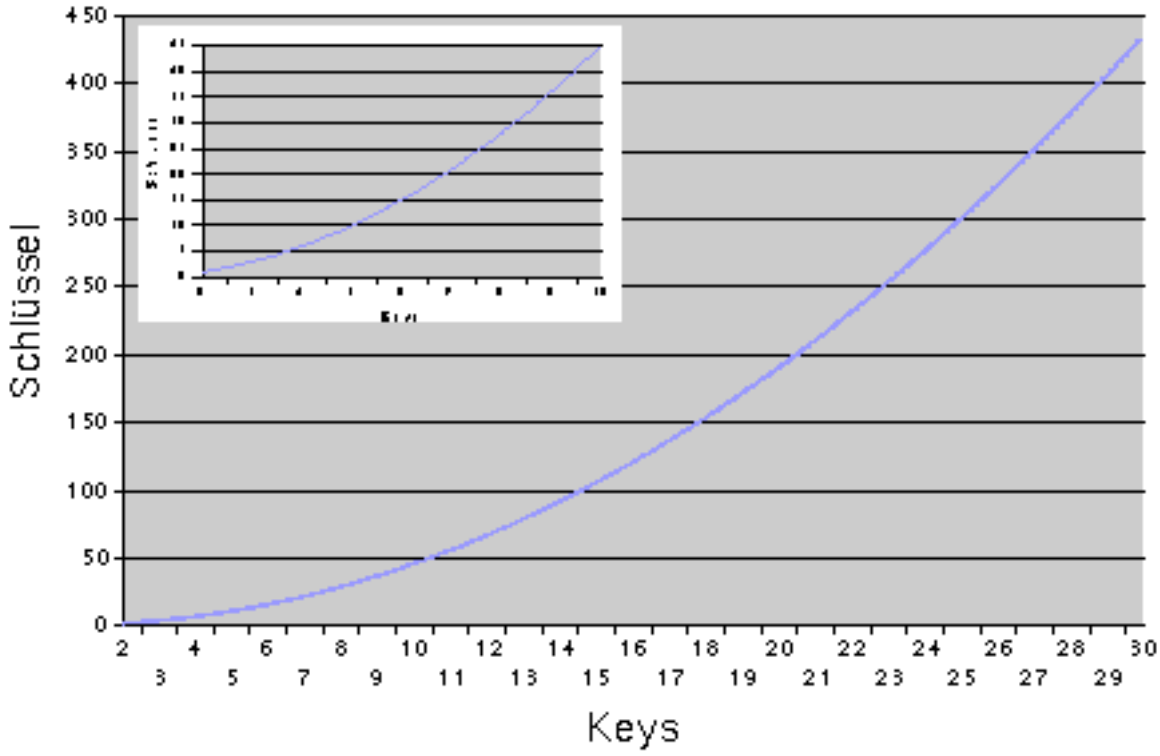
- Der Entschlüsselungsschlüssel (E_K) ist aus dem Verschlüsselungsschlüssel (V_K) ableitbar
- Bei Cäsarverschlüsselung: Zahl der Buchstaben: N

  $\Rightarrow E_K = N - V_K$
- Bekannte symmetrische Verfahren: DES, IDEA, RC2, RC5, CAST, Blowfish, Twofish

Symmetrische Verschlüsslung

- Symmetrische Verschlüsselungen mit weniger als 112 Bit Schlüssellänge gelten als unsicher.
- Sie werden je nach Anwendung in verschiedenen Betriebsmodi eingesetzt
  - ECB Electronic Codebook Modus
  - CBC Cipher Block Chaning
  - CFB Cipher Feedback Modus
  - OFB Output Feedback Modus
- Bei n Kommunikationspartnern sind $\frac{n \cdot (n-1)}{2}$ Schlüssel notwendig

Anzahl der notwendigen Schlüssel (symmetrisch)



Asymmetrische Verschlüsselung

- Der Entschlüsselungsschlüssel kann nicht aus dem Verschlüsselungsschlüssel abgeleitet werden
- Die beiden Schlüssel sind miteinander verknüpft
- Der Verschlüsselungsschlüssel wird nicht geheim gehalten, sondern öffentlich verteilt. Daher heißt er öffentlicher Schlüssel

Asymmetrisch

- Asymmetrische Verfahren lösen das Problem der Schlüsselverteilung
- Bei n Kommunikationspartnern sind n Schlüssel notwendig
- Asymmetrische Schlüssellängen von weniger als 1024 Bit gelten für dauerhafte Nutzung als unsicher
- Bekannte asymmetrische Verfahren sind: RSA, DH, El–Gamal oder die neueren Verfahren mit elliptischen Kurven

Unterschiede

- Symmetrische Verfahren sind recht schnell
- Asymmetrische Verfahren sind eher langsam
- Schlüsselaustausch bei symmetrischen Verfahren ist problematisch
- Symmetrische Verfahren arbeiten meist mit einfachen mathematischen Operationen
- Asymmetrische Verfahren nutzen komplexe mathematische Operationen auf großen Zahlen

Unterschiede

- Asymmetrische Schlüssel müssen bei gleicher Sicherheitsstufe wesentlich länger sein als symmetrische Schlüssel
- Schlüsseläquivalenz:

Symmetrisch	Asymmetrisch
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

Begriffsklärungen

- Symmetrische Verschlüsselungen
- Asymmetrische Verschlüsselungen
- Hashfunktionen oder Checksummenfunktionen
  - Ermitteln einen Kennwert für eine Nachricht
  - Kryptografische Hashfunktionen sind mindestens 128 Bit lang
- Zufallszahlengeneratoren für kryptografische Anwendungen

Authentisierungssysteme

- Systeme, die als vertrauenswürdige Instanz zwischen nicht vertrauenswürdigen Systemen auftreten
- Können mit einem Notar verglichen werden

Angriffsmöglichkeiten

- Angriff auf das verwendete Verfahren oder die aktuelle Implementierung
- Brute–Force–Angriff
- Man–in–the–middle–Angriff
  - Beim Austausch der Schlüssel zweier Kommunikationspartner werden beide Schlüssel durch Schlüssel des Angreifers ersetzt.
  - Verschiedene Methoden der Verhinderung des Angriffs
- Replay–Angriff

Anwendungen

- Secure Shell (ssh)
- Secure Socket Layer (ssl)
- Kerberos
- OpenPGP / Gnu Privacy Guard

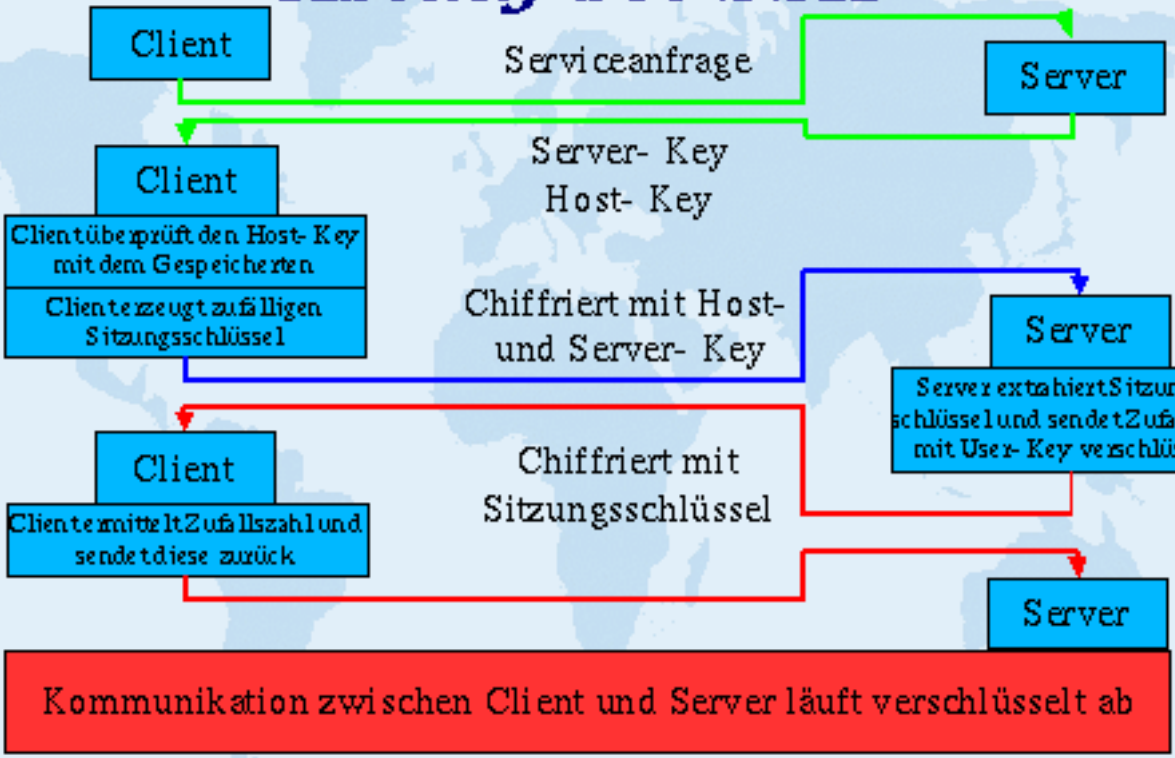
Secure Shell

- Dient als Ersatz für Telnet, rlogin, rsh, rcp
- Kann andere Protokolle (X11, etc.) tunneln
- Fällt bei Nichtverfügbarkeit des Dienstes automatisch (mit Meldung) auf ungesicherte Dienste zurück
- Ist für nahezu jedes übliche Betriebssystem verfügbar

Vorbereitungen

- Jeder beteiligte Rechner erzeugt ein RSA–Schlüsselpaar (Host–Key) der Länge 1024 Bit
- Beim Start des Service auf einem Server wird ein RSA–Schlüsselpaar (Server–Key) der Länge 768 Bit erzeugt. Dieser wird stündlich gewechselt
- Jeder User erzeugt sich ein RSA–Schlüssel–paar (User Authentication Key) der Länge 1024 Bit
- Die öffentlichen Schlüssel sind auf den beteiligten Systemen verfügbar

Ablauf bei SSH



Angriff auf SSH

- Im Sommer wurde ein interessanter erfolgreicher Angriff auf ssh bekannt
- ssh sendet jeden Tastenanschlag sofort verschlüsselt an den Host
- Aus dem zeitlichen Datenstrom kann auf die getippten Zeichen geschlossen werden
- Damit wurden Passworte erfolgreich ermittelt

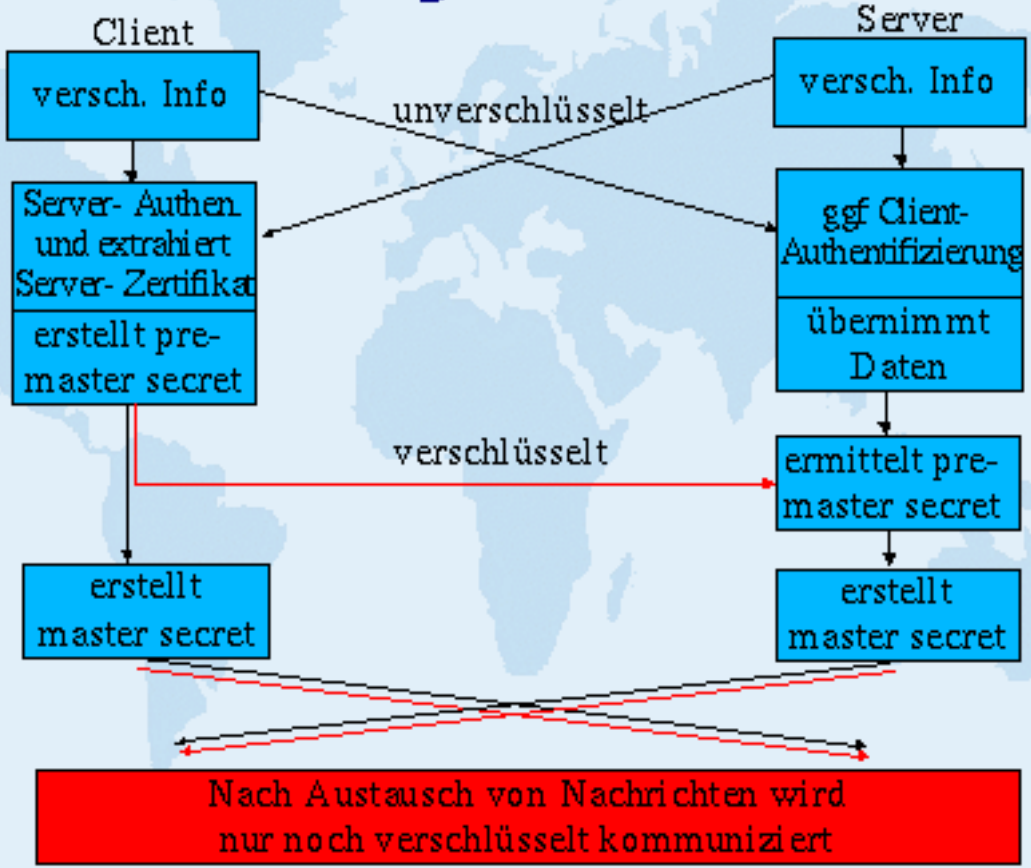
Secure Socket Layer

- SSL „sitzt“ zwischen dem Application- Layer und dem Network- Layer der Netzwerkkommunikation
- Es ist in der Lage verschiedene Protokolle (**http**, ldap, imap, pop3, ...) abzusichern
- Die Nutzung erfolgt transparent für den User
- Die üblichen Browser zeigen den Zustand im allgemeinen über das Symbol eines geschlossenen Schlosses an
- SSL basiert auf verschiedenen ausgestellten Zertifikaten sogenannter Zertifizierungsinstanzen (CA)

Secure Socket Layer

- Verwendet verschiedene symmetrische und asymmetrische Algorithmen für die Verschlüsselung und verschiedene Hashfunktionen für Prüfsummenermittlung
  - DES, Triple-DES, RC2, RC4, SKIPJACK (in Hardware)
  - KEA, RSA, RSA key exchange
  - MD5 und SHA-1 in Verbindung mit DSA
- Algorithmen bilden sog. Cipher–Suiten
- Innerhalb der Cipher–Suiten wird eine Kombination der Verfahren ausgewählt

Ablauf von SSL



Server Authentifikation

- Server hat Zertifikat an den Client gesendet
- Client nimmt vier Prüfungen vor
  - Liegt das aktuelle Datum innerhalb des Validitätszeitraumes des Zertifikates?
  - Findet sich die ausstellende CA in der Liste der vertrauenswürdigen CAs des Clients?
  - Ist die Signatur des Zertifikates in Ordnung?
  - Stimmt der Domainname des Servers mit dem Domainnamen im Zertifikat überein?
- Sind alle Prüfungen i. O., ist der Server okay

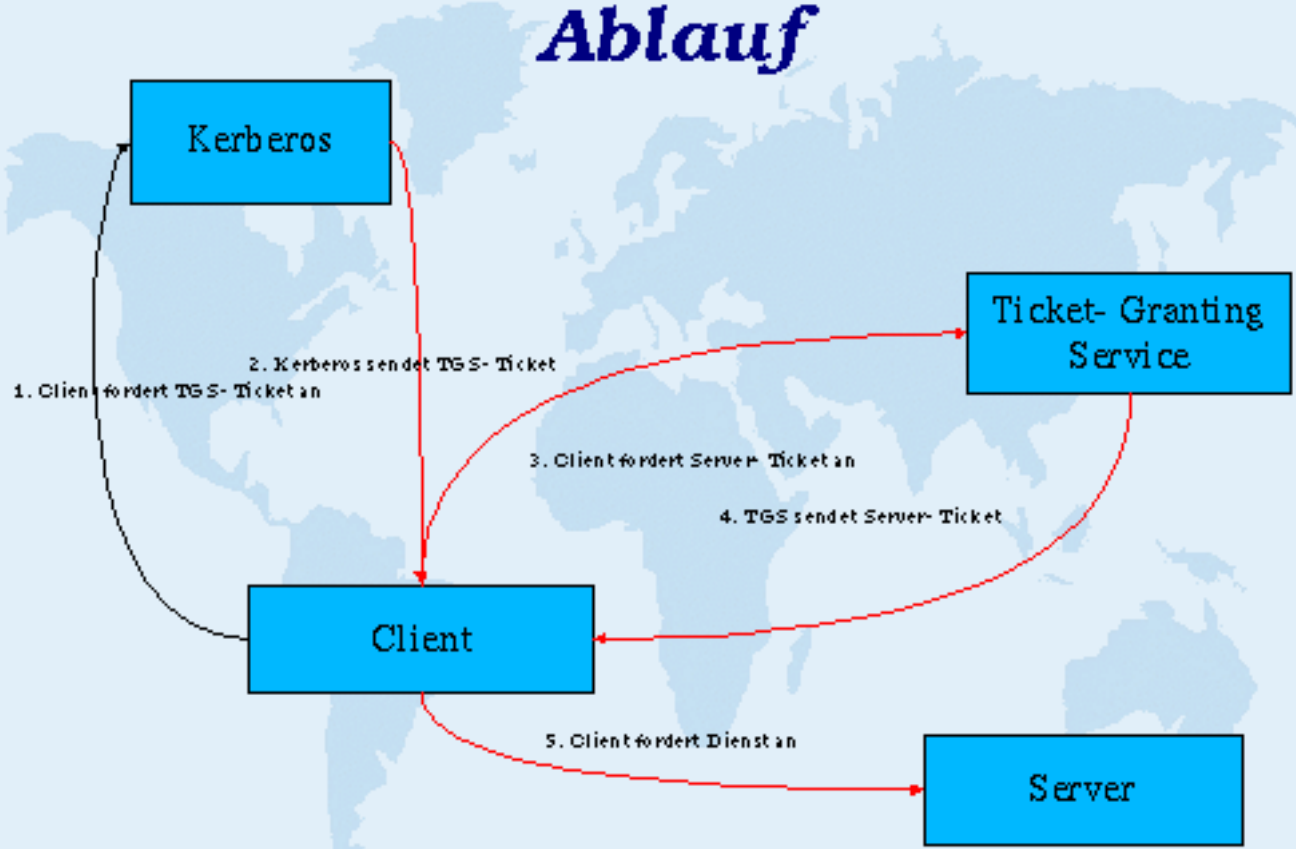
Client Authentifikation

- Ablauf prinzipiell wie Server–Authentifikation
- Zusätzlich eine fünfte Prüfung
  - Ist das Client/User–Zertifikat in dem LDAP–Eintrag für den Client/User aufgelistet?
- Sind alle Prüfungen i. O., ist der Server okay

Kerberos

- Protokoll von Needham und Schroeder (1978)
- Das System kommt mit einem symmetrischen Verschlüsselungsverfahren aus
- Wichtig sind weitgehend synchron laufende Uhren aller beteiligten Systeme
- Benutzt Tickets
  - server, client, client-ip, Zeitbereich, Sitzungsschlüssel
- und Authentikatoren
  - Client, Zeitstempel, Sitzungsschlüssel

Ablauf


Kerberos
Ticket- Granting Service
2. Kerberos sendet TGS- Ticket
1. Client fordert TGS- Ticket an
3. Client fordert Server- Ticket an
4. TGS sendet Server- Ticket
Client
5. Client fordert Dienst an
Server

PGP/OpenPGP/Gnu Privacy Guard

- PGP wurde 1991 erstmalig herausgegeben
- 1992 entstand die berühmte Version 2.x mit RSA und IDEA als Verschlüsselungsroutinen
- PGP ist für Privatnutzer konzipiert und bis zur Version 6.5 privat kostenlos einsetzbar
- Mittlerweile gehört PGP der Firma NAI
- Heute werden RSA, DSA/DSS, CAST, IDEA, u. a. als Verschlüsselungsroutinen verwendet
- Es gibt verschiedene teilweise inkompatible Versionen des Programmes

PGP/OpenPGP/Gnu Privacy Guard

- Definition von RFC1510 als Reaktion
- GPG ist eine Implementierung von RFC1510
- Jeder Benutzer erstellt sich sein Schlüsselpaar
- Es gibt keine zentrale Sicherheitsinstanz!
- Keyserver sind keine Signaturinstanzen!

Schlüsselhandling

- Der geheime Schlüsselteil wird durch ein symmetrisches Verfahren gesichert abgespeichert
- Die Passphrase für das symmetrische Verfahren kann jederzeit geändert werden
- Die Schlüsselgenerierung kann sehr lange benötigen, da zwei sehr grosse Primzahlen gesucht werden
- Schlüssellänge 1024 Bit $\Rightarrow \approx$150 Stellen
  Schlüssellänge 4096 Bit $\Rightarrow \approx$600 Stellen

Schlüsselaustausch

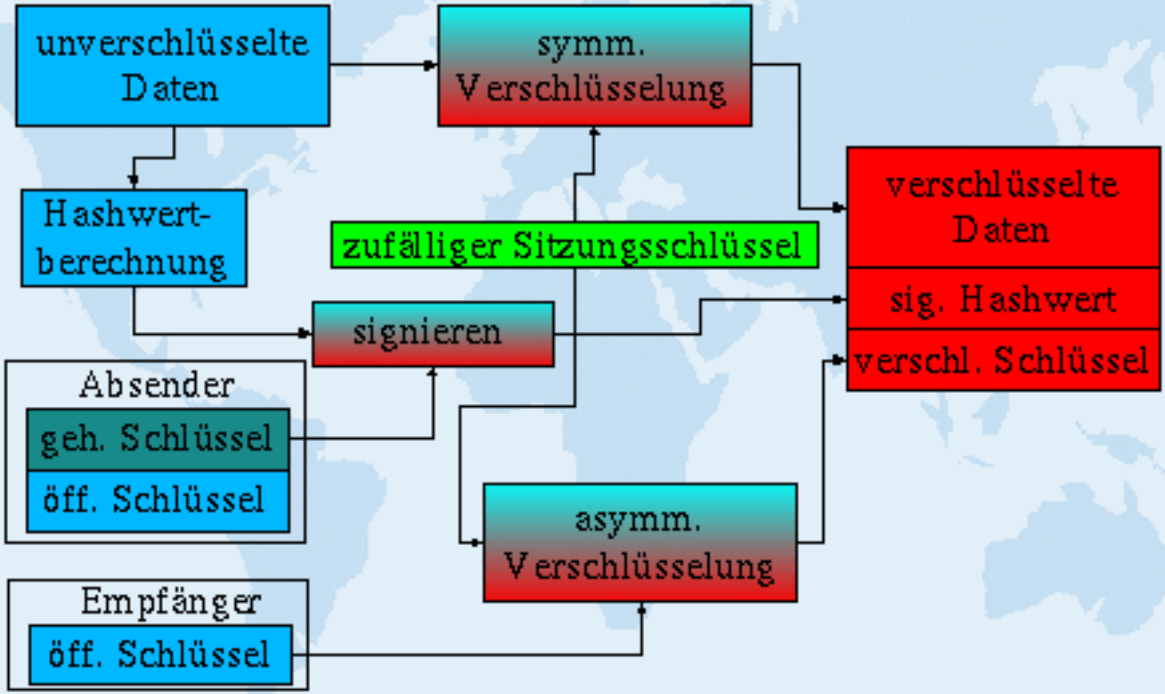
- Wird der Schlüssel nicht persönlich ausge–tauscht, so sollte der Fingerabdruck der getauschten öffentlichen Keys geprüft werden
- Jeden Schlüssel, dem man vertraut, ist die eigene Signatur anzuhängen
- Erhält man einen Schlüssel, der eine Signatur trägt, der man vertraut, so kann man dem Schlüssel vertrauen

Beispiel für einen Key

```
pub  1024D/8D6C472E 1999-08-02 GBV-IT-SiBe Fdh <gbv.itsibe@dornier.dasa.de>
sig         2DB34E09 1999-08-09  Wolff, Marieluise <Wolff. Marieluise>
sig         C0743E43 1999-08-09  GBV-IT-SiBe Ulr <gbv.itsibe@vs.dasa.de>
rev         8D6C472E 2000-03-02  GBV-IT-SiBe Fdh <gbv.itsibe@dornier.dasa.de>
rev         3332F5C  2000-03-02  Krauss Peter <krauss.peter@dornier.dasa.de>
sig         8D6C472E 2000-03-02  GBV-IT-SiBe Fdh <gbv.itsibe@dornier.dasa.de>
sig         DC54191C 2001-01-13  [User-ID nicht gefunden]
sig         3332F5C  2000-03-02  Krauss Peter <krauss.peter@dornier.dasa.de>
sig         3767123F 2000-09-25  Grueneer Herbert <herbert.gruener@m.dasa.de>
sig         DFF43E87 2000-09-25  IT-Sicherheit der Dasa <herbert.gruener@m.dasa.de>
sig         85104EE1 2001-06-20  Menter Karl <menter.karl@vs.dasa.de>
sub  2048g/A3D3D29E 1999-08-02
sig         8D6C472E 1999-08-02  GBV-IT-SiBe Fdh <gbv.itsibe@dornier.dasa.de>
```

- pub -> Public-Key
- sig -> Signatur
- rev -> Zurückgezogene Signatur
- sub -> Unterschlüssel

Verschlüsselung



Entschlüsselung