VerSchlüsselung

<<TableOfContents>>

= Verschlüsselung =

== Was ist Verschlüsselung ==

Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text (Klartext) (oder auch Informationen anderer Art, wie Ton- oder Bildaufzeichnungen) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine „unleserliche“, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird. Als entscheidend wichtige Parameter der Verschlüsselung werden hierbei ein (Symmetrische Verschlüsselung)oder auch mehrere Schlüssel (Asymmetrische Verschlüsselung) verwendet.

=== Symmetrische Verschlüsselung ===

Bei symmetrischer Verschlüsselung haben beide Teilnehmer den gleichen geheimen Schlüssel womit der Klartext verschlüsselt wird. Das Problem ist die Geheimhaltung des Schlüssels.

=== Asymmetrische Verschlüsselung ===

Bei asymetrischer Verschlüsselung hat jeder Teilnehmer einen privaten und einen öffentlichen Schlüssel. Der Klartext wird dabei vom Sender mit seinem geheimen Schlüssel und dem öffentlichen des Empfängers verschlüsselt. Dieser kann die Nachricht wiederum durch seinen geheimen und den öffentlichen Schlüssel des Empfängers entschlüsseln.

== Anwendungen ==

=== Festplattenverschlüsselung ===

Mit WikiPedia:VeraCrypt lassen sich Festplatten unter Windows verschlüsseln, unter Linux stehen verschiedene Verschlüsselungsprogramme zur Auswahl. Bei der Installation wird abgefragt ob die Festplattenpartition verschlüsselt werden soll.

==== Festplattenverschlüsselung unter Linux ====

[[https://help.ubuntu.com/community/EncryptedFilesystemHowto3|Ubuntu Hilfeseite zur Festplattenverschlüsselung nach der Installation mit Luks]]

==== Festplattenverschlüsselung unter Windows ====

[[https://veracrypt.codeplex.com/|Offizielle VeraCrypt Webseite]]

=== Verschlüsselung der IP-Pakete ===

WikiPedia:IPsec verschlüsselt direkt die einzelnen WikiPedia:IP Pakete (Die IP-Pakete sind die Basis der Internetverbindung)

=== Verschlüsselung der Funkverbindung vom Handy zur Funkzelle ===

Die Funkverbindung vom Handy zur Funkzelle ist einfach verschlüsselt. Einfach heißt, dass die Verschlüsselung (sie heißt WikiPedia:A5/1) knackbar ist.

=== Verschlüsselung von Internetverbindung ===

WikiPedia:Https, WikiPedia:SSH_File_Transfer_Protocol und WikiPedia:SSH bieten eine Verschlüsselung vom Client(User) zum Server.

=== Tor und andere Anonymisierungsdienste ===

Anonymisierungsdienste, wie WikiPedia:Tor, benutzen mehrfache Verschlüsselung um die Herkunft zu verschleiern. Anschaulich wird immer das Beispiel des Briefumschlages im Briefumschlag verwendet. D.h. der ursprüngliche Brief wird in einen Umschlag mit dem Empfänger und einem Zwischenabsender. Dieser Brief wird wiederum in einen weiteren Umschlag gepackt mit dem Zwischabsender als Empfänger und einem weiteren Zwischenabsender als Absender. Dieses wird vier bis fünf mal wiederholt, bis im äußersten Umschlag der richtige Absender als Absender steht und als Empfänger der erste Zwischenabsender. Technisch realisiert wird das durch mehrfache Verschlüsseleung der WikiPedia:IP-Pakete. Ein Briefumschlag ist so eine Verschlüsselung des IP-Paketes.

[[http://www.torproject.org/|Webseite des Tor-Projects]]

=== eMail Verschlüsselung ===

Die E-Mail-Verschlüsselung funktioniert in dem die Mail vom Absender mit seinem geheimen und dem öffentlichen Schlüssel des Empfängers verschlüsselt wird. Der Empfänger kann die Mail mit seinem geheimen Schlüssel und dem öffentlichen des Empfängers öffnen. Mathematisch sind die Schlüssel Primzahlen, da die Verschlüsselung mit einer mathematischen Funktion geschieht. (unter [[VeranstaltungsMaterial]] gibt es ein [[http://www.datenschmutz.de/li/PGP/skript.pdf|Skript]] zu PGP und eMail Verschlüsselung)

==== Das Programm GnuPG ====

WikiPedia:GnuPG ist ein frei verfügbares Verschlüsselungsprogramm für eMails.

[[http://www.gnupg.org|Webseite des GnuPG Projects]]

===== GnuPG für Linux =====

Die Beschreibung der GnuPG Installation unter WikiPedia:Ubuntu Linux per Befehlszeile:

[[https://help.ubuntu.com/community/GnuPrivacyGuardHowto|Ubuntu-Hilfeseiten]]

GnuPG Installation unter WikiPedia:Ubuntu per GUI:

[[https://wiki.ubuntu.com/UserDays/01232010/SeahorseGPG|Ubuntu Wiki]]

===== GnuPG für Windows =====

Das Emailprogramm (WikiPedia:Thunderbird) mit GnuPG/Enigmail für den mobilen Einsatz (z.B. mit USB-Stick) unter Windows:

*[[http://portableapps.com/apps/internet/thunderbird_portable|Thunderbird Portable]] einfach auf ein Verzeichnis auf dem USB Stick installieren, und wie [[http://portableapps.com/support/thunderbird_portable#encryption|hier]] vorgehen

Wir haben aus den oben genannten Quellen ein ZIP-Archiv erstellt, das bereits Thunderbird Portable mit GnuPG und Enigmail enthält. [[https://datenschmutz.de/li/ThunderbirdPortable-45.6.0-de_Enigmail_GPG.zip|Hier]] runterladen und auf einem USB-Stick entpacken.

Einige Hinweise: Die Software von Thunderbird kann in der portablen Version aktualisiert werden.

Es ist möglich vorhandenen Daten zu integrieren. Entweder von einer festen oder einer portablen Installation. Die GPG-Schlüssel pubring.gpg und secring.gpg und die Datei trustdb.gpg kommen ins Verzeichnis ThunderbirdPortable\Data\gpg.

Normalerweise kann nur ein E-Mail-Profil in Thunderbird Portable verwaltet werden. Von einem vorhandenen USB-Stick (Thunderbird Portable) das Verzeichnis Data\profile\ kopieren. Von einer Festinstallation das Verzeichnis C:\Users\username\AppData\Roaming\Thunderbird\Profiles???.default\ nach Data\profile\ kopieren.

''Archivanmerkung: Früher mal haben wir das gemacht, was jetzt die Leute von Thunderbird portable machen. Die letzte ('''veraltete''') Fassung von uns lassen wir erstmal noch hier stehen.[[http://www.datenschmutz.de/downloads/Thunderbird_Portable_with_Enigmail+GPG_1.5.0.9_de-de.zip|(veraltete Version, nicht mehr verwenden)]].''

Version #1
Erstellt: 2025-10-27 22:49:52 UTC von Datenschmutz Migration Bot
Zuletzt aktualisiert: 2025-10-27 22:49:52 UTC von Datenschmutz Migration Bot