Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

https://www.all-electronics.de/post-quantum-kryptographie/

Betreuer: Nathanael Huebbe

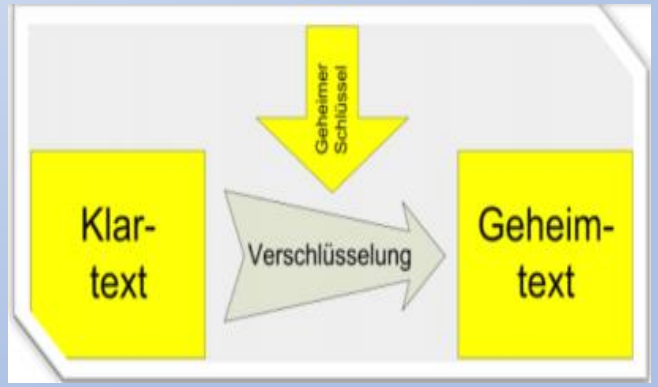
Verschlüsselung - Speicher- & Dateisysteme

Agenda

Infos zum Einstieg (Kryptographie)

<u>Allgemein</u>

- Verwendung versch. Schlüsseln
- Wieso?
    - Vertraulichkeit
    - Datenintegrität
    - Authentifizierung



→ *Hauptziele:*

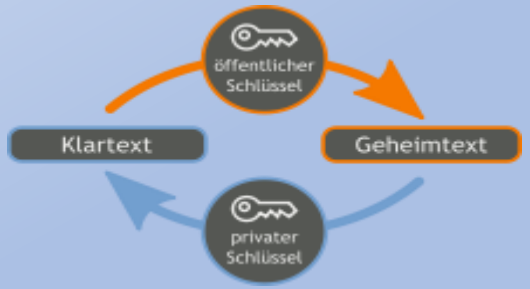
- Zugriffsschutz/Vertraulichkeit
- Fälschungsschutz
- Änderungsschutz

Verschlüsselungsarten

- *Symmetrisch:*
  - = Benutzung desselben Schlüssels

- *Asymmetrisch:*
  - erhöhte Sicherheit
  - hoher Aufwand

    → langsamer als symm.

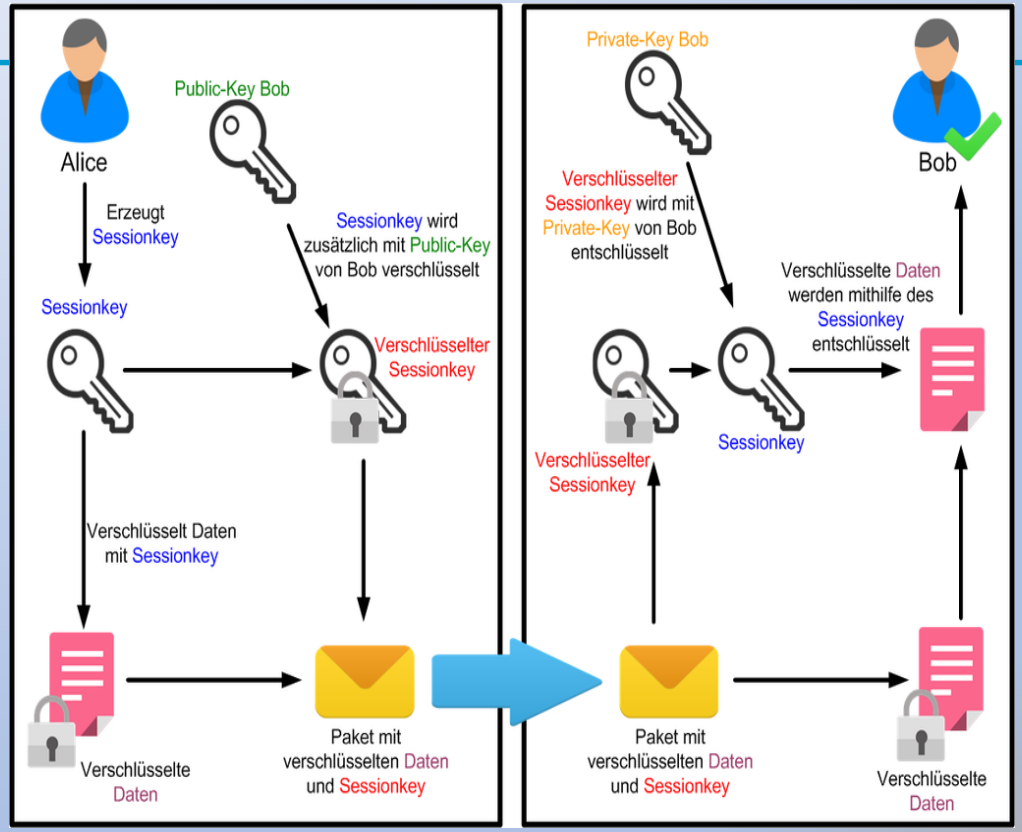


https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem#/media/File:Orange_blue_public_key_cryptography_de.svg

https://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsselung#/media/File:Hybrid_2_encrypt.png

Hybrid:

- Kombination von symm. & asymm. V.
- Session-Key
  - symm. verschlüsselt
  - → asymm. entschlüsselt



Risiken bei Verschlüsselung

- Brute-Force Angriffe
  = Durchprobieren aller mgl. Kombinationen
- Schwache Passwörter
- sorgloser Umgang → private key
- Wörterbuchangriff
  = Ausprobieren aller Wörter einer Sprache
- Man-in-the-middle Angriff
  = Angreifer als Empfänger

Verschlüsselung durch das Dateisystem

Encrypting File System (Encryptfs)

- ≙ Verschlüsselungssystem auf Windows basierend
- Dateien mit NTFS verschlüsseln → New-Technology-File-System

Funktion:

– Verschlüsselte Daten → Verzeichnis 1 speichern
  – Darstellung unverschlüsselt im Verzeichnis 2

Dateisysteme verschlüsseln:

- DS verschlüsselt Datei symm. (*File Encryption Key*)
- Schlüssel für berechtigten Personen wird öffentlich verschlüsselt
- → asymmetrisch verschlüsselt

Mögliches Problem:

- Datensicherheit: Geheimer Schl. Verloren
  →Datenverlust

Lösung:

- FEK & public key verschlüsseln → beim neuen *Key Recovery Agent* abspeichern

Nachteile von EFS:

- Kann keine ganzen Festplattenvolumes verschlüsseln
  - → dafür wird TPM Verschlüsselung (hardwarebasierend) wie BitLocker benötigt

- Schützt keine über Netzwerk gesendete Dateien
  - → entschlüsselt gesendet

Encrypted Filesystem (EncFS)

≙ Erweiterung für Mehrbenutzer-Betriebssysteme(unix)

- Verschlüsselt einzeln
  - → Kein individ. Einfluss
  - → Nutzung aller Werkzeuge, wie Datensicherung/Nachrüstungen

- baut auf FUSE-Framework auf

  Kenel-Modul, ermöglicht Übergang von DS-Treiber aus Kernel in User-Mode

Funktion:

1.Verzeichnis

→ benötigten Daten hier ablgen

Zwischenschritt

→ Daten von EncFS verschlüsselt

2.Verzeichnis

→ verschlüsselt gespeichert

Resultat:

Verzeichnis 1 nur sichtbar

→ falls 2.Verzeichnis für das Erste eingebunden ist

Vor- & Nachteile

+ :

- Datenspeichern bis zum max im EncFs
- → belegt keine feste Größe, nur Platz
- DS-Teile auf versch. Datenträger ablegbar
- Datensicherungsprogramme

  → einzelne veränderte Daten ohne Partition sichern

- :

  - Fragmentierung auf Daten im Verzeichnis
    - → = ungeord. Zergliederung eines Speichers von Datenblöcken des DS

  - Rechteverwaltung wird nicht neu implementiert
    - →Anzahl d. Dateien, Zugriffsrechte, Größe & Länge des Dateinamens & letzte Datum **sichtbar für jeden**

Logische Datenträgerverschlüsselung

dm-crypt:

≙ Kryptographie-Modul des Linuxkernels

Allg. Infos:

- Verwendung: Partitionen, Festplatten oder log. Laufwerke ver- / entschlüsseln
  - → unsichtbare Zwischenschicht zw. Daten & dem DS

- stellt viele Alg. aus Crypto-API des Linuxkernels zur Verfügung

Bezug auf Erweiterung mit LUKS:

= Linux Unified Key Setup (Systemencryptionformat unter Linux)

- Software im Betriebssystemkern
  - Standardmethode in Linux → Verschlüsselung d. **ganzen Betriebssystems**

- Erweiterung = Daten um eine Kopfzeile („Header“) hinzufügen
  → Einfachere Verwaltung d. Daten

Vorteile (i.G.z. dm-crypt):

- Standardisiert
- Vergabe bis 8 Schlüsseln
- Zugriff auf Schlüsseln ohne Umschreiben d. verschlüsselten Daten
- Erleichtert Angriffe
- z.B. klaut Angreifer → jedoch kommt nicht an Daten

VeraCrypt

≙ Open-Source-Software für Datenverschlüsselung

→ um einzelne Datenbestände/Betriebssystem zu verschlüsseln

Allg. Infos:

- Abspaltung von TrueCrypt (2012)
- i.G.z. LUKS: Betriebssystem nachträglich verschlüsseln
- Entwicklungsende TrueCrypt → Nachfolgerprojekt VeraCrypt

  → basiert auf TrueCrypt

Vor- & Nachteile:

+ :

- systemübergreifende Verfügbarkeit
  - unterstützt mehrere Systemplattformen
- sicherer Dateiaustausch (für ext. Datenträger)
- glaubhafte Abstreitbarkeit
  - Passwortherausgabe → wichtige Daten geschützt
- Komplettverschlüsselung d. Betriebssystems
- mehrsprachig
- Truecrypt kompatibel

- :

  - max. 26 Laufwerkbuchstaben
  - Zusammenfassen mehrerer Laufwerke(VeraCrypt) → nicht möglich
  - Probleme mit UEFI
    - Version unterstützt, aber Probleme mit Secure Boot
    - im Nachteil i.G.z. Nativen Lösungen (TrueCrypt, LUKS, etc.)

→ Unattraktiv bei modernen Betriebssystemen

Literatur

- https://de.wikipedia.org/wiki/Verschl%C3%BCsselung
- https://www.itwissen.info/Verschluesselung-encryption-ENC.html
- https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem
- https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem
- https://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsselung
- https://de.wikipedia.org/wiki/Kryptoanalyse
- https://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption
- https://wiki.archlinux.org/index.php/disk_encryption
- https://wiki.ubuntuusers.de/ecryptfs/
- https://de.wikipedia.org/wiki/EncFS
- https://de.wikipedia.org/wiki/Dm-crypt
- https://de.wikipedia.org/wiki/Dm-crypt#Erweiterung_mit_LUKS
- https://curius.de/verschluesselung/veracrypt-systemuebergreifende-verschluesselung
- https://www.t-online.de/digital/sicherheit/id_80523692/veracrypt-festplatte-von-windows-verschluesseln.html
- https://de.wikipedia.org/wiki/VeraCrypt