CryptoParty KHG

15.06.2016

Lukas Braun, Florian Snow, Michael Groh, Christopher Schirner

Inhaltsverzeichnis

- Hackerspace Bamberg
- Gegründet 23.10.2011
- 53 Mitglieder
- https://www.hackerspace-bamberg.de
- Dienstag ab 19 Uhr

Warum überhaupt verschlüsseln?

- Schutz der Privatsphäre
- “Ich habe doch nichts zu verbergen!”
- Vielleicht gibt es aber doch private Dinge

Was muss Verschlüsselung leisten?

- Nachricht muss geheim bleiben
- Nachrichtenaustausch mit dem richtigen Kommunikationspartner

Wie funktioniert Verschlüsselung?

- Historische Symmetrische Verfahren
  - z.B. Cäsar-Chiffre oder Vertauschung von Zeichen
- Moderne Symmetrische Verfahren
  - Komplexere Verfahren, aber alle mit nur einem Schlüssel zum Ver- und Entschlüsseln
  - Verifikation des Kommunikationspartners begrenzt möglich
  - Problem: Schlüsselaustausch und Schlüsselanzahl

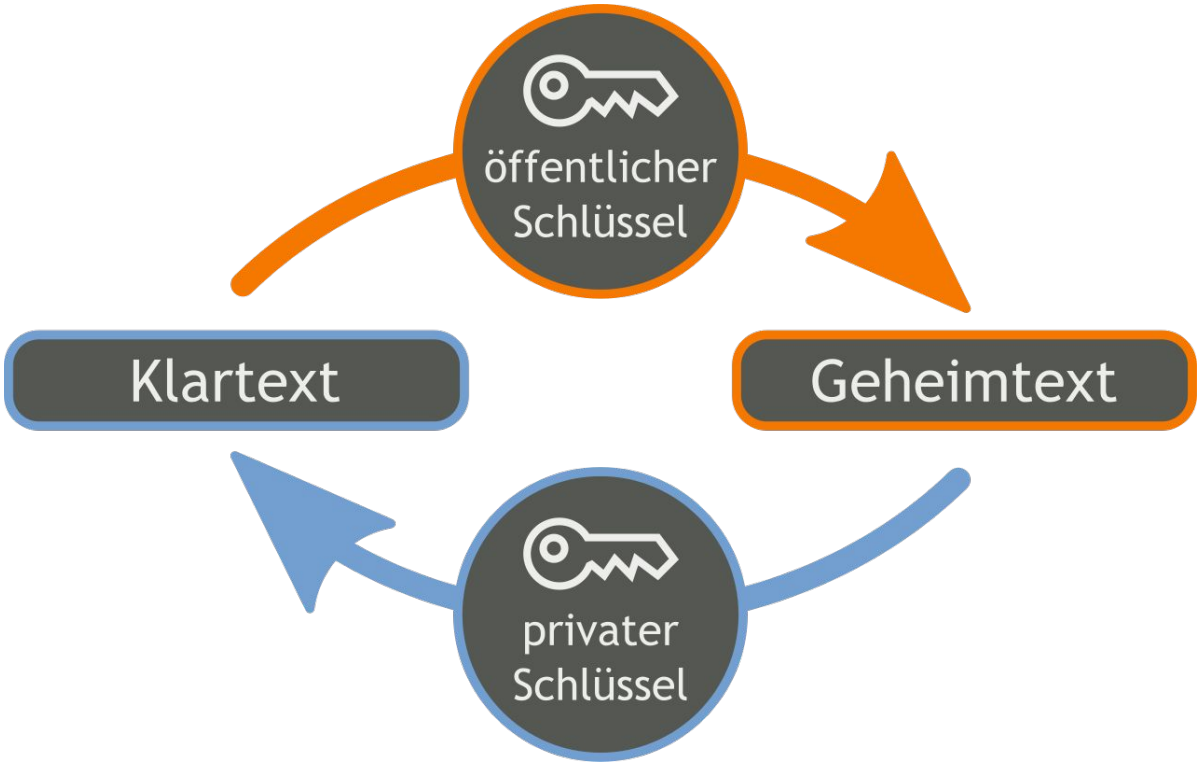
Wie funktioniert Verschlüsselung?

- Asymmetrische Verfahren
  - Verfahren mit geheimem und öffentlichem Schlüssel
  - Jeder Schlüssel kann den Geheimtext entschlüsseln, der mit dem jeweils anderen Schlüssel erstellt wurde (Vorhängeschloss)
  - löst das Problem des Schlüsseltauschs und der Schlüsselanzahl
  - Prinzip: einseitig schwierige mathematische Verfahren (Falltüralgorithmus)

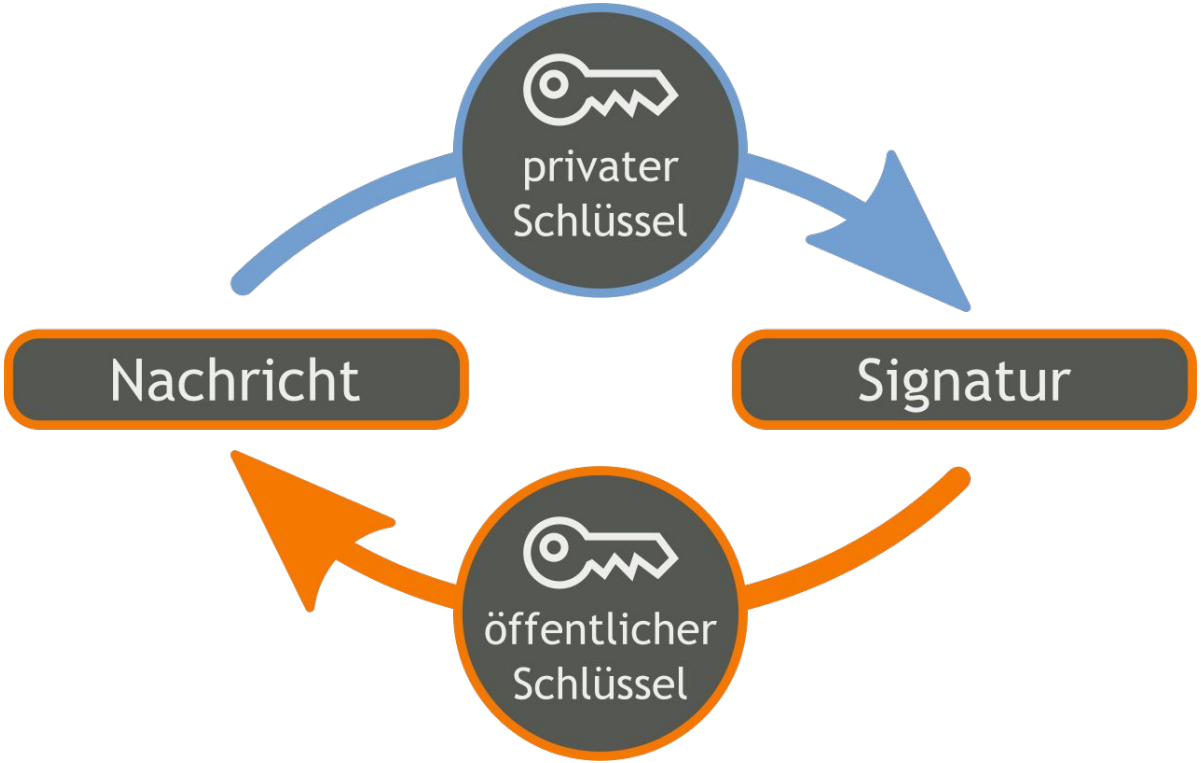
OpenPGP/GnuPG

- Asymmetrisches Verschlüsselungsverfahren
- Hauptsächlich für Mailverschlüsselung verwendet
- Als Erweiterung für Mailclients und Browser verfügbar
- Jeder besitzt ein Schlüsselpaar (öffentlicher und geheimer Schlüssel)
- geheimer Schlüssel nur für sich selbst bestimmt
- öffentlicher Schlüssel kann und soll beliebig geteilt werden
- Verifizierung mittels Fingerprint/Web of Trust

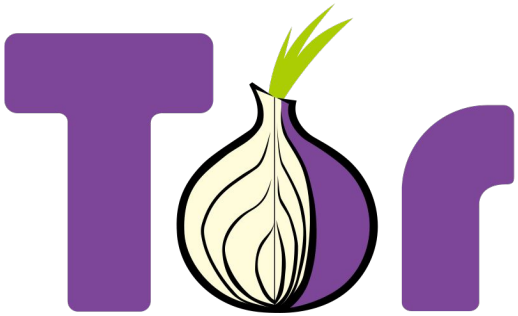
OpenPGP/GnuPG



OpenPGP/GnuPG

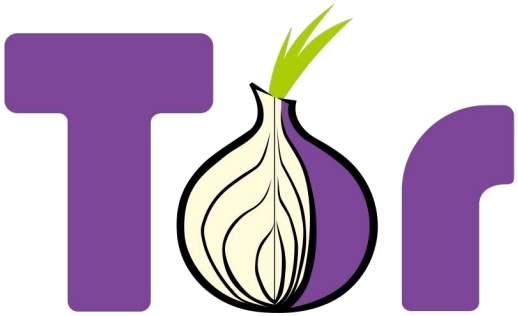


Anonymes Surfen



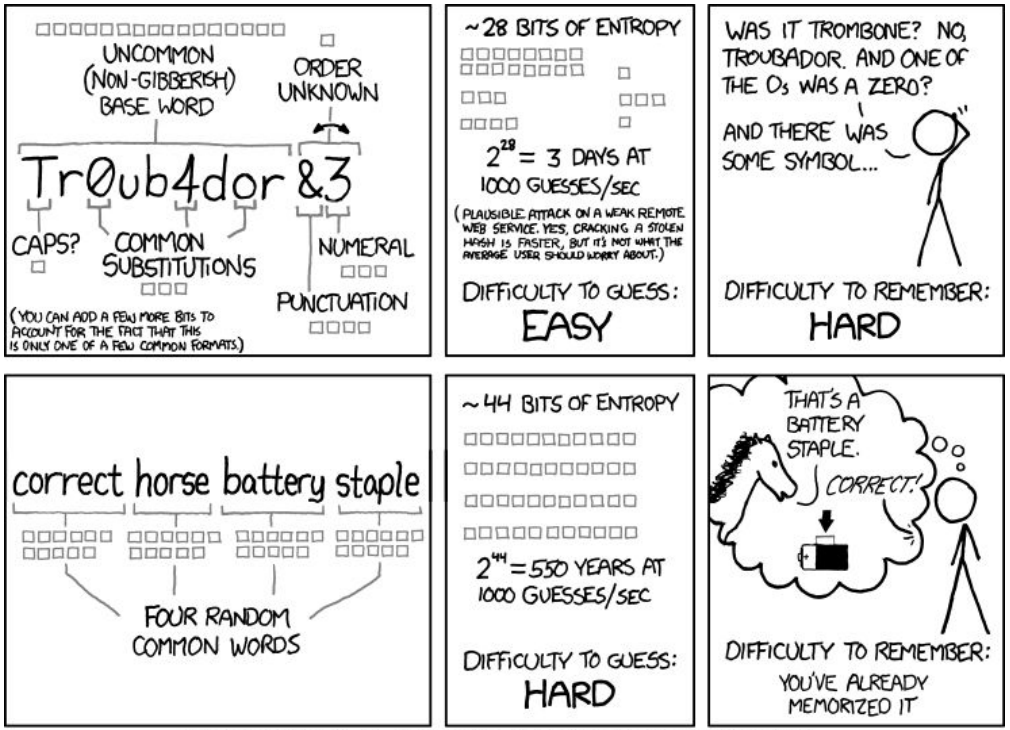
- Beim normalen Surfen kann man verfolgt werden
  - IP-Adresse
  - Cookies
  - Fingerprinting

Anonymes Surfen



- TOR - The Onion Router
- Aufgebaut wie eine Zwiebel
- Baut darauf auf, dass man keinem einzelnen Knotenbetreiber trauen muss
- Daten werden über zufällige Routen geleitet
- Anonymisiert nur die IP-Adresse

Passwörter


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Passwörter

- Mögliche Methoden
  - “Zufällige” Kombination von Wörtern: MargaretThatcherIs100%Sexy
  - Anfangsbuchstaben eines Satzes: “Ich mag keine Gummibärchen, weil die in den letzten Jahren immer so zwischen 2 Zähnen kleben bleiben.” => ImkG,wdidlJisz2Zkb.
  - Vorteil: einfach zu merken
  - Problem: unsere Ideen sind nicht richtig zufällig
  - Lösung: Diceware

Praxisteil

Einrichten von GnuPG und TOR

E-Mail-Verschlüsselung mit GnuPG:

- Windows: GPG4Win installieren: https://www.gpg4win.de
- Mac OS X: GPGTools installieren: https://www.gpgtools.org
- GNU/Linux: gnupg aus Paketquellen installieren

Mailprogramm einrichten:

- Thunderbird: https://www.enigmail.net
- Outlook: Plugin in GPG4Win enthalten

Schlüssel erzeugen: 4096 Bit lang und Ablaufdatum setzen (verlängerbar)

Optional: Schlüssel auf Keyserver veröffentlichen