EINSTIEG VERSCHLÜSSELUNG

Stadtbibliothek Saarbrücken

Landesmedienanstalt Saarland

06.02.2019
Wolf-Dieter Scheid

SID 19
SAFER INTERNET DAY

EINSTIEG

Quelle:
CC-Zero:
https://pixabay.com/de/elefanten-elfenbein-tiere-afrika-970456/, Sponchia

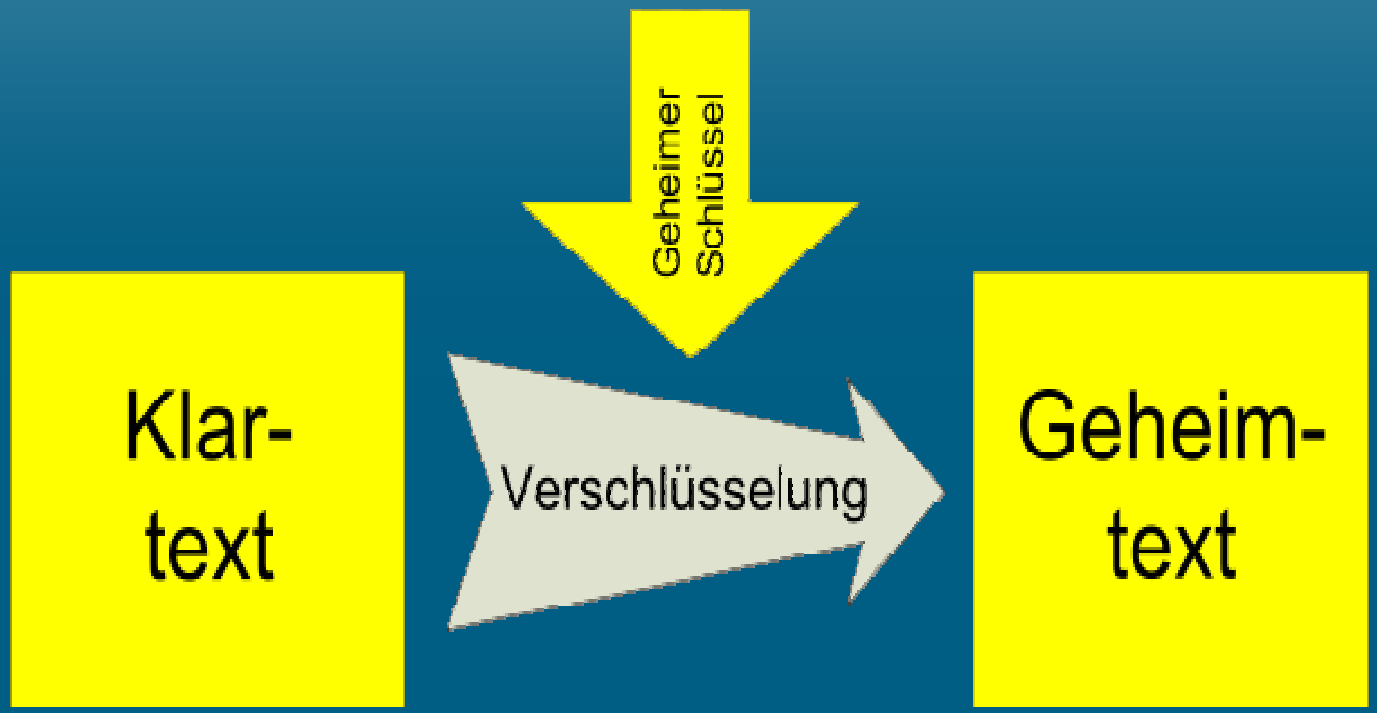
Die Blinden (Männer) und der Elefant
https://de.wikipedia.org/wiki/Die_blinden_M%C3%A4nner_und_der_Elefant

INHALT

- Was ist das?
- Warum – Ich habe nichts zu verheimlichen!
- Varianten
- Vorkommen im Alltag
- Programme und Anwendungen

WAS IST DAS?

Schaubild Verschlüsselung



WAS IST DAS?

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“ Zeichenfolge (Geheimtext) umgewandelt wird.

WAS IST DAS?

Als entscheidend wichtige Parameter der Verschlüsselung werden hierbei ein oder auch mehrere **Schlüssel** verwendet.

Das wissenschaftliche Forschungsgebiet, das sich mit Verschlüsselungsverfahren und ihrer Geschichte beschäftigt, wird als **Kryptographie** bezeichnet.

(Quelle: https://de.wikipedia.org/wiki/Verschl%C3%BCsselung)

WAS IST DAS?

Beispiel:

Verschlüsselung des Wortes „BIBLIOTHEK“

Verschlüsselung: Ersetzung jedes Buchstabens durch den Nachfolgebuchstaben im Alphabet

Großbuchstaben	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Kleinbuchstaben	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

„CJCMJPUIFL“

WAS IST DAS?

Weitere Infos:

Aktuelle Infos zum Thema Verschlüsselung bei heise.de: **tinyurl.com/mrquw5a**

Anonymität, Verschlüsselung und Datenschutz: **privacy-handbuch.de**

WARUM – ICH HABE NICHTS ZU…

Beispiele:

E-Mail:

- Schöne Grüße aus dem Schwarzwald sendet Dir Klaus

- Einladung zum Geburtstag am 6.2.2019, Feier am Tag selbst

Die E-Mail ist eine elektronische Postkarte

WARUM – ICH HABE NICHTS ZU…

Beispiele:

Surfen im Internet:

- Suche nach Krankheiten

- Suche nach Islamismus, Nazis, etc.

Standard Android: Erfassung aller Aktivitäten bei der Internetsuche und Verwendung von Apps

WARUM – ICH HABE NICHTS ZU…

Problem:

Erfassung/Mitlesen dessen, was wir suchen und machen

Auswertung durch Computerprogramme

Kein Blick auf die Beweggründe, warum wir etwas tuen

Was mir unwichtig erscheint, kann für Andere wichtig sein - Werbung

WARUM – ICH HABE NICHTS ZU…

Vier Ziele bei der Kommunikation im offenen Internet:

Identität des Senders

Integrität der Information

Vertraulichkeit

Verbindlichkeit

WARUM – ICH HABE NICHTS ZU…

Identität des Senders:

Diese Nachricht stammt von mir

Integrität der Information:

Ich habe diese Nachricht so abgeschickt und sie kommt unverändert bei Dir an

WARUM – ICH HABE NICHTS ZU…

Vertraulichkeit:

Nur Personen, für die die Nachricht bestimmt ist, dürfen sie lesen

Verbindlichkeit:

Was ich hiermit erkläre, ist verbindlich

WARUM – ICH HABE NICHTS ZU…

Vier Ziele bei der Verschlüsselung von Daten auf eigenen Geräten:

Unberechtigter Zugriff

Schutz bei Verlust und Diebstahl

Gespeicherte Passwörter

Gesetze wie die DSGVO

VARIANTEN

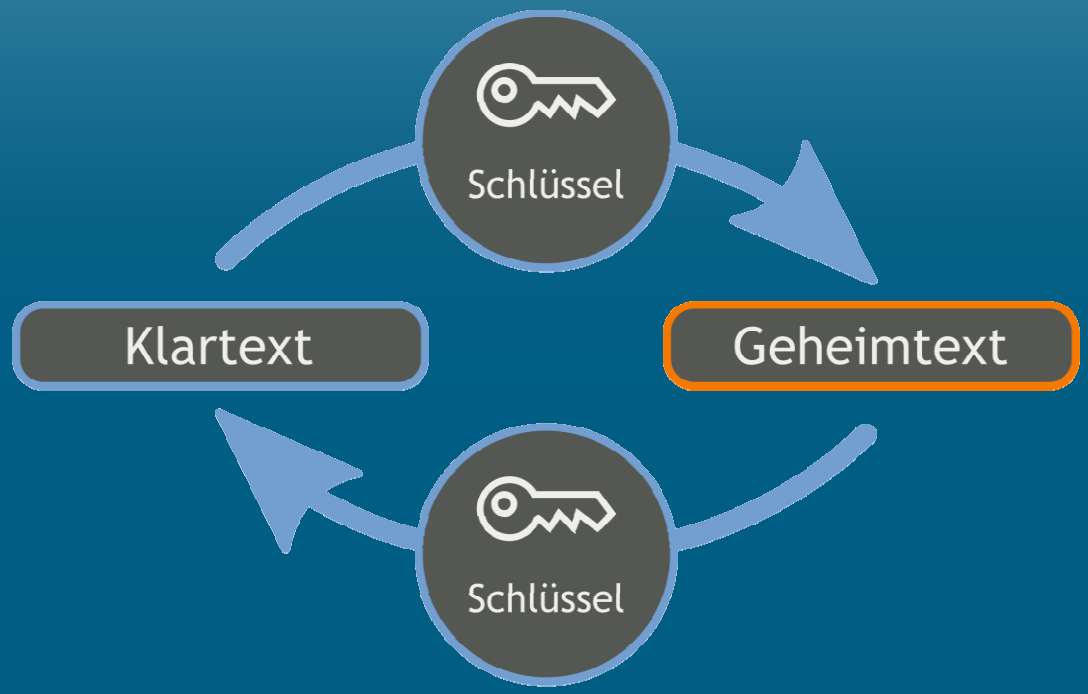
Symmetrische Verschlüsselung

Asymmetrische Verschlüsselung

Hybride Verschlüsselung

VARIANTEN

Symmetrische Verschlüsselung



Bananenfalter [CC0], from Wikimedia Commons

VARIANTEN

Symmetrische Verschlüsselung

VARIANTEN

Symmetrische Verschlüsselung (Beispiele)

Der **Data Encryption Standard (DES)** ist ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus.

Der **Advanced Encryption Standard (AES)** ist als Nachfolger für DES 2000 vom National Institute of Standards and Technology (NIST) als Standard bekanntgegeben wurde.

VARIANTEN

Verschlüsselung (Problem)

Es gibt einen Zusammenhang zwischen dem Schlüssel und dem verschlüsselten Text.

Durch Berechnung lässt sich jede Verschlüsselung rückgängig machen.

Ausprobieren, bis der Schlüssel passt:
Brute Force Attacke

VARIANTEN

Verschlüsselung (Lösung)

Schlüssellänge

Der Schlüssel muss so lang sein, dass er innerhalb einer sinnvollen Zeitspanne nicht berechnet werden kann.

Angabe der Schlüssellängen in Bit:
AES 128, 192 oder 256 Bit

VARIANTEN

Verschlüsselung (Lösung)

AES 128 Bit:

770A8A65DA156D24EE2A093277530142

AES 256 Bit:

B374A26A71490437AA024E4FADD5B497FDFF1
A8EA6FF12F6FB65AF2720B59CCF

ARTEN

Symmetrische Verschlüsselung

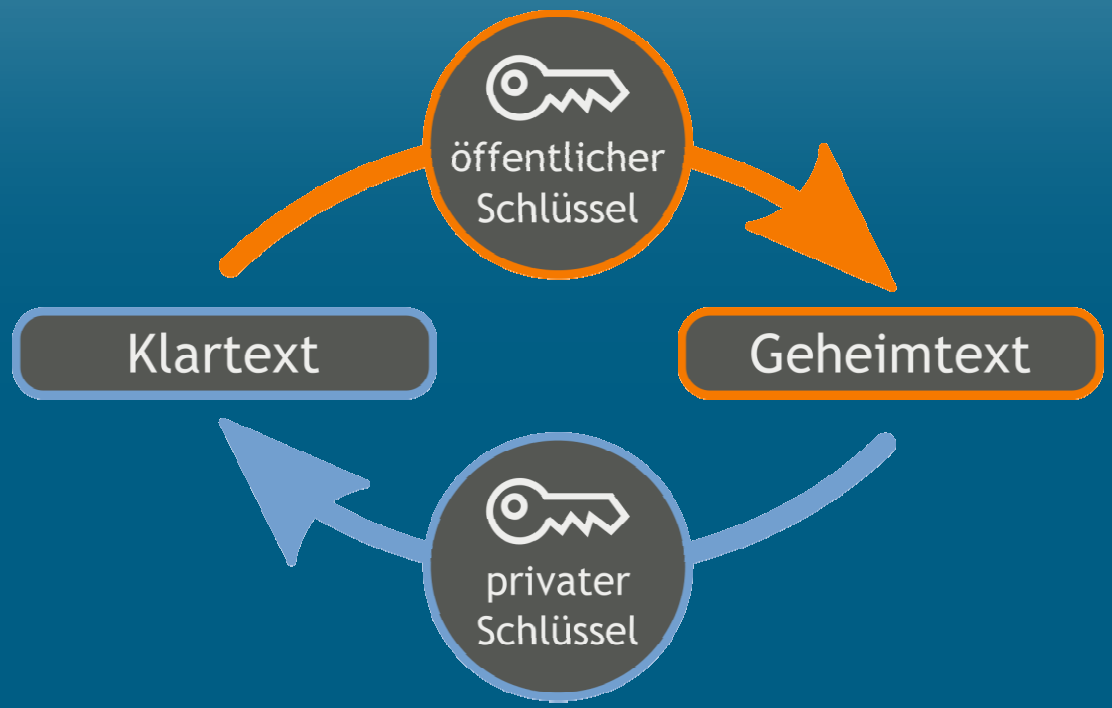
Problem:

Schlüsseltausch

- Wie kommt der Schlüssel sicher von einer Person zu einer anderen? -

VARIANTEN

Asymmetrische Verschlüsselung



Bananenfalter [CC0], from Wikimedia Commons

VARIANTEN

Asymmetrische Verschlüsselung (Beispiel)

RSA (benannt nach Rivest, Shamir und Adleman)
ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann

VARIANTEN

Asymmetrische Verschlüsselung (Verfahren)

Jeder TN erzeugt ein Schlüsselpaar aus einem öffentlichen und einen geheimen Schlüssel

Der geheime Schlüssel verbleibt immer beim TN

VARIANTEN

Asymmetrische Verschlüsselung (Verfahren)

Der öffentliche Schlüssel wird maximal verbreitet und öffentlich zugänglich gemacht:

Versand und Schlüsselserver

VARIANTEN

Asymmetrische Verschlüsselung (Verfahren)

Die Verschlüsselung erfolgt immer mit dem öffentlichen Schlüssel der Empfangsperson

Die Entschlüsselung erfolgt immer mit dem eigenen privaten Schlüssel der Empfangsperson

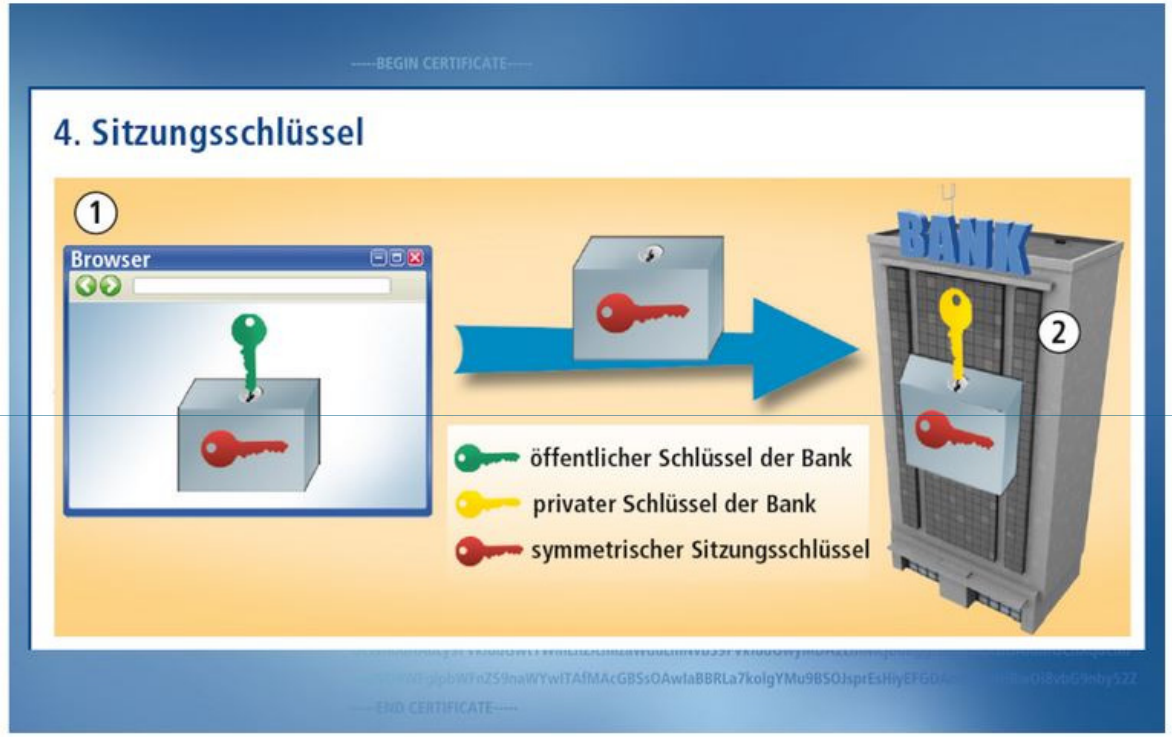
VARIANTEN

Hybirde Verschlüsselung (Verfahren)

Kombination von symmetrischer und asymmetrischer Verschlüsselung

VORKOMMEN IM ALLTAG

Onlinebanking: https

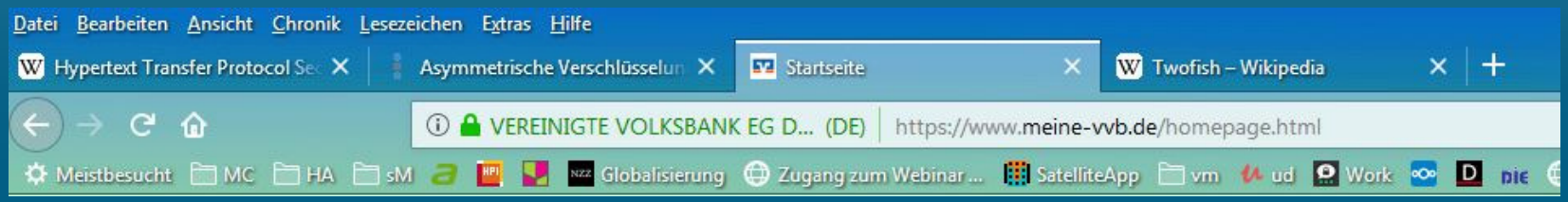


Ihr Browser erstellt einen Schlüssel, mit dem das Online-Banking verschlüsselt werden soll (rot). Dieser Schlüssel muss zur Bank. Dazu wird er wiederum verschlüsselt - mit dem öffentlichen Schlüssel der Bank (1). Die Bank öffnet das Paket mit ihrem privaten Schlüssel (2)

Quelle: com-magazin.de

VORKOMMEN IM ALLTAG

Onlinebanking: https



Nachrichten, die du in diesem Chat sendest, sowie Anrufe, sind jetzt mit Ende-zu-Ende-Verschlüsselung geschützt. Tippe für mehr Infos.

VORKOMMEN IM ALLTAG

Ende zu Ende Verschlüsselung: WhatsApp

Quelle: https://www.mimikama.at/whatsapp/die-ende-zu-ende-verschlsselung-von-whatsapp/

PROGRAMME UND ANWENDUNGEN

Ausgewählte Beispiele:

1. Verschlüsselter USB-Stick
2. Verschlüsselte E-Mails und Dateien
3. Verschlüsselte Festplatten und USB-Sticks
4. Einfaches Verschlüsseln von Dateien
5. Verschlüsselungstrojaner und Co
6. Passwortmanager

PROGRAMME UND ANWENDUNGEN

1. Verschlüsselter USB-Stick:

Verschlüsselung durch Software:

Punkt 2, 3 und 4

oder

USB-Stick mit eingebauter Verschlüsselung

PROGRAMME UND ANWENDUNGEN

1. Verschlüsselter USB-Stick:

USB-Stick mit eingebauter Verschlüsselung

Quelle: amazon.de

PROGRAMME UND ANWENDUNGEN

2. Verschlüsselte E-Mails und Dateien

Notwendige Software:

GPG4win: gpg4win.org

Thunderbird/Outlook: thunderbird.net

Erweiterung Enigmail: Addon-Suche

PROGRAMME UND ANWENDUNGEN

3. Verschlüsselte Festplatten und USB-Sticks

VeraCrypt: Nachfolger von Truecrypt

Verschlüsselt Partitionen, Festplatten und Ordner

Bebilderte Anleitung:
tinyurl.com/muvyjm2

Download:
tinyurl.com/kehvdwn

PROGRAMME UND ANWENDUNGEN

4. Einfaches Verschlüsseln von Dateien und Ordnern

Drag'n'Crypt ULTRA, auch für USB-Stick

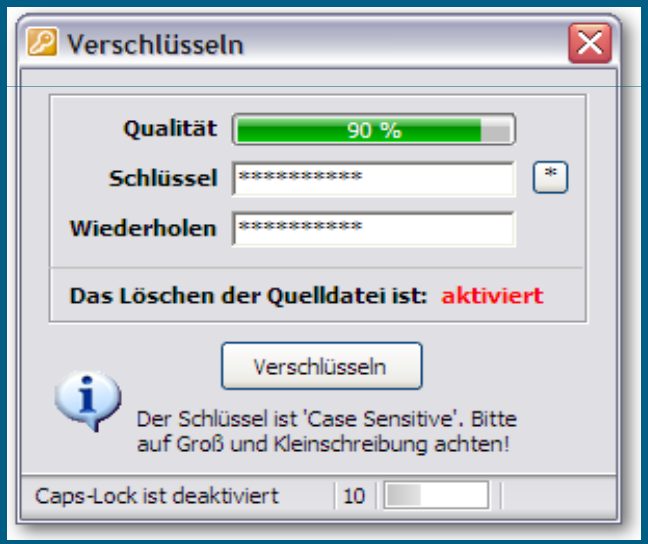
Symmetrische Verschlüsselung

hdcu.bplaced.net/home.html

PROGRAMME UND ANWENDUNGEN

4. Einfaches Verschlüsseln von Dateien und Ordnern

Ziehen Sie die Datei auf das Symbol und geben Sie ein Passwort ein



PROGRAMME UND ANWENDUNGEN

5. Verschlüsselungsviren: Ransomware

Viren, die den PC, das Smartphone oder das Tablet infizieren

Kein Zugriff auf das System mehr möglich

Lösegeldforderung

Anlaufstelle:
nomoreransom.org/de

PROGRAMME UND ANWENDUNGEN

Quelle: http://www.polizei-praevention.de/aktuelles/chimera-ransomware.html

PROGRAMME UND ANWENDUNGEN

6. Passwortmanager

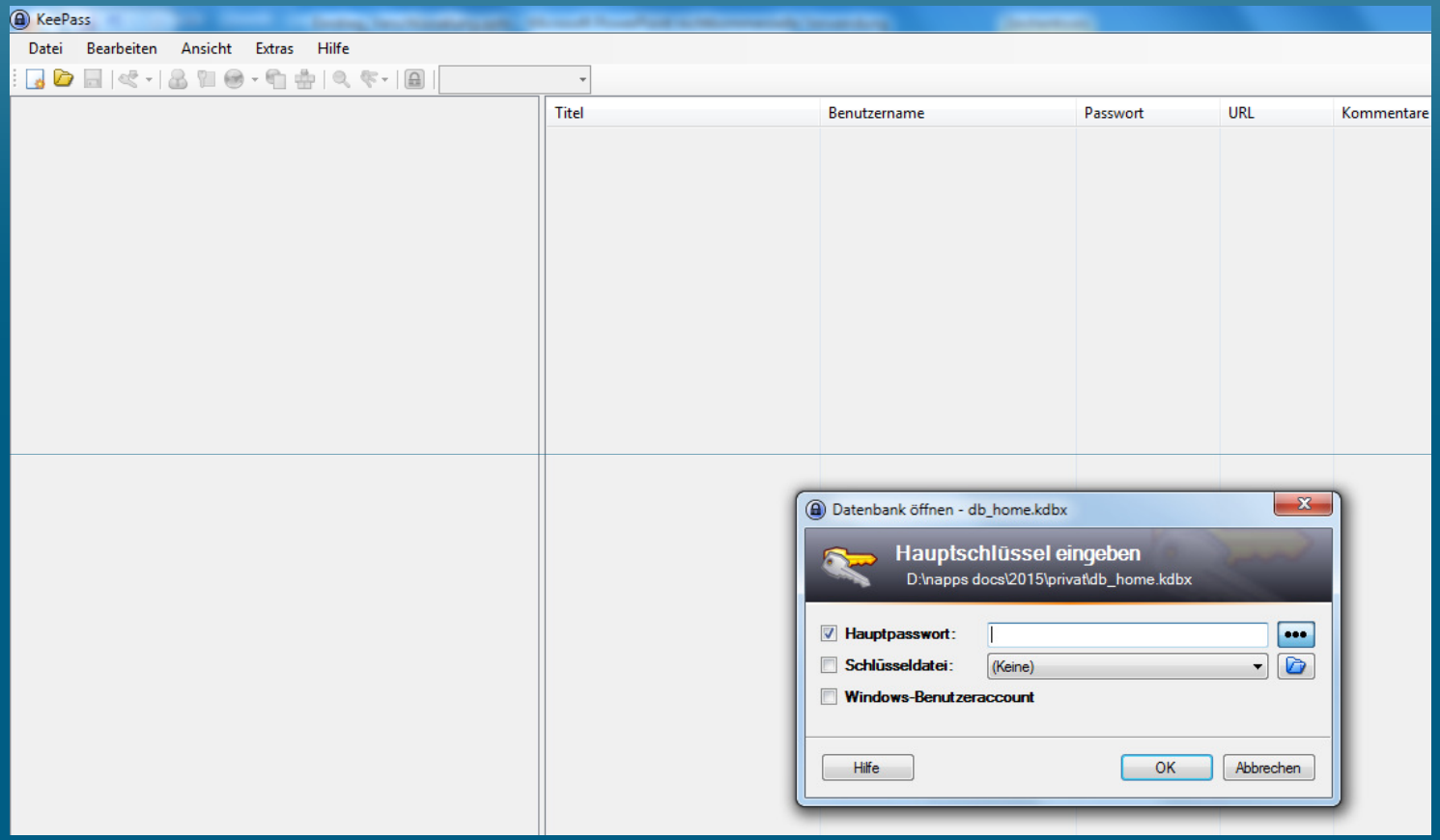
Programme oder Apps, die Passwörter in einer Datei speichern

Verschlüsselung der Datei und Zugriffsschutz mit einem Masterpasswort: KeePass

keepass.info

PROGRAMME UND ANWENDUNGEN

6. Passwortmanager



VERANSTALTUNGEN

Sicherheitsberatung für Smartphones und Tablets
Donnerstag, 07. Februar 2019, 18–20 Uhr

Daten sicher verschlüsseln
Mittwoch, 08. Mai 2019, 16–19 Uhr

Aktuelle Termine Onlinerland Saar
olsaar.de

VERANSTALTUNGEN

Safer Internet Day

12. März: Saarbrücken, LMS

08. April: Landratsamt Saarlouis

14. Mai: Landratsamt Merzig

03. September: Landratsamt St. Wendel

22. Oktober Landratsamt Homburg
29. Oktober: Landratsamt Neunkirchen

Wolf-Dieter Scheid
Dienstlich:
Mainzer Straße 269
66121 Saarbrücken
Telefon: 0681 / 68570176
Mail: wd.scheid@lag-eeb-sl.de