Verschlüsselung und IT-Sicherheit

Rechtsanwalt Dr. Alexander Koch

Programm

- Einführung
- E-Mail
  - Metadaten
  - Inhalte
  - Mobile Geräte
- Datenverschlüsselung
  - Container
  - Vollverschlüsselung von Laptops und PCs
  - Mobile Geräte
- (Sichere Internetnutzung)
- Datensicherheit (Backups)

Warum verschlüsseln?

- Schutz vor Wirtschaftsspionage/Geheimdiensten.
- Schutz von Geschäftsgeheimnissen gegenüber staatlichen Stellen.
  - Es sind schon Kanzleiräume durchsucht worden, um ***entlastendes*** Material in ***Beleidigungs***verfahren ***zugunsten*** des beschuldigten Anwalts zu finden.
- Schutz vor neugierigen Familienmitgliedern/ Kollegen.
- Schutz bei Diebstahl/Verlust von Laptops/ Smartphones.

Im Alltag gehen die größten Gefahren nicht von mächtigen Geheimdiensten aus …

… praktisch relevanter ist der verlorene USB-Stick oder Laptop mit Mandantendaten

bzw. die E-Mail, die an den falschen Empfänger gesendet wurde!

AES

- Advanced Encryption Standard.
- Wurde in Belgien entwickelt.
- Sehr einfach (500 Zeilen Programmcode).
- Sehr gut erforscht.
- AES-192 und AES-256 sind in den USA für Dokumente mit der höchsten Geheimhaltungsstufe „TOP SECRET“ zugelassen.
- 2^{256}=115.792.089.237.316.195.423.570.985.008. 687.907.853.269.984.665.640.564.039.457.584. 007.913.129.639.936 (115 Dodezilliarden)
- Die Sicherheit hängt allerdings von der konkreten Umsetzung im Programm ab!

Passwörter

- Schlechte Passwörter:
  - Passwort, qwertz, 12345, Harry Potter.
  - Jedes Wort, das in ***irgendeinem*** Wörterbuch stehen könnte.
- Gute Passwörter:
  - %34Pb+m8M*x0<h, !Ui9x"X?Is:+PX
  - Ega1eT,l&gmP7e.Dbm71M0mM.

Merkbare und sichere Passwörter

Es gibt allerdings einen einfachen Trick, lange und gut merkbare Passwörter zu erstellen. Dazu bildet man zunächst einen Merksatz oder mehrere Merksätze.

Merkbare und sichere Passwörter

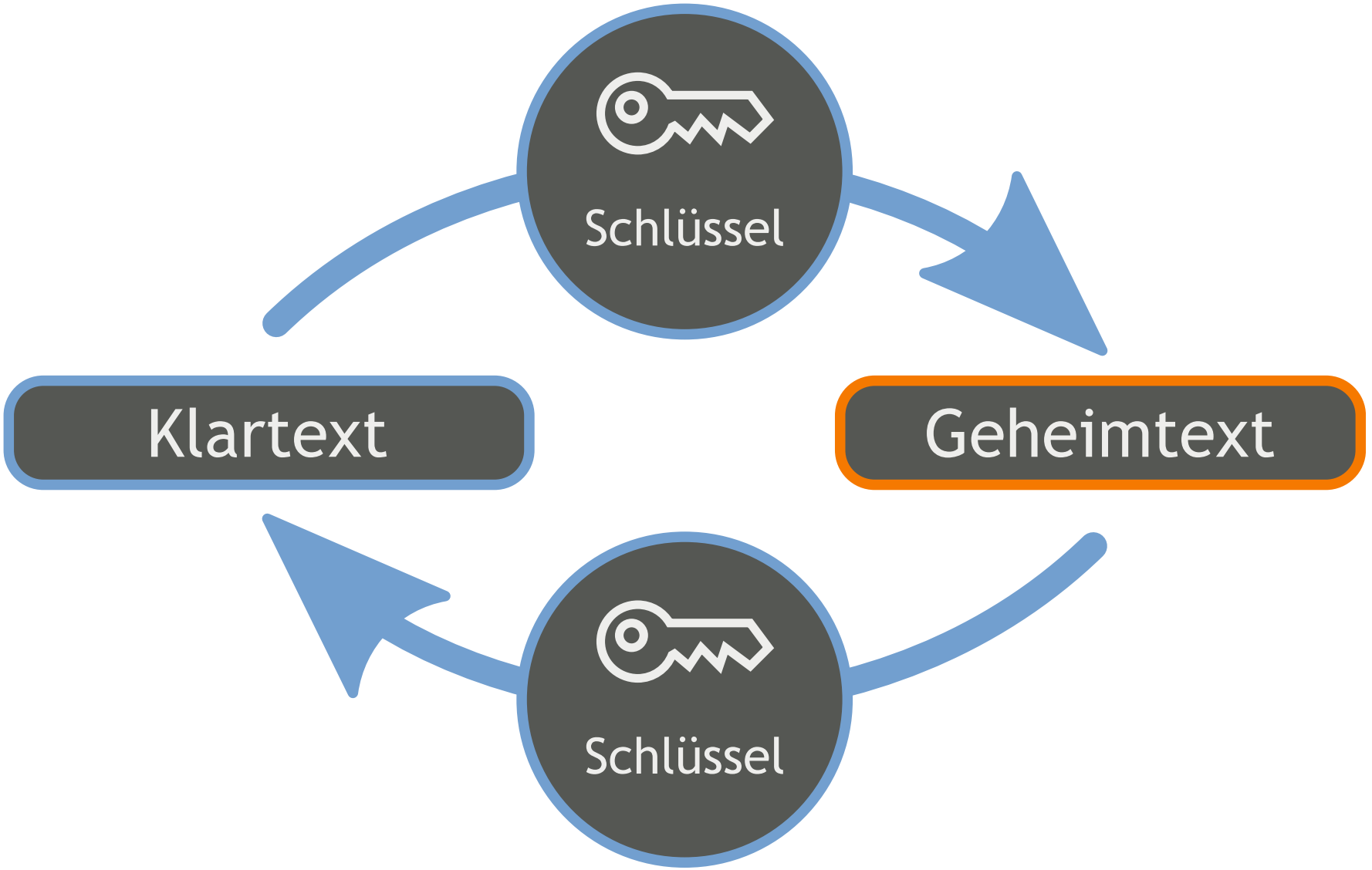
E**s **g**ibt **a**llerdings **e**inen **e**infachen **T**rick**,** **l**ange **u**nd **g**ut **m**erkbare **P**asswörter **z**u **e**rstellen**.** **D**azu **b**ildet **m**an **z**unächst **e**inen **M**erksatz **o**der **m**ehrere **M**erksätze**.

EgaeeT,lugmPze.DbmzeMomM.

E**s **g**ibt **a**llerdings **einen** **e**infachen **T**rick**,** **l**ange **und** **g**ut **m**erkbare **P**asswörter **z**u **e**rstellen**.** **D**azu **b**ildet **m**an **z**unächst **einen** **M**erksatz **o**der **m**ehrere **M**erksätze**.

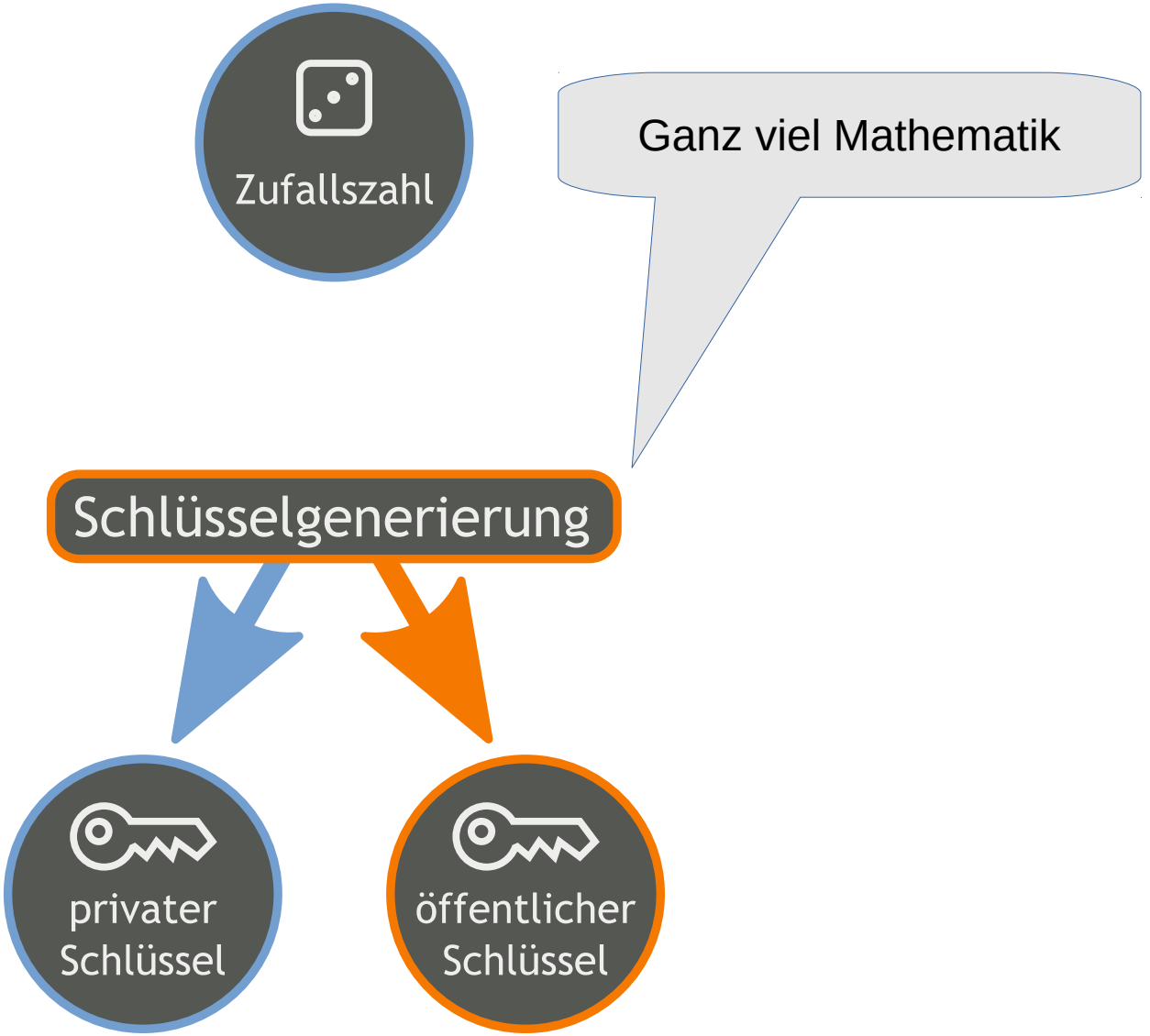
Ega**1**eT,l**&**gmP**7**e.Dbm**71**M**0**mM.

Symmetrische Verschlüsselung



https://de.wikipedia.org/wiki/Datei:Orange_blue_symmetric_cryptography_de.svg

Asymmetrische Verschlüsselung

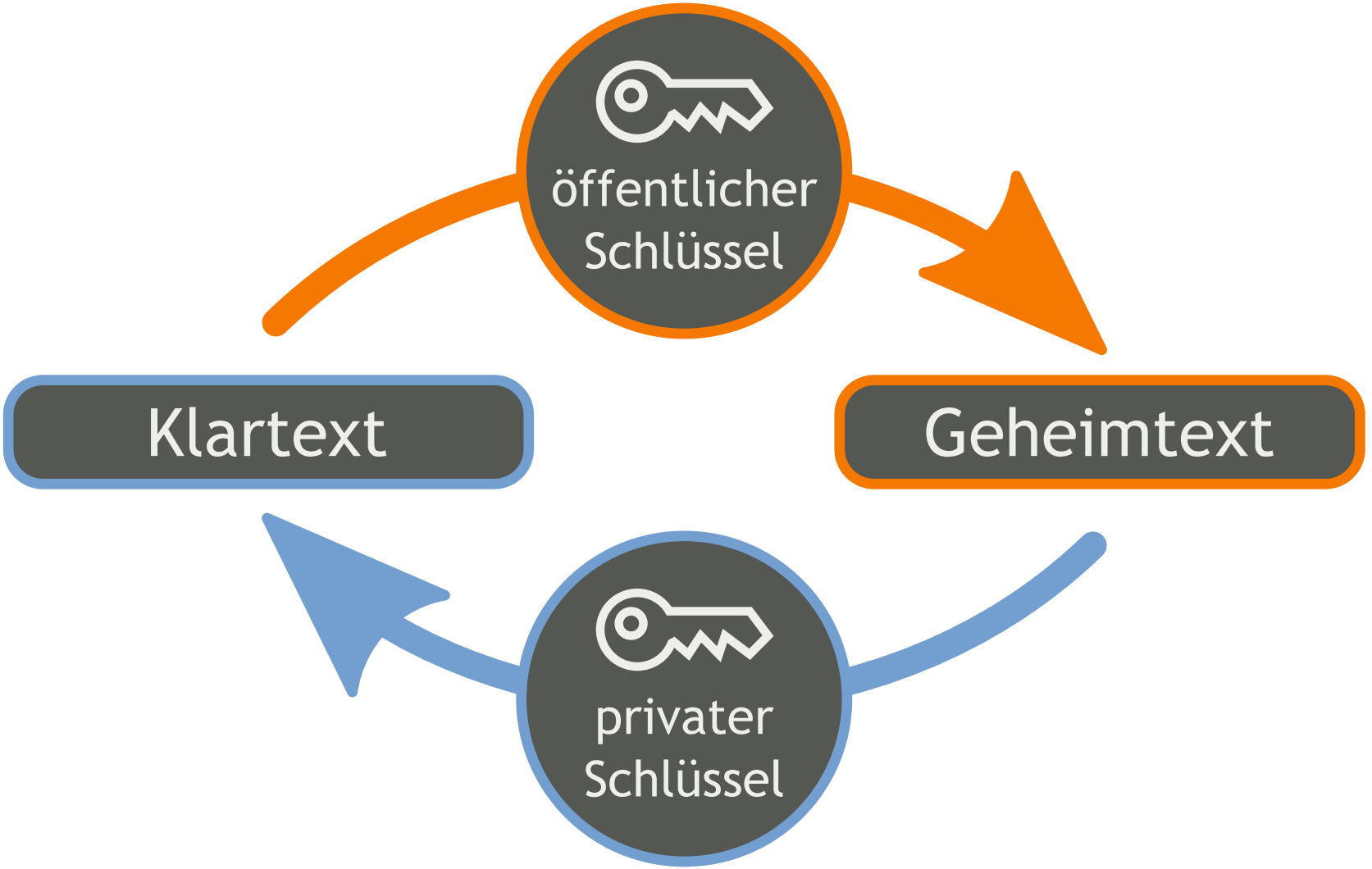


https://de.wikipedia.org/wiki/Datei:Orange_blue_public_private_keygeneration_de.svg

Mathematik

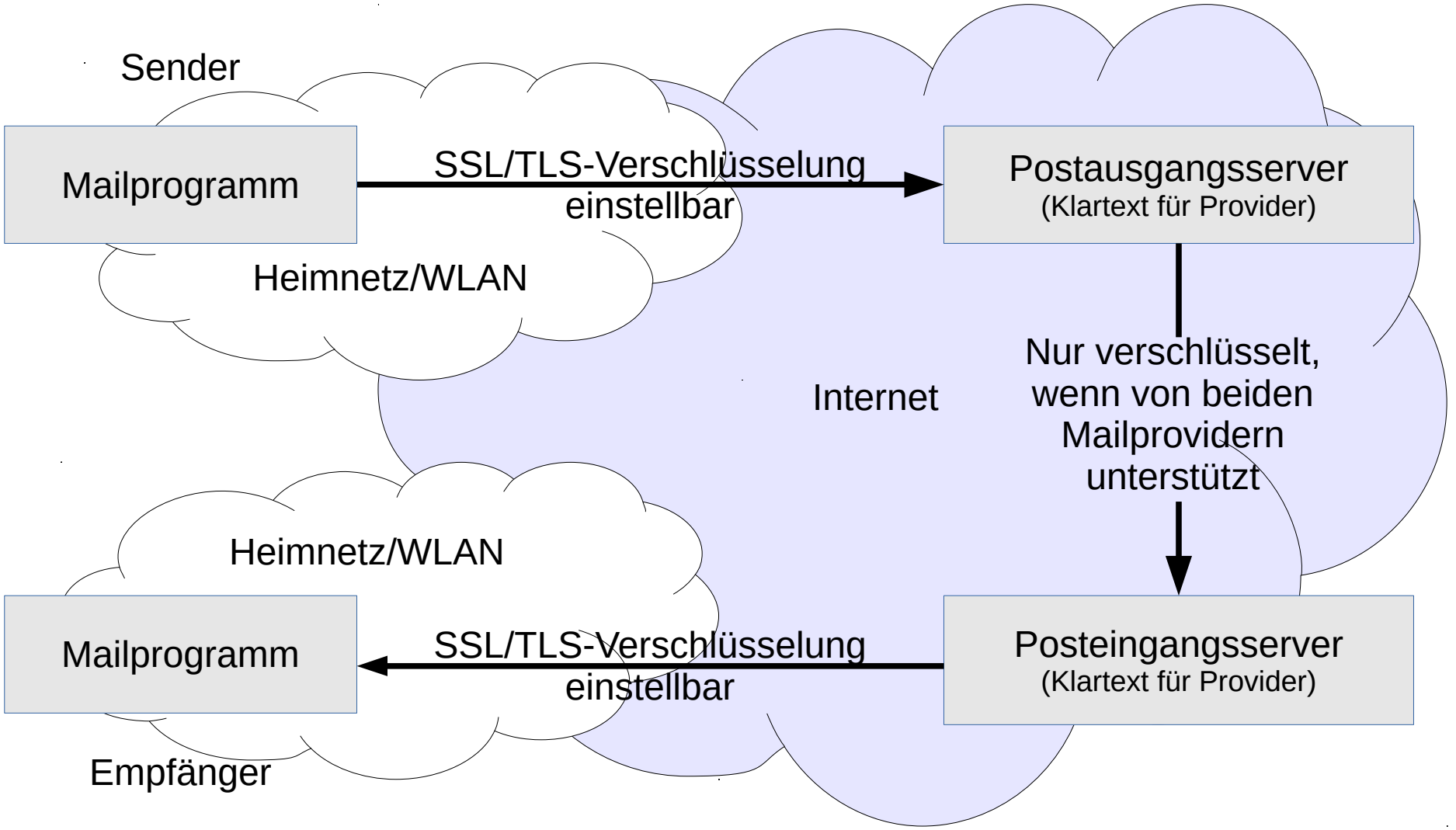
- Was ist 76.333 x 80.149?
  - 6.118.013.617.
  - Multiplikation ist sogar per Hand ohne weiteres möglich.
- Was sind die Primfaktoren von 4.634.629.529?
  - 58.417 und 79.337.
  - Primfaktorenzerlegung ist äußerst aufwändig!

Asymmetrische Verschlüsselung



https://de.wikipedia.org/wiki/Datei:Orange_blue_public_key_cryptography_de.svg

E-Mail


Sender
Mailprogramm
SSL/TLS-Verschlüsselung einstellbar
Postausgangsserver
(Klartext für Provider)
Heimnetz/WLAN
Internet
Nur verschlüsselt, wenn von beiden Mailprovidern unterstützt
Heimnetz/WLAN
Mailprogramm
SSL/TLS-Verschlüsselung einstellbar
Posteingangsserver
(Klartext für Provider)
Empfänger

Metadaten

- Es kann nur der Weg zum und vom eigenen E-Mailserver kontrolliert werden.
- Es muss davon ausgegangen werden, dass (staatliche) Angreifer Zugriff auf die Metadaten (Sender, Empfänger, Betreff) nehmen können.
- **IMMER, IMMER, IMMER** SSL/TLS verwenden …
- … sonst kann jeder im gleichen Netz mitlesen!

PGP/GnuPG

- PGP wurde Anfang der 1990er-Jahre von Phil Zimmermann entwickelt.
- GnuPG ist eine quelloffene Umsetzung von PGP.
- PGP/GnuPG arbeiten mit öffentlichen und privaten Schlüsseln.
- Umsetzungen sind für alle Betriebssysteme (einschließlich Smartphones) verfügbar.

S/MIME

- System zum Verschlüsseln und Signieren von E-Mails.
- Nichtkompatibel zu PGP/GnuPG.
- Zentrale Verwaltung der Zertifikate.
- Zertifikat muss (sinnvollerweise) von einer anerkannten Zertifizierungsstelle erzeugt werden – z.B. <startssl.com>.
- S/MIME funktioniert meist ohne weitere Konfiguration!

ZIP

- … wenn PGP/GnuPG oder S/MIME zu kompliziert sind …
- Es können nur Anhänge verschlüsselt werden.
- Es muss zunächst ein Passwort sicher ausgetauscht werden.
- Mac und Windows können von Hause aus nicht mit (sicher) verschlüsselten ZIP-Dateien umgehen.
- Darauf achten, dass das ZIP-Programm die AES-256-Verschlüsselung beherrscht.

Was nun?

	PGP/GnuPG	S/MIME	ZIP
Verbreitung	--	-	++
Einrichtung	--	--	+ (AES wird nicht von Hause aus unterstützt)
Nutzung	O	++	+
E-Mail-Integration	++ (Outlook -)	++	--
Schlüsseltausch	+	++	--
Sicherheit	++	++	++ (AES) / --

… auch die schlechteste Verschlüsselung ist immer noch besser als überhaupt keine Verschlüsselung!

iOS (iPhone/iPad)

- S/MIME wird von Hause aus unterstützt.
  - Zertifikat muss (regelmäßig) per E-Mail auf das Gerät geschickt werden.
  - Zertifikat muss in den E-Mailaccount eingebunden werden.
  - Erhält man signierte Nachrichten, muss das Zertifikat importiert werden (Klick auf den Namen).
- PGP/GnuPG
  - Mittels iPGMail (erhältlich im Appstore) kann auch PGP/GnuPG genutzt werden.

Android

- Android kann von Hause aus nicht (sinnvoll) mit PGP/GnuPG oder S/MIME umgehen.
- R2Mail2 (erhältlich u.a. über den Google Play Store) ist ein alternatives E-Mailprogramm, welches mit PGP/GnuPG und S/MIME umgehen kann.
  - Die Schlüssel sollten über USB auf das Gerät übertragen werden.

Datenverschlüsselung

- Alle Daten, die man verlieren kann, sollten verschlüsselt sein!
- Also: Keine ungesicherten Daten auf Laptops oder USB-Sticks transportieren!

Verschlüsselte Container

- Mit TrueCrypt lassen sich verschlüsselte Container erstellen, die sich wie externe Festplatten/USB-Sticks nutzen lassen.
  - Entwicklung ist eingestellt worden.
  - Die (vor-)letzte Version gilt aber als sicher.
- Solche Container können auch auf USB-Sticks gespeichert werden.
- (Es ist sogar ein Abgleich über die DropBox möglich …)

Vollverschlüsselung

- MacOS: FileVault.
  - Über die Systemeinstellungen aktivieren und vergessen. (Arbeitet bei mir seit Jahren ohne Probleme!)
- Windows:
  - BitLocker: Wenn die eigene Windowsversion und der PC kompatibel sind …
  - TrueCrypt: Geht immer ...

Mobile Geräte

- iOS (iPhone/iPad):
  - Die Geräte sind von Hause aus vollverschlüsselt.
  - Einfacher Code und „Code anfordern“: „Sofort“ oder Langes PWD und „Code anfordern“: „Nach 1 Stunde“.
- Android:
  - Vollverschlüsselung muss manuell eingerichtet werden.
  - Es muss jedes Mal zum Entsperren das (lange) PWD eingegeben werden.
- Funktionen zur Fernortung und zum Fernlöschen aktivieren!

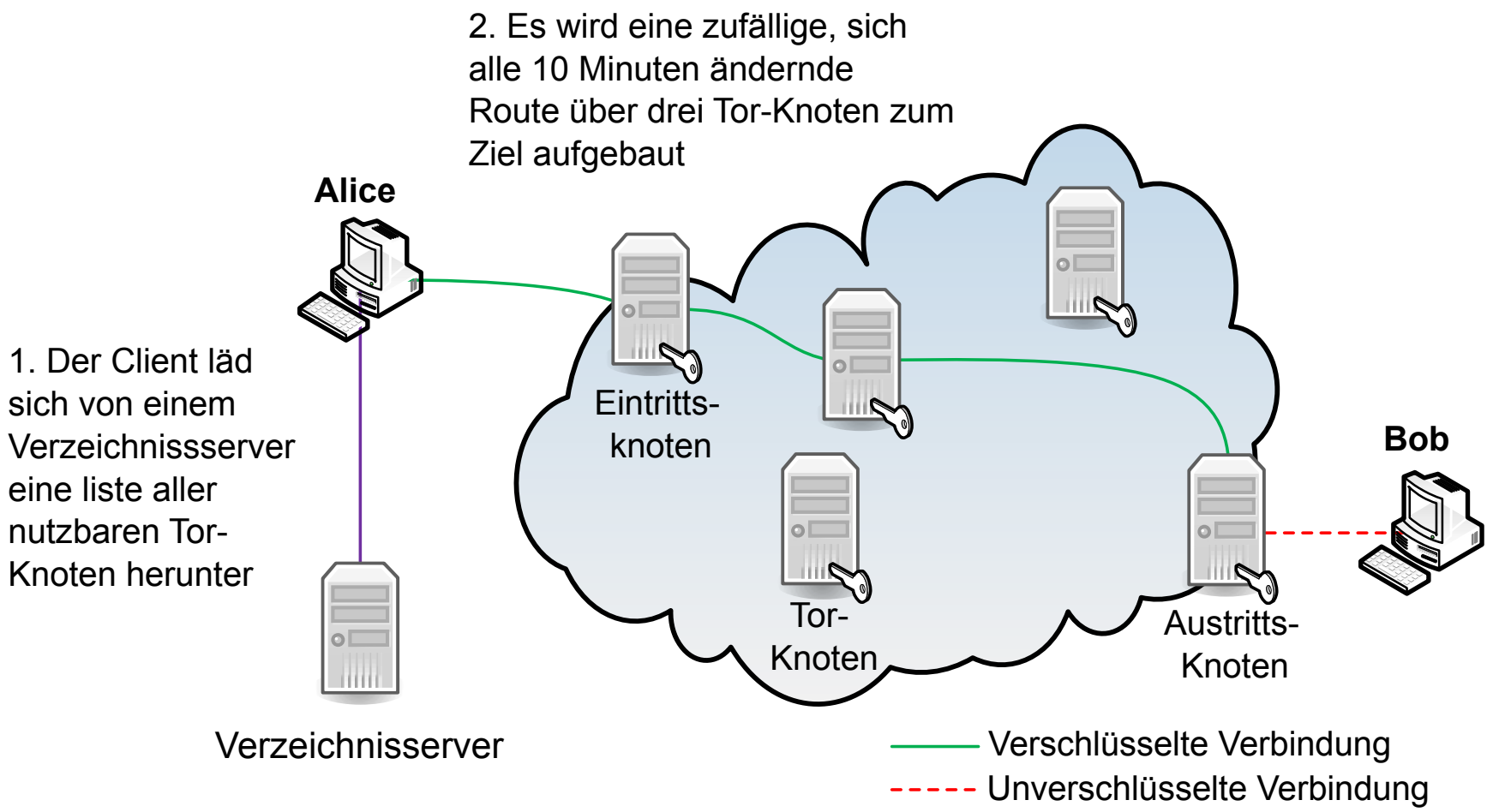
Sichere Wege ins Netz

- HTTPS:
  - Die Verbindung zum Server ist verschlüsselt.
  - Ein Angreifer kann nur sehen, mit welcher IP-Adresse man kommuniziert.
  - Der Serverbetreiber kann die eigene IP sehen.
  - Immer nutzen, wenn irgend möglich!
- VPN:
  - Die Verbindung zum VPN-Server ist verschlüsselt.
  - Ein Angreifer kann nur sehen, dass man mit einem VPN-Server kommuniziert.
  - Der Serverbetreiber sieht die IP des VPN-Servers.
  - In öffentlichen WLANs (Café, Flughafen, Hotel) nutzen!

Anonymität

- … im Internet ist (eher) eine Illusion …
- Praktisch jeder Browser lässt sich eindeutig identifizieren.
  - Je mehr man unternimmt, um den Browser abzusichern, desto einmaliger wird er …
- Dennoch: Aktive Inhalte und Cookies sollten nur fallweise zugelassen werden!

Tor-Netzwerk



https://de.wikipedia.org/w/index.php?title=Datei:TOR_Arbeitsweise.svg&filetimestamp=20140405003315&

Datensicherheit

- Festplatten sind Verschleißteile!
- Wichtige Daten möglichst auf einem RAID-System sichern.
  - Daten werden parallel auf zwei (oder mehr) Festplatten gespeichert.
  - Fällt eine Festplatte aus, kann diese (im Betrieb) ohne Datenverlust gegen eine neue ersetzt werden.
- RAID-Systeme ersetzen kein Backup!

Backup

- Backup sollte automatisiert erfolgen.
- Generationenbackup erzeugen:
  - Stündlich, täglich, wöchentlich, monatlich.
- Backup sollte an einem anderen Ort aufbewahrt werden …
- … oder besser gleich über das Internet dort erzeugt werden.
- Ein Backup ist gut. Zwei Backups sind besser!

… vielen Dank für die Aufmerksamkeit!

Kontakt:
Dr. Alexander Koch
Koch & Neumann
Rheinweg 67
53129 Bonn
Tel: 0228/8 50 86 63
E-Mail: ak@KochNeumann.de
WWW: http://KochNeumann.de

http://kochneumann.de/index.php5?direktmodus=vortrag-verschluesselung-it-sicherheit