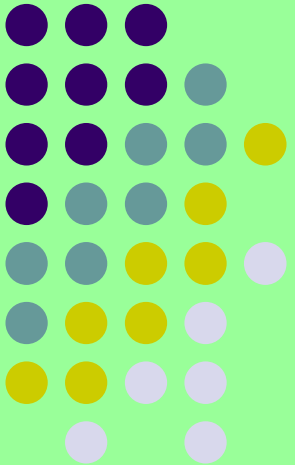
Verschlüsselungstechniken
(Überblick)

PC & Internet:

- e-Mail
- Datenverbindung
- Dateien



Verschlüsselungstechniken

Warum Verschlüsselung im Zusammenhang mit PC und Internet?

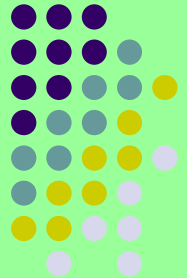
PC:

- eigene Daten vor Anderen schützen
- eigene Daten „unsichtbar" machen
- WLAN

Internet:

- Kommunikation nicht „veröffentlichen"
- „sichere" Verbindung zu Servern mit vertraulichen Daten (online-Händler, online-Banking, skype etc.)

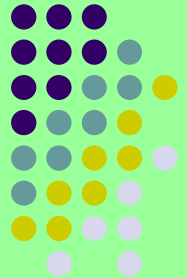
Verschlüsselungstechniken



Was ist Verschlüsselung?

Verschlüsselung (auch: Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“, so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.
Durch Verschlüsseln wird ein „Klartext“, also ein klar lesbarer Text, in einen „Geheimtext“, also in eine unverständliche Zeichenfolge umgewandelt. Die Begriffe Klartext und Geheimtext sind historisch gewachsen und symbolisch zu sehen. Außer Textnachrichten lassen sich auch andere Arten von Information verschlüsseln, wie Sprachnachrichten oder Bildaufzeichnungen. Die dahinterstehenden kryptographischen Prinzipien bleiben die gleichen.

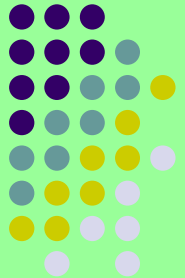
Verschlüsselungstechniken



Der Schlüssel

Der entscheidend wichtige Parameter bei der Verschlüsselung ist der „Schlüssel“. Die gute Wahl eines Schlüssels und sein sicherer Schutz vor unbefugtem Zugriff sind wichtige Voraussetzungen zur Wahrung des verschlüsselten Geheimnisses. Im Fall der Codierung stellt das Codebuch den Schlüssel dar. Im Fall der meisten klassischen und auch einiger moderner Methoden zur Verschlüsselung ist es ein Passwort. Bei vielen modernen Verschlüsselungen, beispielsweise bei der E-Mail-Verschlüsselung, wird dem Benutzer inzwischen die (Qual der) Wahl eines Schlüssels abgenommen. Der Schlüssel wird automatisch generiert, ohne dass er es bemerkt. Hierdurch wird auch der „menschliche Faktor“ eliminiert, nämlich die nicht selten zu sorglose Wahl eines unsicheren, weil zu kurzen und leicht zu erratenden, Passworts.

Verschlüsselungstechniken



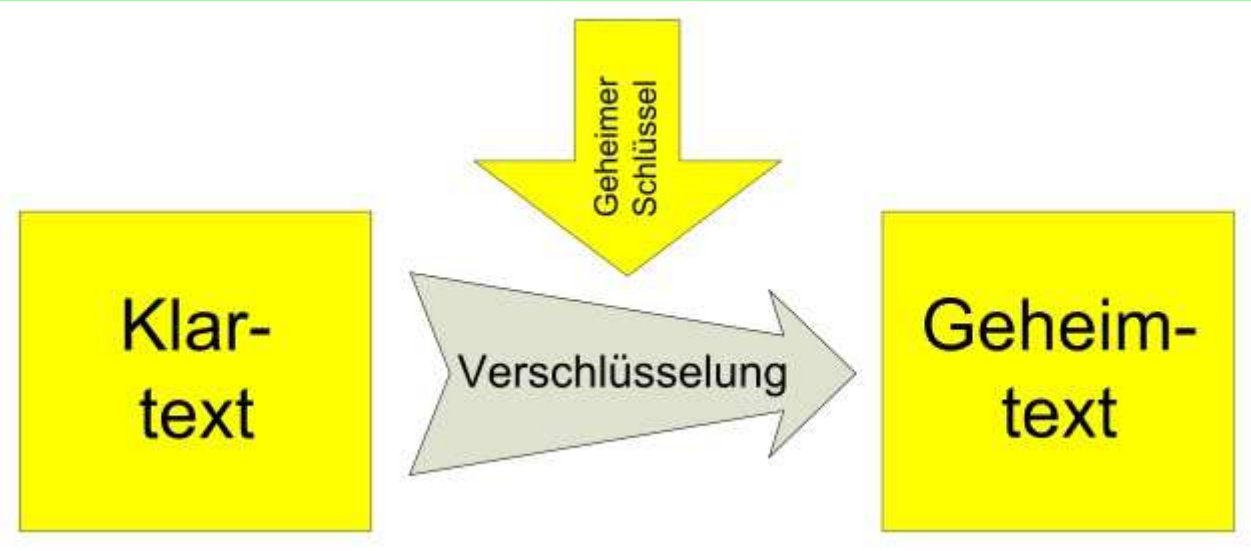
Die Entschlüsselung

Der zur Verschlüsselung umgekehrte Schritt ist die Entschlüsselung.

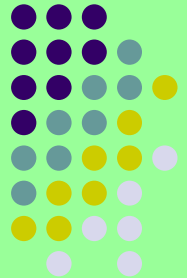
Zum Entschlüsseln wird der geheime Schlüssel benötigt, mit dessen Hilfe der befugte Empfänger den Geheimtext wieder in den Klartext zurückverwandeln kann. Geht der Schlüssel verloren, dann lässt sich der Geheimtext nicht mehr entschlüsseln. Gerät der Schlüssel in fremde Hände, dann können auch Dritte den Geheimtext lesen, das Geheimnis ist also nicht länger gewahrt.

Verschlüsselungstechniken

Übersicht:



Verschlüsselungstechniken



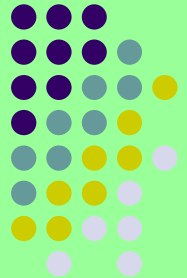
Warum muß verschlüsselt werden

Unverschlüsselte Daten sind für jedermann sichtbar und lesbar. Dies ist bei allgemeinen Informationen natürlich völlig unbedenklich, da keine privaten Interessen betroffen sind.
Dies können sein:
Berichte, Bilder u. Beschreibungen allgemeiner Themen, die die Privatsphäre nicht tangieren.
Da gibt es genügend Daten deren Inhalt unpersönlich ist.

Etwas heikler wird es schon bei e-Mails, Webseiten mit Login, Registrierungsdaten, Online-Bestellungen, Online-Banking, Anmeldungen, Formblättern, sozialen Netzwerken, usw.

Risiken:
- unverschlüsselt sind alle Daten für jedermann lesbar
- Gefahr des Mißbrauchs der persönlichen Daten bis hin zum Identitäts-Diebstahl
- Verbreitung persönlicher Daten und Gewohnheiten
- Existenzbedrohung

Verschlüsselungstechniken



Welche technischen Möglichkeiten kann man zur Verschlüsselung von Daten nutzen:

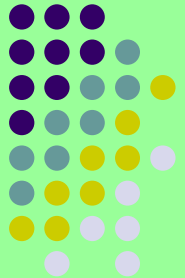
- **e-Mail**: OpenPGP, Gpg4win, S/MIME, TLS

- **Browser**: SSL, TLS (ab FF 39 ausschließlich), https-everywhere (AddOn),

- **WLAN**: WEP, WPA, WPA2

- **Dateien**: TrueCrypt, VeraCrypt, AxCrypt, Advanced File Security BitLocker

Verschlüsselungstechniken



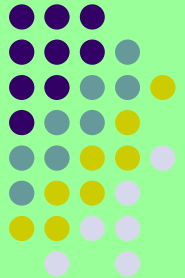
Verschlüsselung von e-Mails

- verschlüsselte Verbindung zum Server

- verschlüsselte e-Mail: Ende zu Ende Verschlüsselung

- versenden verschlüsselter Dokumente

Verschlüsselungstechniken



Verschlüsselung von Dateien

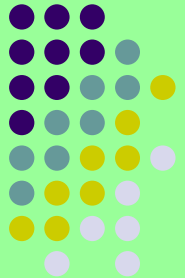
- Verschlüsselte Datei – passwortgeschützte Datei

- Verschlüsselung mit Windows Bordmitteln

- Verschlüsselung mit speziellen Programmen

- „Verschlüsselung“ durch passwortgeschützte Komprimierung

Verschlüsselungstechniken

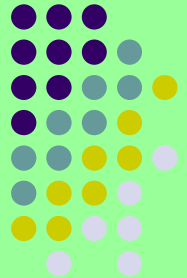


Verschlüsselung WLAN

- **WLAN im Eigenheim**:
  Mit WPA 2 verschlüsseln

- **öffentliches WLAN**:
  kein unverschlüsseltes WLAN benutzen
  nur verschlüsseltes WLAN mit Paßwort

Verschlüsselungstechniken

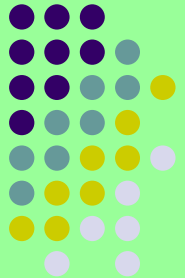


Unterschied: Verschlüsselung / Anonymisierungstechnik

- **verschlüsselte Verbindungen** können nicht bzw. nur mit großem Aufwand von Dritten eingesehen werden. Sie stellen eine Punkt-zu-Punkt Verbindung zweier Teilnehmer dar. Meist von Servern mit besuchten Webseiten oder Mailservern und sogenannten Clients, den Webseiten-Besucher bzw. den Mail-Sender/Empfänger.

- **Anonymisierungstechnik** bedeutet, daß man sozusagen anonym im Netz surft. Ein VPN-Kanal zu einem speziellen Server wie **Tor** oder **Cyberghost** schafft eine sichere Verbindung. Der Anonymisierungsserver tauscht die eigene IP-Adresse gegen eine von sich selbst aus und gibt erst dann den Verbindungswunsch weiter.

Verschlüsselungstechniken

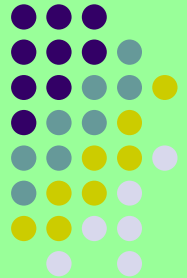


Techniken, Einstellungen und Programme:

e-Mail:

- **verschlüsselte Verbindung zum Server**
  Einstellungen im Client
  z.B. Outlook: Erweiterte Einstellung bei den E-Mail Konten
  Einige Server/Provider lassen eine unverschlüsselte Verbindung durch e-Mail Clients nicht mehr zu.
  Auch SSL-Verschlüsselung ist nicht immer möglich. Aktuell wird mit TLS verschlüsselt.
  Ältere Outlook-Versionen können keine Verbindung zu einigen Mail-Servern mehr aufnehmen.
  Tipp: Der kostenlose Mozilla e-Mail Client Thunderbird.
  https://www.mozilla.org/de/thunderbird/

Verschlüsselungstechniken

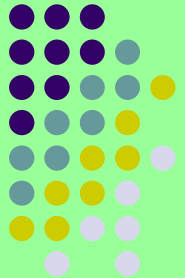


Techniken, Einstellungen und Programme:

e-Mail:

- **verschlüsselte e-Mail**
  Ende zu Ende Verschlüsselung
  nur Sender und Empfänger können die e-Mail lesen
  Nachteil: Nur möglich wenn Sender und Empfänger das gleiche Verschlüsselungsverfahren und die gleichen Schlüssel haben -> aufwendig
  Beispiel: Vom BSI (Bundesamt für Sicherheit in der Informationstechnik) empfohlen: Gpg4win, Freeware
  https://www.bsi.bund.de/DE/Themen/ProdukteTools/Gpg4win/gpg4win_node.html
  http://www.gpg4win.org/index-de.html

Verschlüsselungstechniken



Techniken, Einstellungen und Programme:

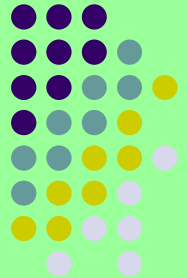
e-Mail:

- **versenden verschlüsselter Dokumente**

  Vorteil: Empfänger benötigt nur das PW zum Öffnen
  des Dateianhangs in dem die Information gesendet wird
  PW wird z.B. per SMS verschickt ->
  zusätzlicher Kommunikationsweg

  http://macpaw.com/encrypto
  (für Windows und Apple, Freeware)

Verschlüsselungstechniken



Techniken, Einstellungen und Programme:

e-Mail:

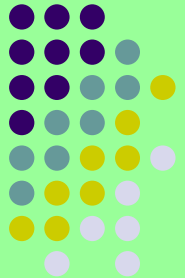
- **versenden verschlüsselter Dokumente**

  weitere Möglichkeiten:

  - PW-geschützte zip bzw rar Datei, umbenannt in *.pdf
  - schreib- / lesegeschützte Word-Datei, umbenannt in *.txt
  - Datei in Datei: in ein Word-Dokument wird eine geschützte Datei eingefügt

  usw.

Verschlüsselungstechniken



Techniken, Einstellungen und Programme:

Verschlüsselung von Dateien – Ordnern – Containern:

Dateien und Ordner -> s. e-Mail

weitere Programme:

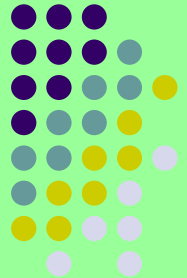
Advanced File Security, AES, 256 Bit (Shareware)
bindet sich nach Installation in das Kontextmenü des Explorers ein
kann auch auf USB-Sticks verwendet werden

http://www.wintotal.de/softwarearchiv/?id=3099

AxCrypt, AES, 128 Bit (Open Source)
bindet sich nach Installation in das Kontextmenü des Explorers ein

http://www.wintotal.de/softwarearchiv/?id=2505

Verschlüsselungstechniken



Techniken, Einstellungen und Programme:

Eingebaute Verschlüsselung einiger Programme:

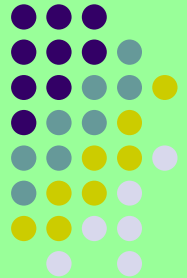
- Word
- Excel
- Adobe
- WinZip

Auch hier wird nur die Datei verschlüsselt.

Die verschlüsselte Datei kann so gespeichert werden und/oder per e-Mail versendet werden.

Wird das PW vergessen, gibt es keine Möglichkeit die verschlüsselte Datei zu öffnen.

Verschlüsselungstechniken



Techniken, Einstellungen und Programme:

Verschlüsselung von Dateien – Ordnern – Containern:

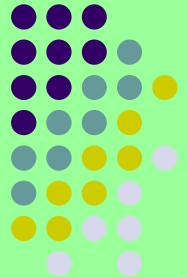
Container:

Ein beliebiger Bereich auf der Festplatte wird als verschlüsselter Datencontainer angelegt.
Freeware: **TrueCrypt** bzw. **VeraCrypt**

TrueCrypt

Wurde Ende 2014 eingestellt. Vermutlich wg. NSA, da kaum zu knacken. Es kursiert eine Version 7.2, die aber unsicher ist, vermutlich mit Backdoor.
Sicher ist aber immer noch die Version 7.1a.
http://www.chip.de/downloads/TrueCrypt_13015067.html

Verschlüsselungstechniken



Techniken, Einstellungen und Programme:

Verschlüsselung von Dateien – Ordnern – Containern:

VeraCrypt

VeraCrypt wird als „Nachfolger" von TrueCrypt gehandelt.
Aussehen und Verhalten sind TrueCrypt sehr ähnlich und es basiert auf TrueCrypt 7.1a.

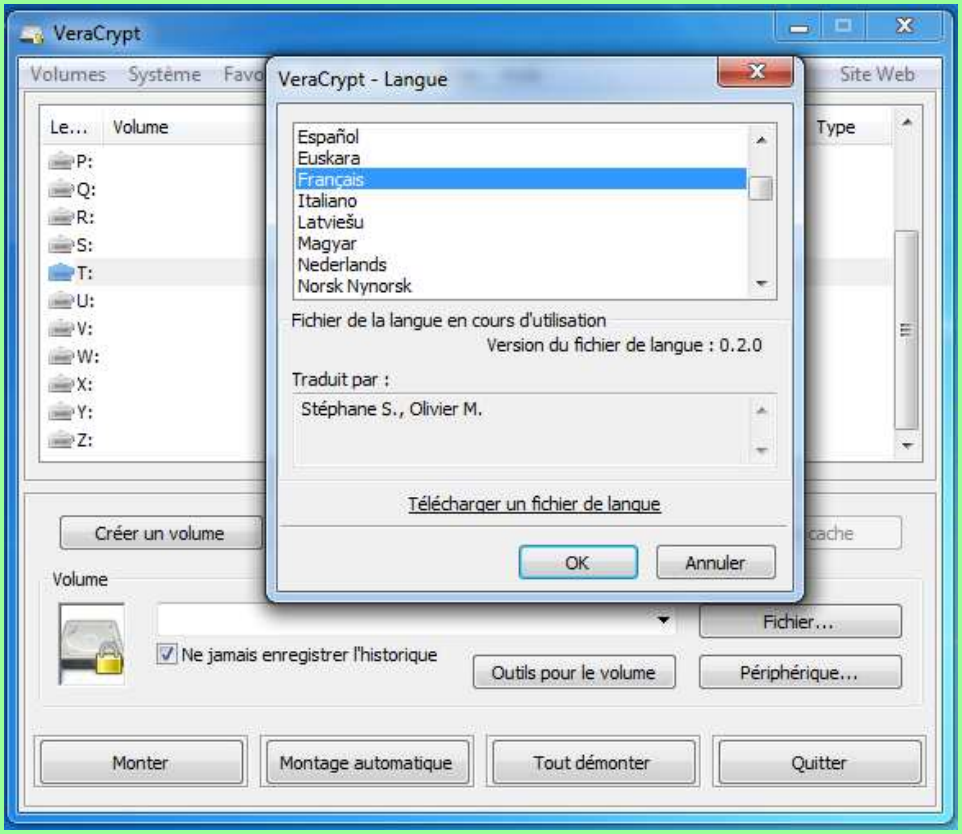
https://veracrypt.codeplex.com/

Aktuell: Version 1.17

Verschlüsselungstechniken

VeraCrypt:

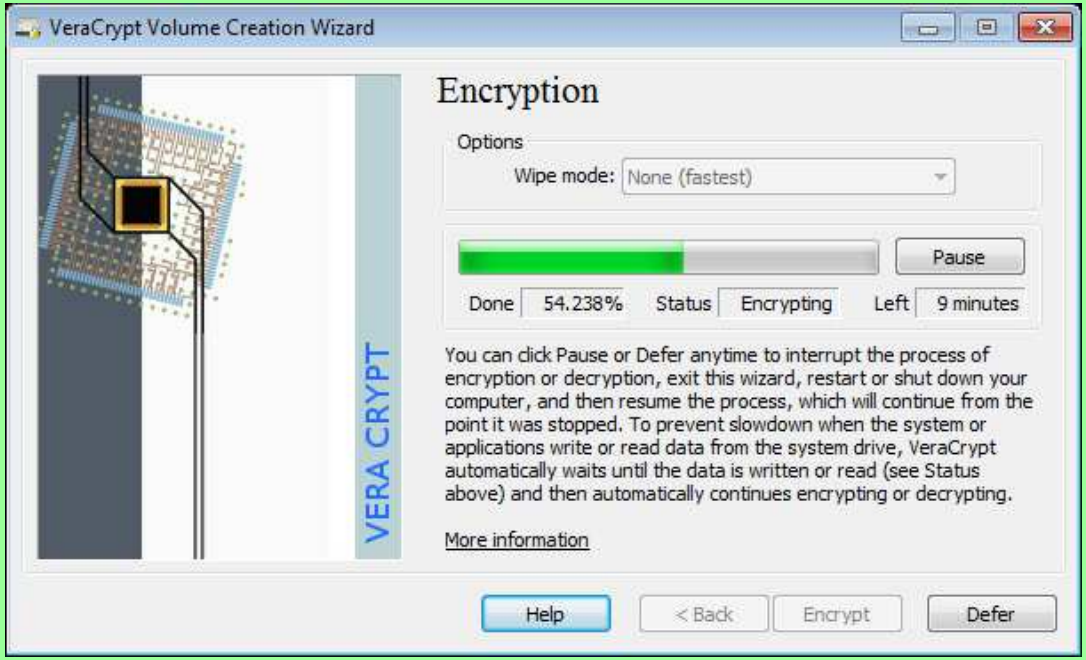
Einstellung der Sprache:



Verschlüsselungstechniken

VeraCrypt:

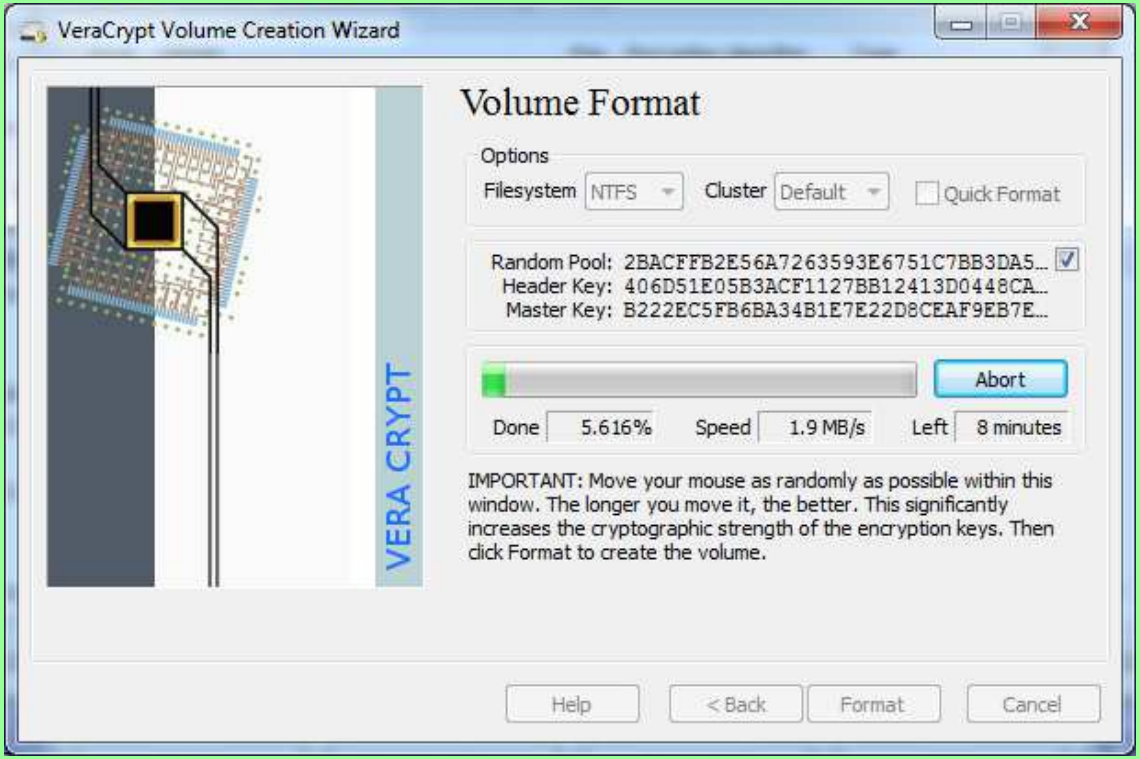
Partition verschlüsseln:



Verschlüsselungstechniken

VeraCrypt:

Container verschlüsseln:

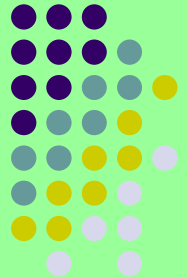


Verschlüsselungstechniken

VeraCrypt:

Verschlüsselungsoptionen:

Verschlüsselungstechniken



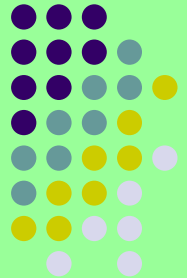
WLAN:

- **privates WLAN** im Heimbereich:

  Es sollte aus Sicherheitsgründen immer verschlüsselt sein.
  Jedoch schreibt auch der Gesetzgeber eine Verschlüsselung vor. Sonst kann man für Mißbrauch haftbar gemacht werden.

  Verschlüsselungsarten:
  WEP, WPA und WPA2, immer mit Algorithmus AES.
  Wobei WPA2 als der derzeit sicherste Standard ist.

Verschlüsselungstechniken

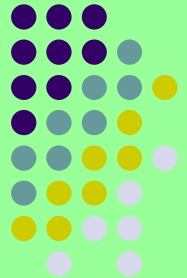


WLAN:

- **öffentliches WLAN**:

  Wenn möglich ein verschlüsseltes WLAN benutzen.
  Über ein nicht verschlüsseltes öffentliches WLAN keine vertraulichen Daten senden/empfangen.
  -> keine e-Mails, kein WhatsApp, kein Tapatalk, kein online Banking usw.
  Jede App, mit der irgendein persönlicher Login verbunden ist, nicht starten.
  Möglich ist z.B. Wetter-App, Online-Zeitung/-Zeitschrift usw.

Verschlüsselungstechniken



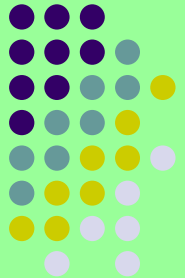
Unterschied: **Verschlüsselung** <-> **Anonymisierung**

Mit der **Verschlüsselung** wird der Zugriff auf persönliche Daten und Dokumente verwehrt.

Mit **Anonymisierung** wird die eigene IP-Adresse vor den besuchten Servern versteckt.
Daher auch „anonym".

Bekannte, sog. Proxy-Server sind **Tor** und **CyberGhost**.
Von **Tor** wird abgeraten, da schon im Fokus der NSA.
Die **CyberGhost** S.R.L. wird im rumänischen Bukarest betrieben.

Verschlüsselungstechniken

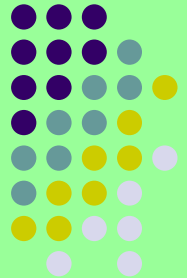


Anonymisierung:

Beiden Anonymisierungsdiensten (**Tor** bzw. **CyberGhost**) ist gemein, daß sie für die Verbindung zum Client, der die Dienste in Anspruch nimmt, einen VPN Kanal aufbauen.
Verschlüsselt mit 256 Bit und AES Protokoll.
Jedoch erhalten beide Dienste Daten von den Kunden, die auf Servern gespeichert werden.

Darüber muß man sich im Klaren sein.

Verschlüsselungstechniken



CyberGhost:

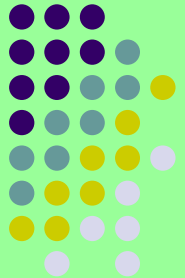
CyberGhost VPN richtet ein verschlüsseltes ***Virtual Private Network*** ein.
Der Anwender loggt sich mit seiner IP-Adresse ins VPN ein.
Er erhält daraufhin die Adresse des Anonymisierungsservers (auch Proxy-Server genannt) und diese erscheint bei den vom Anwender besuchten Webseiten als Adressat.

Die Privatsphäre wird allerdings nur dann gesichert, wenn auf dem proprietären Windows-Client (auf dem Anonymisierungsserver) die Übermittlung identifizierender Daten gesperrt wird.
Das sind Betriebssystem- und Browser-Kennungen.
Entfernung von Social-Plug-ins wie Facebook-Like-Buttons.
Blockade von Tracking- und Analyse-Seiten.

Der Anbieter betreibt ein eigenes DNS. Regionale Zensoren sollen auf diese Server des Diensteanbieters nicht zugreifen können.

https://www.cyberghostvpn.com/de_de/index/indexa?utm_expid=85864364-16.rpyKYws5QEqQ9-K_VVF5cQ.1

Verschlüsselungstechniken



Bitte stellen Sie jetzt Ihre Fragen