# Verschlüsselung im Alltag

Bürgernetzvortrag

Putzbrunn, 1.04.2008

Referent: Rüdiger Zwarg

(cms-professionals.de)

# Anwendungsfelder

- Passwort-Safe (PINs, TANs, Zugangsdaten)
  - Einzeldaten einsehen
- Laufwerkverschlüsselung
  - mit Dokumenten arbeiten
- Einzelverschlüsselung, sicheres Löschen
  - z. B. Dokumente versenden
- Zertifikate / Schlüssel (PGP u. S/MIME)
  - sicherer eMail-Versand

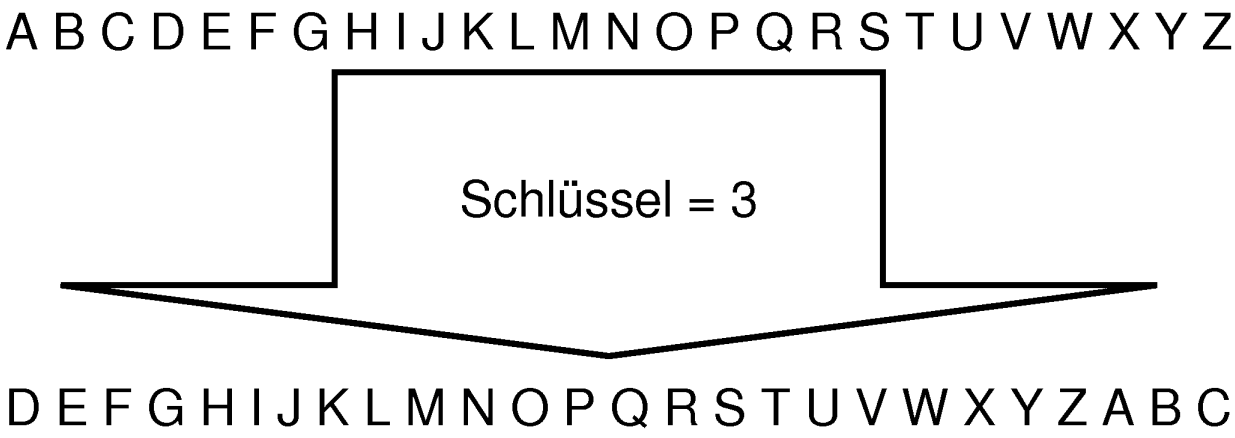
# Die Programme

KeePass, RohosMini und RemoraDiskguard sind direkt ausführbar

- KeePass (Passwort-Safe)
- Truecrypt / RohosMini (virtuelle Laufwerke)
- AxCrypt / RemoraDiskguard (Dateiverschlüsselung)
- WipeFree, FileShredder (sicheres Löschen)
- abylon Selfcert (Signaturen, Zertifikate)

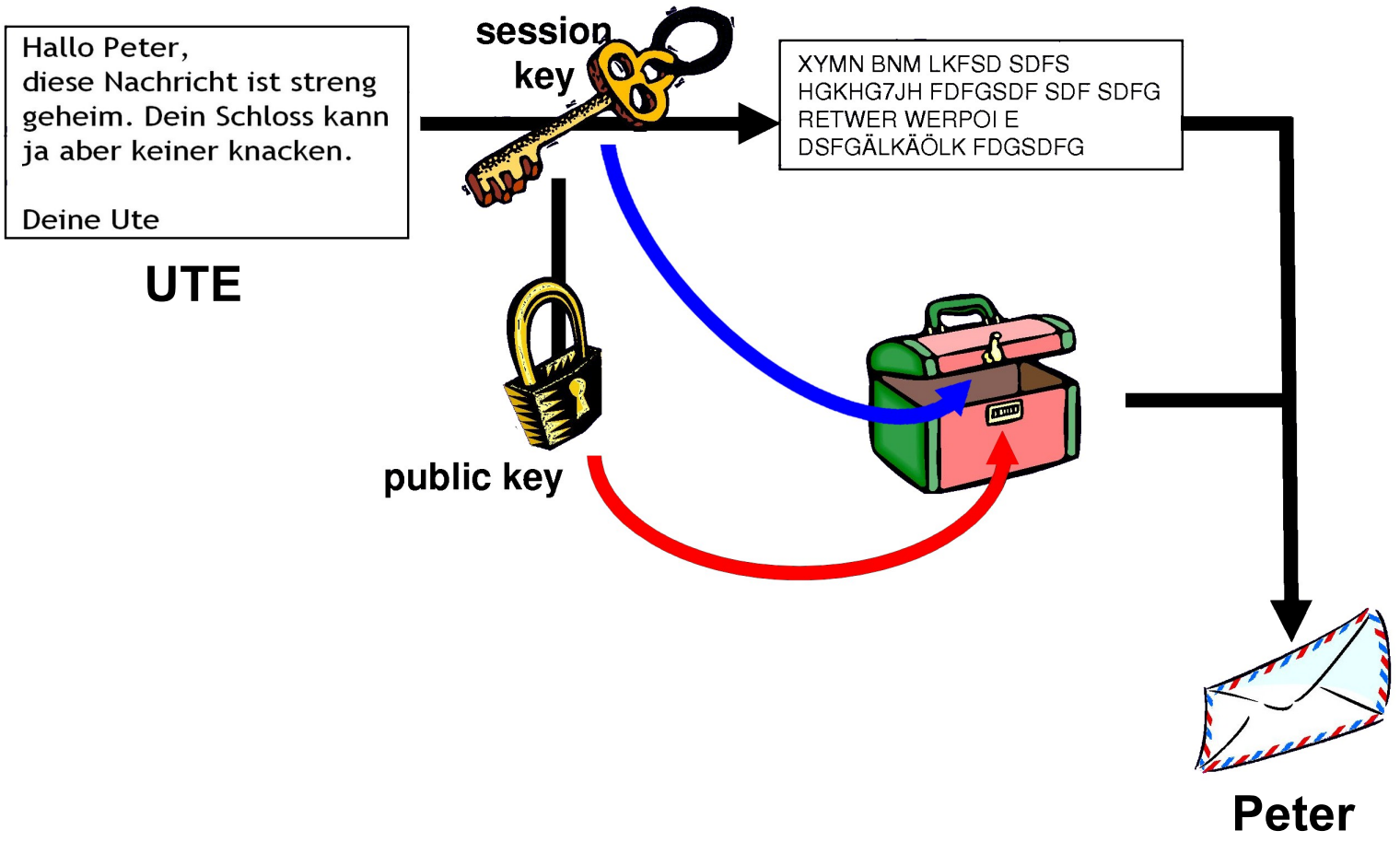
# Symmetrische Verschlüsselung

**Julius Caesar**




**JULIUS CAESAR ⟶ MXOLXV FDHVDU**

# Hybride Verschlüsselung



# Beispiele für die Verschlüsselungsverfahren

**Symmetrische Verfahren**
DES, Triple-DES, IDEA, RC2, Blowfish

**Asymmetrische Verfahren**
RSA, DAS, Elliptic Curve, Diffie Hellman

**Hybride Verfahren**
PGP, S/MIME, PGP MIME, SSL

# Empfehlungen

- Passwörter, PINs und TANs nur im Passwort-Safe
- Sensible Daten auf verschlüsselte Laufwerken
- Ab und zu leere Speicherbereiche physisch löschen
- eMails nach Bedarf verschlüsseln