

# Verschlüsselung Teil (I)

LUG-VS (Ulf Bartholomäus)

GnuPG

PGP

Email Verschlüsselung

Daten Verschlüsselung

Platten / Partition Verschlüsseln

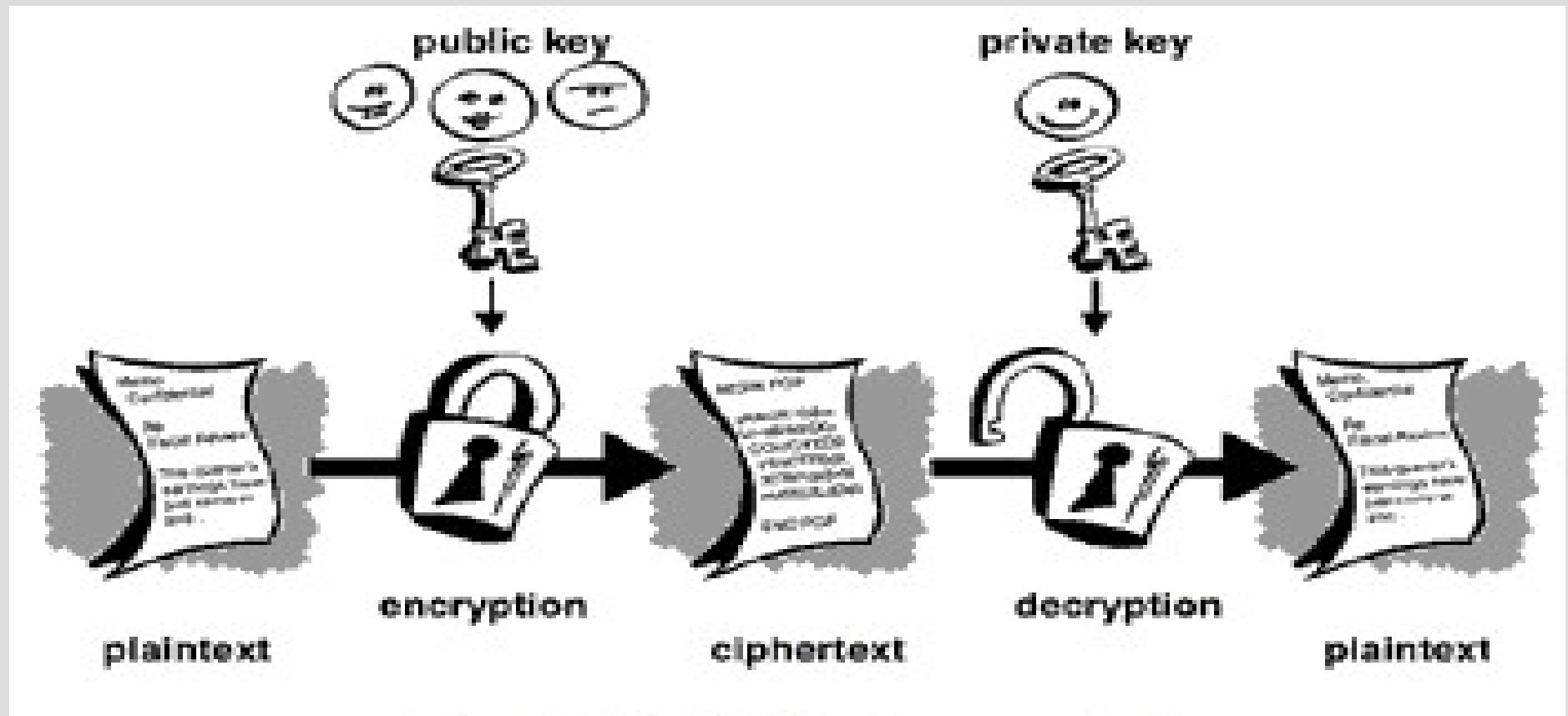
# Übersicht

- Warum Verschlüsselung
- Wie funktioniert Verschlüsselung
- Welche Verfahren gibt es
- Welche Schlüssellänge wann verwenden
- Womit Verschlüsselt man
- Wie sichere ich meine Schlüssel
- Passwort richtig generieren

# Warum Verschlüsselung

- Beim Datenaustausch
  - Internet-Daten (Email) normalerweise Klartext (Über unbekannte Rechner)
  - Problem Datensammlung und Vermarktung
- Lokal (insbesondere auf Mobilten Rechnern)
  - Einbruch durch Intranet bzw. Internet
  - Lokaler Angriff auf Rechner
- Sonder Anwendung – Signatur
  - Digitale Unterschrift

# Wie funktioniert Verschlüsselung



# ☐ Welche Verfahren gibt es

- Symmetrische Verfahren
  - Einfache Verfahren bei denen der Sender und der Empfänger den gleichen Schlüssel benutzen
- Asymmetrische Verfahren (public-key)
  - Hier wird ein Schlüsselpaar generiert, bei dem es einen öffentlichen (publizierten) key und einen privaten (durch ein langes Passwort – die so genannte „passphrase“ - gesichert)
- Misch-Verfahren (heute meist verwendet)
  - Hier wird der Sitzungsgenerierte Sym. Schlüssel für die Daten per Asym. Schlüssel übertragen

# ☐ Welche Schlüssellänge wann verwenden

Grundsätzlich muss man sich fragen, wie wichtig sind die Daten für mich bzw. können sie für einen Angreifer sein?

Je wichtiger die Daten, um so höher sollte der Aufwand für die Verschlüsselung sein!

D.h. im konkreten Fall, je wichtiger die Daten desto länger muss der Schlüssel gewählt werden (im Idealfall ist er so lang wie die Daten)!

# ☰ **Womit Verschlüsselt man**

Grundsätzlich hängt das verwendete Verfahren stark von dem Anwendungszweck ab.

- Email oder Daten die über große Distanzen unter Umständen mit nicht näher bekannten Personen ausgetauscht werden.
  - Asymmetrische oder Mischverfahren  
z.B. GnuPG, PGP, S/MIME, ...
- Lokale Daten die schnell Verarbeitet werden müssen (Schlüssel auf geeigneter HW)
  - Symmetrische Verfahren  
z.B. DES, IDEA, AES, ...

## ☰ Wie sichere ich meine Schlüssel

Da der Schlüssel für jeden potentiellen Angreifer interessant ist sollte er so sicher wie möglich aufbewahrt werden.

- Sicherung wieder durch Verschlüsselung mit einem Passwort bzw. „passphrase“.
- Sicherung durch Pin und einem Schlüssel auf einem sicheren Medium (z.B. auf einer Chip-Karte)
- Sicherung durch spezielle Verfahren (Hardware)

## ☐ **Password richtig generieren**

- Damit das Passwort bzw. die „passphrase“ möglichst schwer zu erraten ist, sollte es genügend Lang sein und in geeigneter weise aufgebaut sein.
- z.B. „DieT,fesP,a212“ im Klartext (Dieses ist ein Test, für ein sicheres Passwort, am 28.11.2003)
- Ein sicheres Passwort / „passphrase“ setzen sich aus Buchstaben (groß und klein), Zahlen und Sonderzeichen zusammen!

# ☰ **Schlussbemerkung**

Ich habe hier das Thema „Verschlüsselung“ nur angerissen. Es gibt zahlreiche unterthemen und -gebiete.

- Signatur  
(Bestätigung der Urheberschaft und Richtigkeit – digitale Unterschrift)
- Steganographie  
(Verstecken einer meist Verschlüsselten Daten in einem andern Datenstrom wie z.B. Bilder, Musik, Filme, usw.)

PS: Literaturhinweise demnächst auf <http://www.lug-vs.de/>