



"[L]ike a Tupperware party for learning crypto"
- Cory Doctorow

Anton Weber
anon@anonweb.de

PGP
8A82 F029 F576 1B6B A467
6A30 E06D 5FB7 D614 A20F

Über die Veranstaltung

- Weltweite Bewegung
- Chaos Computer Club München e.V.
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung



Vorwort

- Organisiert von Freiwilligen
- 100% Sicherheit gibt es nicht
- Digitaler Raum verändert sich ständig

Vor wem schützen?

- Kleinkriminelle
- Internet-Konzerne
- Massenüberwachung
- "Datenpannen"

Welche Gefahren bleiben?

- Gezielte Angriffe
- Geheimdienste
- ...

Grundlagen

Vertrauen

- Wem vertraut ihr im analogen Leben?
 - Familie
 - Nachbarn
 - Bank

Vertrauen

- Selbe Frage wichtig im digitalen Leben
 - Absender einer E-Mail
 - E-Mail App
 - Hersteller des Betriebssystems
 - Hersteller des Handys

Wem sollte man vertrauen?

- Immer eine Abwägung
- Fragen können helfen:
 - Motivation (Geschäftsmodell)
 - Was vertraue ich an (welche Daten)

Wert der Daten

- Angriff lohnt sich nur, wenn Wert > Kosten
- ABER: Wert wird oft unterschätzt
- Urlaubsfotos, wenn sie plötzlich verschlüsselt sind
- Telefonbuch gibt viel preis



Metadaten

- E-Mail: Absender, Empfänger, Betreff (!)
- Telefon: Einzelverbindungs nachweis
- Foto: Aufnahme datum, -ort, Kameramodell
- Handy: Funkzelle

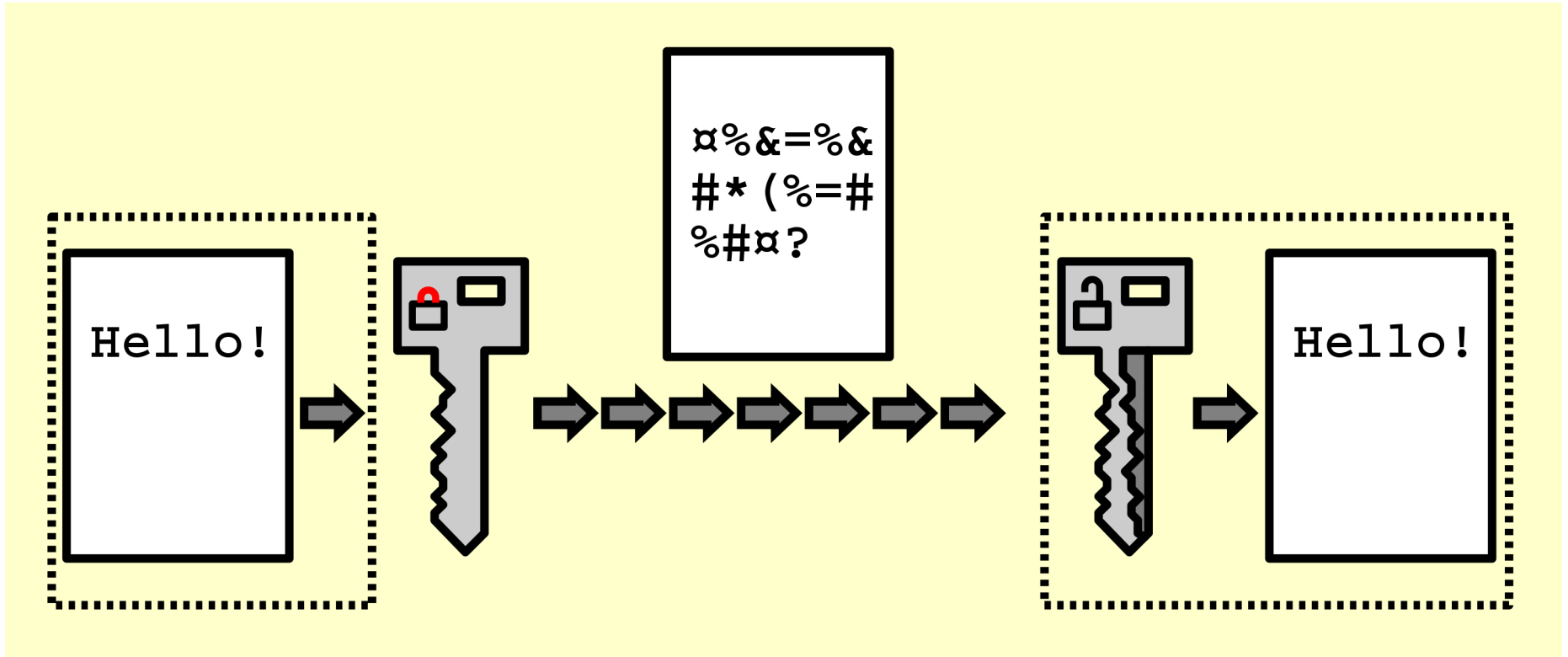
Metadaten

- Besonders in größeren Mengen problematisch
 - Funkzelle → Bewegungsprofil
 - Zeit, Dauer des Gesprächs → Art von Beziehung

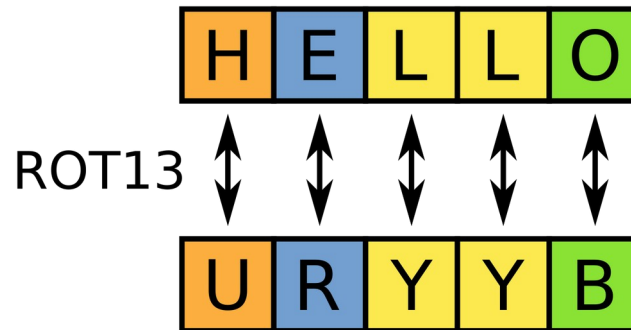
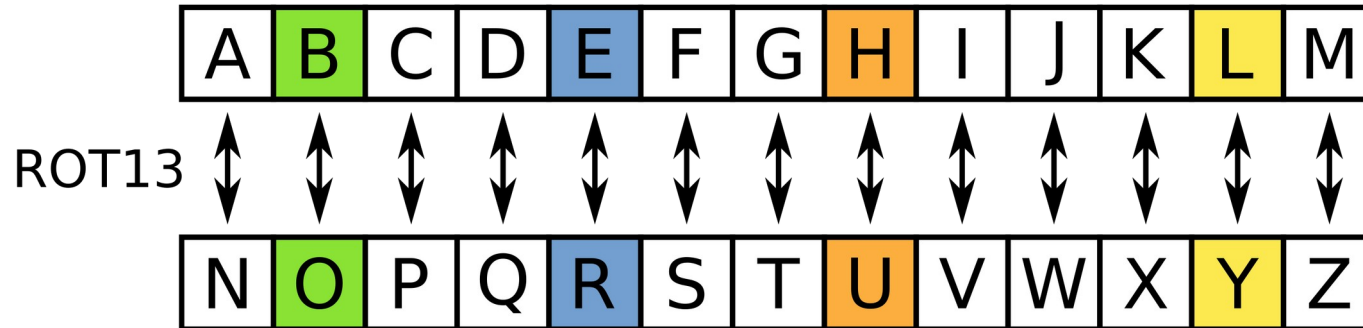
Metadaten

- Können nicht verschlüsselt werden
- Können nur schwer verschleiert werden
- ABER können evtl. vermieden werden

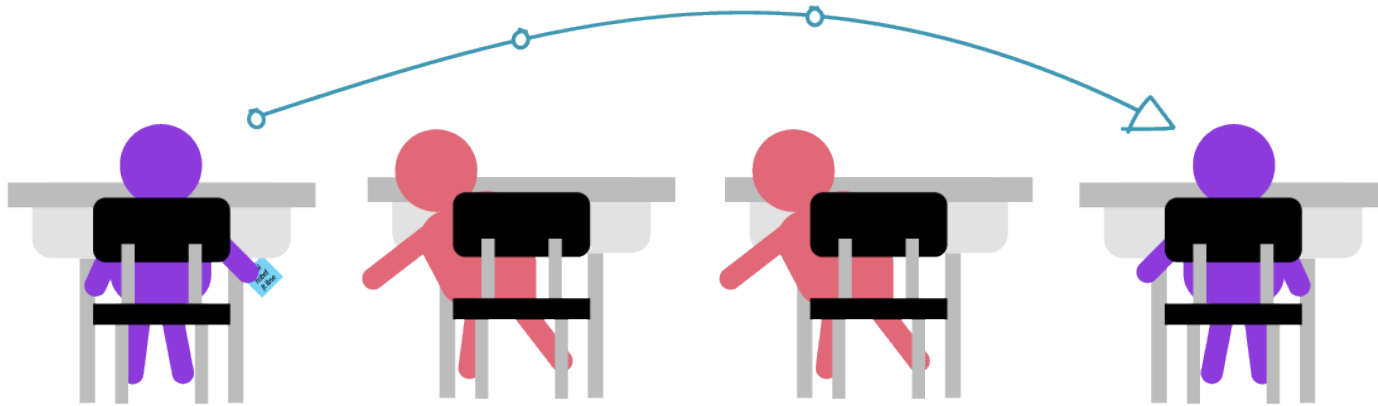
Verschlüsselung



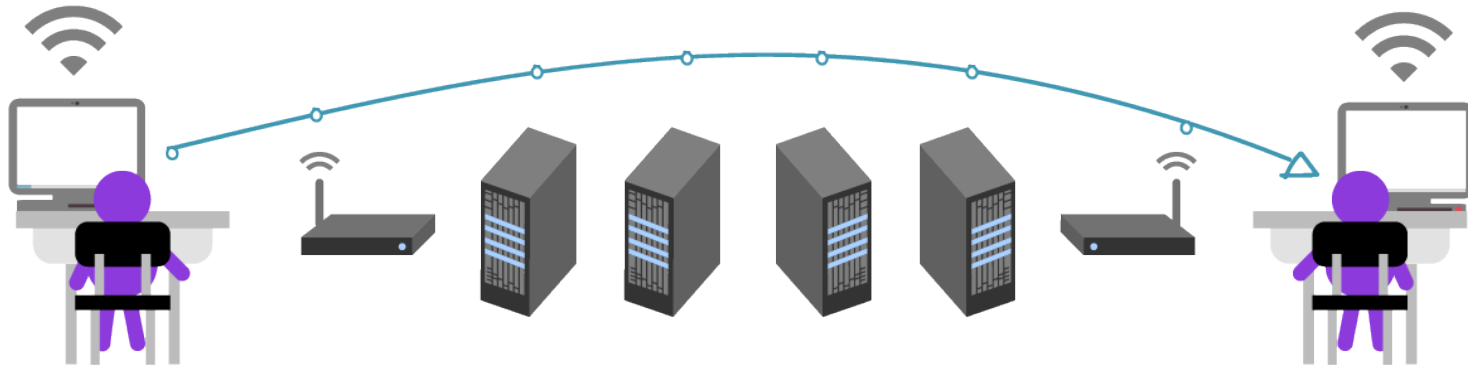
Verschlüsselung



Verschlüsselung



Verschlüsselung



Asymmetrische Kryptographie



public key



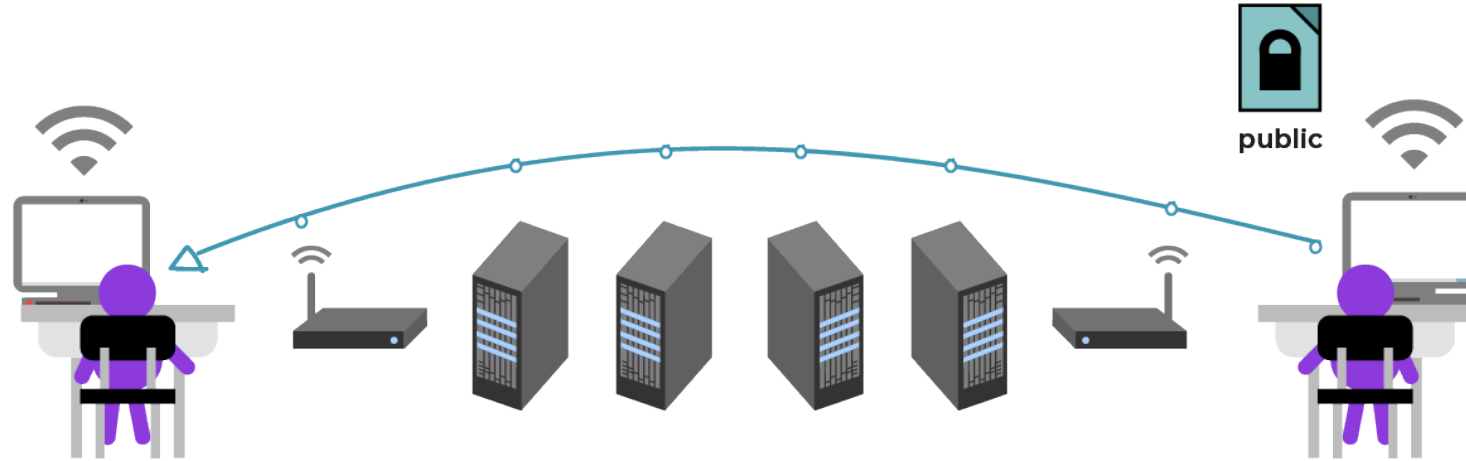
private key

Asymmetrische Kryptographie

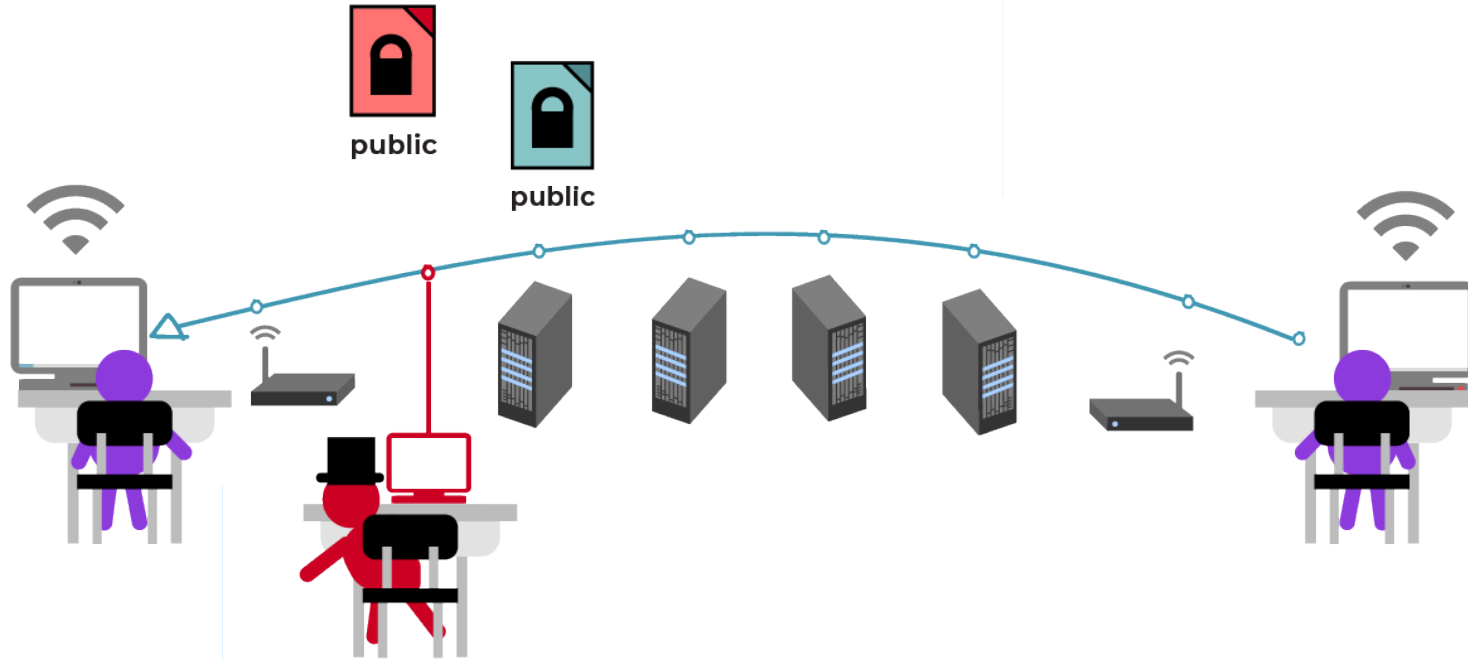
- Verschlüsselung
 - Public Key verschlüsselt
 - Private Key entschlüsselt

- Signatur
 - Private Key signiert
 - Public Key bestätigt Signatur

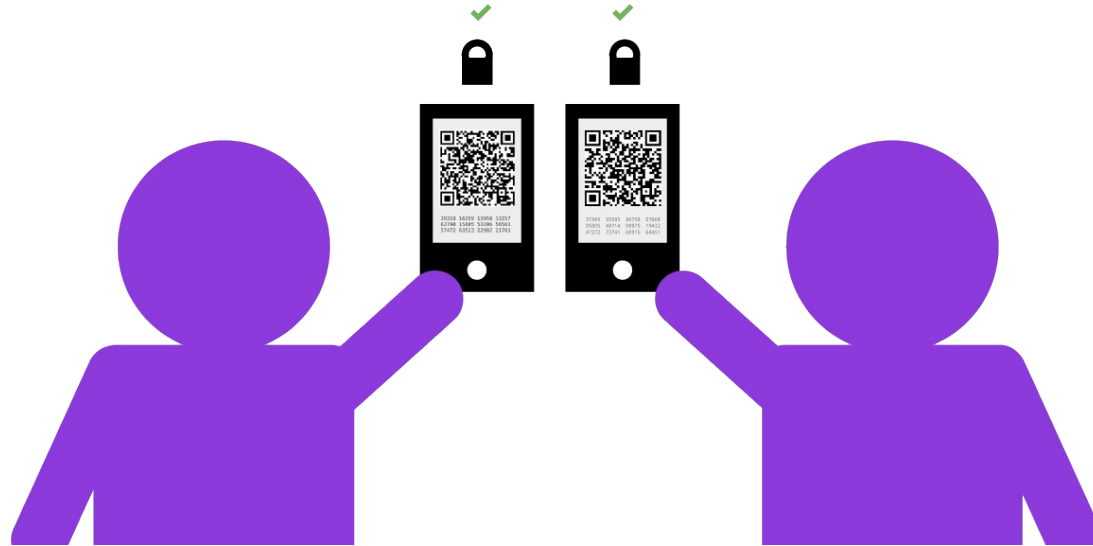
Asymmetrische Kryptographie



Asymmetrische Kryptographie



Asymmetrische Kryptographie



Asymmetrische Kryptographie

Sichere E-Mail Kommunikation

TODO: Animation

OpenPGP

- Dezentraler Vertrauensansatz
 - Jeder legt fest, wem er vertraut
- Schlüssel müssen ausgetauscht werden:
 - Persönliches Treffen, Telefonat
 - Mehrere Online-Quellen

Passwörter

Gefahren

- Anbietern werden Datenbanken geklaut
→ Für jeden Dienst andere Zugänge verwenden
- Angreifer probieren Zugangsdaten aus
→ Starke Passwörter verwenden

Have I Been Pwned?

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, [Gravatar release an FAQ detailing the incident.](#)

Compromised data: Email addresses, Names, Usernames



MGM Resorts (2022 Update): In July 2019, [MGM Resorts](#) discovered a data breach of one of their cloud services. The breach included 10.6M guest records with 3.1M unique email addresses stemming back to 2017. In May 2022, a superset of the data totalling almost 25M unique email addresses across 142M rows was extensively shared on Telegram. On analysis, it's highly likely the data stems from the same incident [with 142M records having been discovered for sale on a dark web marketplace in mid-2020.](#) The exposed data included email and physical addresses, names, phone numbers and dates of birth.

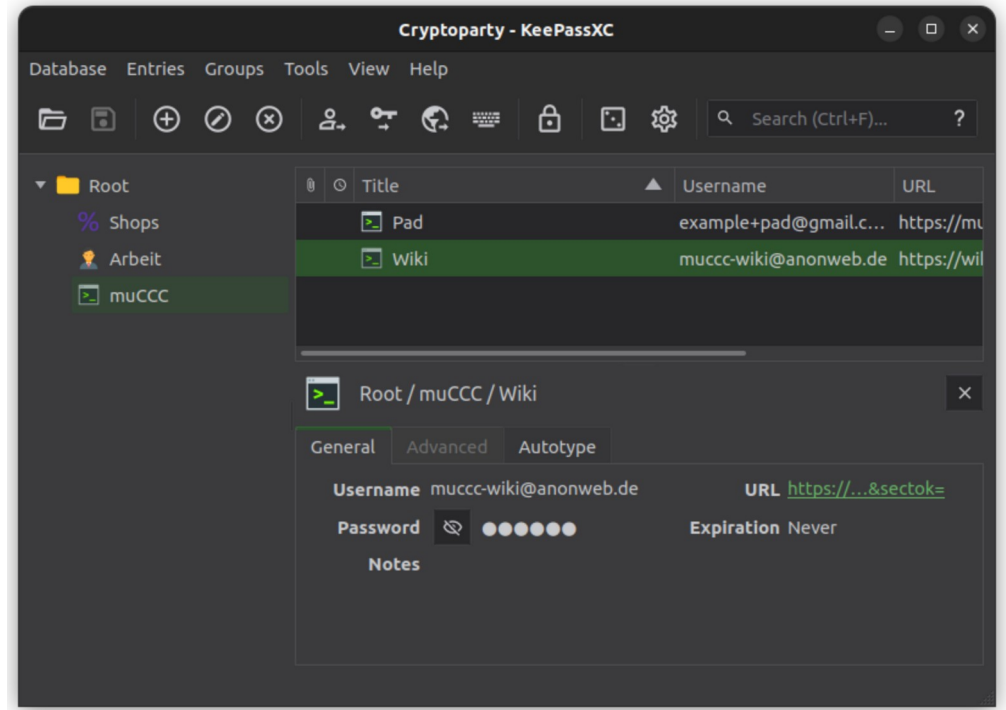
Compromised data: Dates of birth, Email addresses, Names, Phone numbers, Physical addresses

Gefahren

- Besonders wichtig: E-Mail Account
→ Wird für “Passwort vergessen” genutzt
- Starke Passwörter + überall unterschiedlich
→ Unmöglich alle zu merken

Passwort-Manager

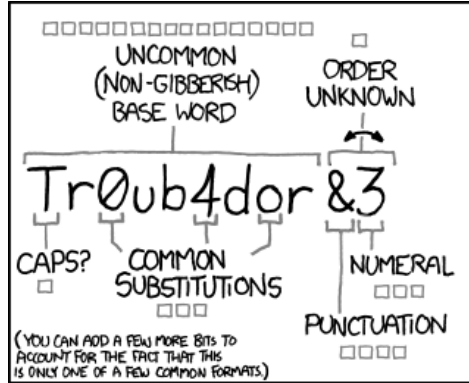
- Verschlüsselte Passwort-Datenbank
- Hat einen Master-Schlüssel
- Kann sichere Passwörter generieren
- Risiko: Alle Passwörter an einer Stelle



Sichere Passwörter

- Einige Passwörter solltet ihr kennen
 - Master-Passwort für Passwort Datenbank
 - Passwort für E-Mail Account

Passphrase



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

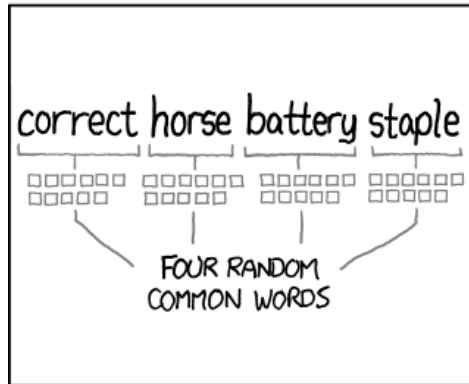
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOKEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

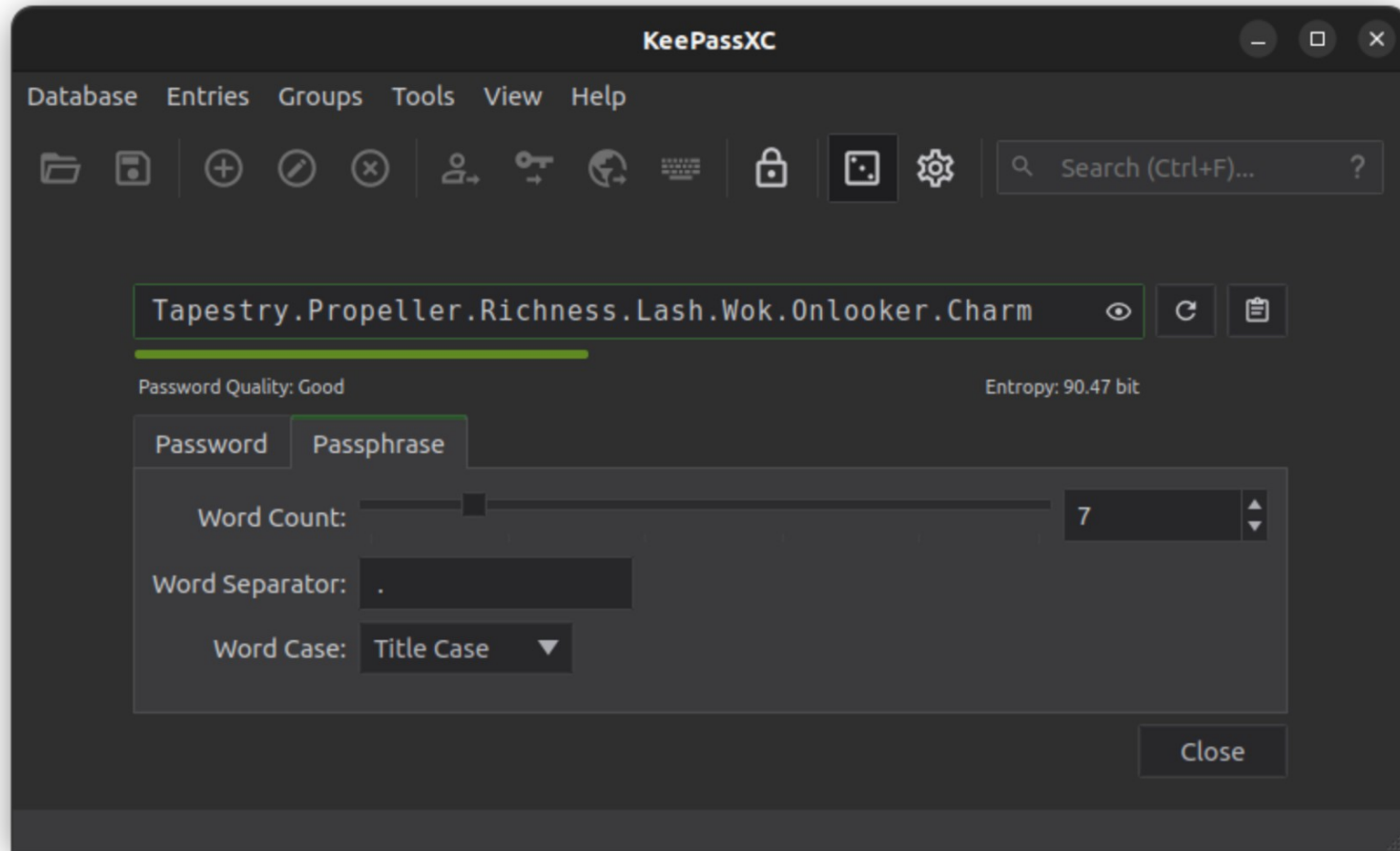
THAT'S A BATTERY STAPLE.

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.

Passphrase



Zwei-Faktor Authentifizierung

- Etwas wissen + etwas haben
- Guter Zusatzschutz vor Passwortklau
- Sollte möglichst getrennt vom Passwort liegen

Messenger

Netzwerkeffekt

- Wer benutzt
 - WhatsApp
 - Signal
 - Telegram
 - Threema

Netzwerkeffekt

- Mitmachen heißt oft Kompromisse machen
- Wichtig: konkrete Risiken verstehen
- Messenger sind im Detail sehr unterschiedlich

Schwache Verschlüsselung

- Viele Messenger bieten Verschlüsselung
- Aber nicht alle
- Und nicht alle gleich gut

Backups

- Liegen oft in der Cloud
- Teilweise im Klartext!

Metadaten

- Kann man nicht verschlüsseln
- Aber vermeiden
- Geschäftsmodelle betrachten

Telefonbuch

- Messenger laden eure Kontakte in die Cloud
- Gibt euer ganzes Netzwerk preis

Schutzmaßnahmen

- Berechtigungen entziehen
 - Zugriff auf Telefonbuch verhindern
- Schlüssel verifizieren
- Bewusst Vertrauen abwägen

Fragen? Anmerkungen?