freeware

OTP-Crypt.com

- die perfekte Verschlüsselung -

OTP-Crypt.com

#1: Die Bedienung von OTP-Crypt

Verfügbar für Windows© und Linux©

… das beste Verfahren zum Aufbewahren und Teilen von Geheimnissen …

Wie sicher ist OTP-Crypt

OTP-Crypt.com

- Wie sicher ist OTP-Crypt?

- OTP = One-Time-Pad ist ein Verschlüsselungsverfahren das nachweislich nicht gebrochen werden kann.
- Es gilt als das sicherste (perfekte) Verschlüsselungsverfahren – weltweit.

- Das OTP besteht aus Zufallszahlen, die mit Ihren Dokumenten oder Dateien verschlüsselt werden. Das OTP ist Ihr persönlicher Schlüssel. Die OTP-Schlüssel und die Anwendungssoftware erhalten Sie auf diesen Seiten.

Welche Daten können verschlüsselt werden?

OTP-Crypt.com

Es kann jede einzelne Datei für sich verschlüsselt werden. Wenn Sie für jede Datei einen individuellen Schlüssel verwenden, dann entspricht es den Regeln für eine perfekte Verschlüsselung. Diese Vorgehensweise gilt als unknackbar.

In der Computerpraxis werden mit speziellen Programmen ganze Festplatten verschlüsselt. Beim Start muss der Anwender das Passwort angeben. Nun steht die gesamte Festplatte mit den einzelnen Dateien für den Anwender zur Bearbeitung bereit. Hier gibt es also einen Schlüssel für tausende von Dateien. Es ist außerdem sehr unsicher, da der Schlüssel (Passwort) sich auf der Festplatte befindet. Jeder Benutzer, der das Passwort kennt, hat Zugang. Man kann die Sicherheit dieses Systems mit einem Haustürschlüssel vergleichen, der unter der Fußmatte liegt.

Ähnlich unsicher ist eigentlich die gesamte Softwarepalette, die Dateien verschlüsselt und dabei den Schlüssel in diese Datei hinterlegt.

Welche Daten können verschlüsselt werden?

OTP-Crypt.com

Für jedes dieser Softwareprogramme gibt es entsprechende Software um an den internen Schlüssel zu gelangen.

Für Ihre Datensicherung ist es unpraktisch, tausende von Schlüsseln einzusetzen. Natürlich wäre dabei die Verwaltung des riesigen Schlüsselkastens eine sehr umfangreiche und fast nicht zu lösende Aufgabe. Auch ist die Sicherheit verloren, wenn andere Personen in den Besitz des Schlüsselkastens gelangen. Diese Szenarien lassen sich beliebig erweitern ...

Verschlüsseln Sie ganze Ordner, indem Sie diese Ordner vorher mit entsprechender Pack-Software (Winzip, RAR, usw.) zusammenfassen und anschließend diese eine gepackte Datei mit OTP-Crypt und ihrem eigenen individuellen Schlüssel verschlüsseln.

Bedenken Sie, dass der Schlüssel immer größer sein muss als die zu verschlüsselnde Datei. OTP-Crypt lässt außerdem keine kleineren Schlüssel in der Bedienung der Software zu.

Welche Versionen von OTP-Crypt gibt es?

OTP-Crypt.com

Die Software ist für Windows© und Linux© erhältlich. Die Versionen gibt es nur für 64bit. Für jedes Betriebssystem gibt es eine Version mit graphischer Oberfläche. Die graphische Version ist jeweils die Hauptversion. Mit ihr können in gewohnter Umgebung sowohl Dateien verschlüsselt, als auch wieder entschlüsselt werden.

Zusätzlich gibt es je 2 Versionen für den Konsolen- bzw. Terminalmodus. Diese Versionen eignen sich für die Automation der Ver- und Entschlüsselung von Datenbeständen und ist eher für versierte Benutzer in beruflicher Umgebung gedacht.

Welche Versionen von Schlüsseln gibt es?

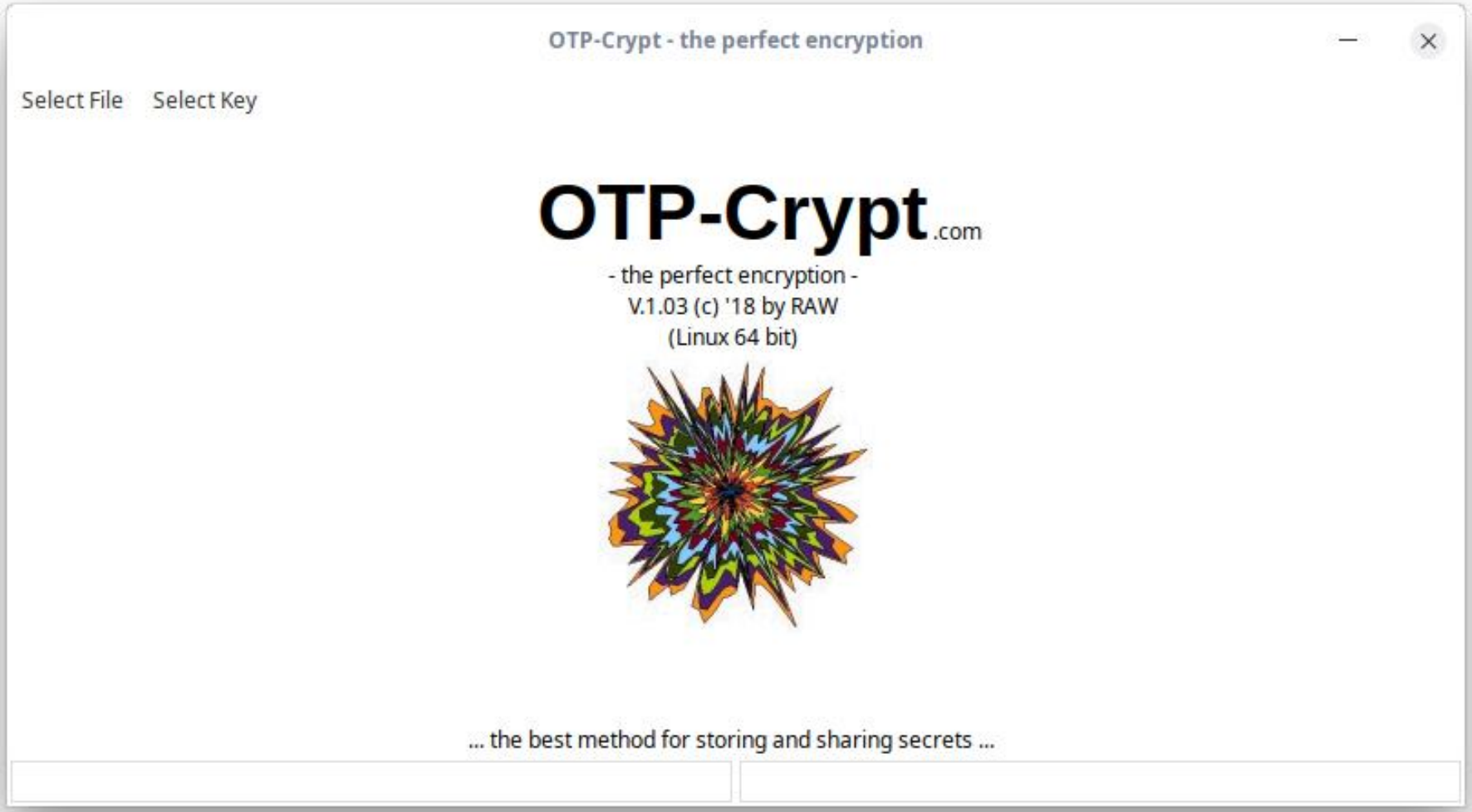
OTP-Crypt.com

Alle Schlüssel, die auf diesen Seiten zum Download bereitgestellt werden, sind Dateien mit absolut zufälligen Inhalten. Diese Schlüsseldateien sind ausschließlich durch unsere Hardware-Generatoren erzeugt worden. Die Sicherheit ist allerdings verfallen, da diese Schlüssel öffentlich downloadbar sind.

Wenn Sie individuelle Schlüssel benötigen, so setzen Sie sich bitte mit uns in Verbindung.

Jeder Schlüssel ist individuell hergestellt und besitzt im Dateinamen seine eigene CRC32-Prüfsumme. Er lässt sich damit einfach von anderen Schlüsseln unterscheiden. Ein typischer Dateiname könnte ‚key_0ef7ee65.otpkey' lauten. Die Endung ‚.otpkey' ist als Kennung notwendig. Die CRC32-Prüfsumme findet sich aus Sicherheitsgründen nicht in den Dateinamen der verschlüsselten Datei wieder.

Die graphische Oberfläche



OTP-Crypt.com

Die Varianten für Windows© und Linux© sind gleich aufgebaut.

OTP-Crypt.com

1. Wählen Sie eine Datei ‚Select File‘ aus. Nach dem Klick müssen Sie zuerst ‚ENCRYPT‘ oder ‚DECRYPT‘ auswählen. Das Menu wird entsprechend angehakt. Durchsuchen Sie ihren Datenbestand und wählen die Datei aus. Unten in der linken Fußzeile wird die Auswahl angezeigt.
2. Wählen Sie im Menü ‚Select Key‘. Wählen Sie im Normalfall ‚… your private key‘ oder ‚… other key‘, wenn Sie einen Fremdschlüssel zum Ver- oder Entschlüsseln einsetzen möchten (dient zum Datenaustausch mit anderen Personen). Unten rechts in der Fußzeile wird die Auswahl angezeigt.
3. Entscheiden Sie bei der Sicherheitsabfrage zwischen Ja und Nein, ob eine Verschlüsselung stattfinden soll oder nicht.
4. Bei ‚Ja‘ können Sie OTP-Crypt beenden. Die verschlüsselte Originaldatei wird im Konsolen- bzw. Terminalmodusicht nicht gelöscht und bleibt Ihnen erhalten. Die neue verschlüsselte Datei bekommt mit ‚.otpcrypt‘ eine zusätzliche Endung.

Die Varianten für Windows© und Linux© sind gleich aufgebaut.

OTP-Crypt.com

5. Verfahren Sie zur Entschlüsselung von Dateien in ähnlicher Weise.
6. Wird eine verschlüsselte Datei entschlüsselt, so wird ohne Nachfrage die originale Datei überschrieben. Sie erhalten so den originalen Zustand der Datei ohne Nachfrage zurück.

Die Bedienung der Software ist für den Anwender so einfach wie möglich gehalten.

Der Konsolen- bzw. Terminalmodus

OTP-Crypt.com

Es gibt jeweils ein Programm für die Verschlüsselung (otp-encrypt) und ein Programm für die Entschlüsselung (otp-decrypt). Sie entscheiden sich bei Aufruf des Programms für den jeweiligen Zweck.

Wir hätten auch nur ein einziges Programm entwickeln können, welche die Ver- und Entschlüsselung enthält. Dazu hätten Sie einen zusätzlichen Parameter beim Aufruf mit abgeben müssen. Nach kurzer Zeit hätten Sie aber die Reihenfolge der 3 Aufrufe verwechselt. Diese Variante erschien uns zu fehlerbehaftet. Sie brauchen in diesen 2 Varianten nur jeweils 2 Parameter angeben. Der erste Parameter ist die Datei, die Sie ver- oder entschlüsseln wollen. Der zweite Parameter ist die Angabe des Schlüssels. Beide Parameter sind natürlich mit den Pfadangabe zu versehen.

Die Bedienung der Software ist wie in der graphischen Version, so einfach wie möglich gehalten. Das bedeutet aber nicht, dass die Software keine Intelligenz besitzt.

Der Konsolen- bzw. Terminalmodus

OTP-Crypt.com

Gewisse Vorkehrungen, wie eine Verriegelung, erhöhen auch hier den Bedienkomfort:

Encrypt:

- Keine Dateien mit Inhalt (otp,key) im Namen erlaubt
- Zu verschlüsselnde Dateien erhalten keinen neuen Namen
- Zu verschlüsselnde Dateien erhalten die Endung: Name.otp-crypted
- Nur 2 Namen im Aufruf notwendig: Name.irgendwas mit private.otpkey
- Beispiel: Aus Name.irgendwas wird Name.irgendwas.otp-crypted

Decrypt:

- Nur der Type Name.irgendwas.otp-crypted mit private.otpkey ist zulässig
- Beispiel: Aus Name.irgendwas.otp-crypted wird automatisch: Name.irgendwas

Was noch von Interesse ist

OTP-Crypt.com

Das Ver- und Entschlüsseln von Dateien findet aus Gründen der Performance im Arbeitsspeicher statt. In heutiger Zeit steht hinreichend Speicherplatz zur Verfügung.

Achten Sie daher bei älteren Computern auf ausreichend Speicherplatz.

Die Bedienung im Konsolen- bzw. Terminalmodus gestaltet sich schwieriger als die Bedienung der Software in der graphischen Oberfläche. Gelegentlich werden Bedienfehler durch den Nutzer verursacht.

Die Fehlerausgabe wird nach Prüfung mit einem Error-40 quittiert.

Error-40 bedeutet, dass sich der Fehler 40 cm vor dem Monitor befindet. 🙂

Kontakt

OTP-Crypt.com

Senden Sie eine E-Mail an unsere interne Mailingliste:

support@otp-crypt.com

Wir beantworten Anfragen in:

- Deutsch
- Englisch
- Französisch
- Spanisch

Anfragen, die nicht auf Deutsch eingehen, werden länger dauern. Unvollkommenes Deutsch ist willkommen. 🙂