Allgemeine Informationen zu Random Crypt

Zuerst einmal vielen Dank, dass Sie sich für Random Crypt entschieden haben. Wir möchten Ihnen hier ein paar grundlegende Fakten zu Random Crypt beschreiben.

Was unterscheidet Random Crypt so grundlegend von anderen Chiffrierungsverfahren?

Alle bisherigen Chiffrierungsverfahren chiffrieren mit aufwendigen mathematischen Algorithmen. Je aufwendiger der Algorithmus, desto sicherer. Werden Computer schneller, sind die eben noch sicheren Verschlüsselungsverfahren veraltet und neue müssen her.

Random Crypt verschlüsselt nicht mit einem mathematischen Algorithmus!

Das macht Random Crypt so einzigartig. Es gibt keinen mathematischen Algorithmus. Nichts was ein Computer nachverfolgen oder zurückrechnen könnte. Random Crypt verschlüsselt mit echten Zufällen, welche von Ihnen als Nutzer erzeugt und sich durch die Anordnung der Bytes im zu chiffrierenden Original ergeben. Zur Steuerung von Random Crypt werden auch vereinzelt während der Chiffrierung sogenannte Pseudo-Zufallszahlen erzeugt. Es handelt sich dabei aber immer um eine einzelne Zahl, welche im Chiffrat verschlüsselt eingetragen wird. Random Crypt chiffriert **nicht** mit Pseudo-Zufallszahlen. Eine Chiffrierung mit Pseudo-Zufallszahlen ist absolut unsicher!
Wenn ein Chiffrierungsverfahren sicher gegen Quantenrechner und künstliche Intelligenzen ist, dann Random Crypt.

Woran können Sie erkennen, dass Random-Crypt nicht mit einem mathematischen Algorithmus chiffriert?

Jedes mathematische Verschlüsselungsverfahren erzeugt bei Verwendung des gleichen Schlüssels, beim gleichen Original immer wieder das gleiche Chiffrat. Kann ja auch nicht anders, da Berechnungen in der Mathematik bei gleichen Werten immer wieder das gleiche Ergebnis liefern. Bei Random Crypt können Sie von dem gleichen Original, bei Verwendung des gleichen Schlüssels Millionen von Chiffraten herstellen und keine zwei erzeugen, die identisch sind. Für den Zufall gibt es keine Beschränkung in der Anzahl. Obwohl jedes Chiffrat anders ist, kann jedes einzelne Chiffrat mit dem Schlüssel wieder zum Original zurück dechiffriert werden.
Diese Fähigkeit aus lauter unterschiedlichen Chiffraten wieder das gleiche Original zu erzeugen ich einzigartig.
Kein mathematisches Verfahren kann bei dieser Chiffriertechnik einen Ansatz finden, um es zu knacken. Nicht jetzt und nicht in der Zukunft. Deshalb ist Random Crypt die richtige Wahl, wenn Sie ein zukunftssicheres Chiffrierungsverfahren benötigen.

Bedienungsanleitung für Random Crypt

Einstellungen nach der Installation

Random Crypt ist in seiner Bedienung einfach gehalten und die meisten Funktionen sind selbsterklärend.
Hier eine Übersicht über alle Funktionen.

Nach dem Download von Random Crypt müssen Sie als erstes die Sprache in der Sie Random Crypt nutzen wollen auswählen. 11 Sprachen stehen Ihnen zurzeit zur Verfügung.

Dazu klicken Sie auf eine der Flaggen auf der linken Seite in Random Crypt.

Sofort schaltet sich Random Crypt auf die ausgewählte Sprache um.

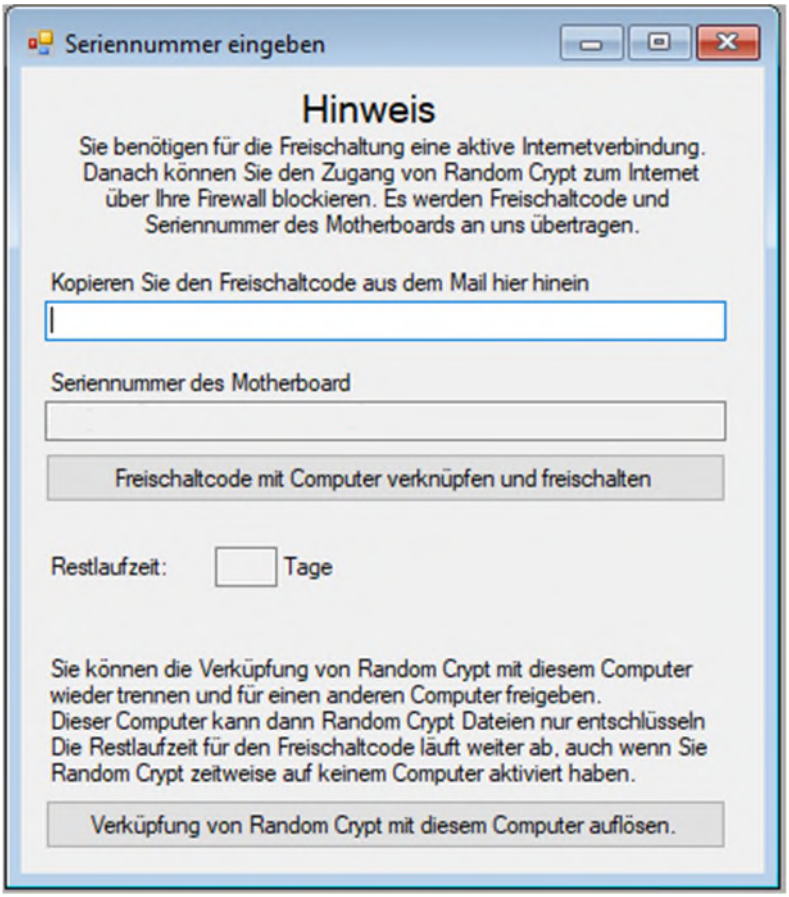
Sie können die Sprache jederzeit wechseln.

Danach klicken Sie auf den Button links. Er befindet sich links unten in Random Crypt
Bitte beachten Sie hierbei, dass Sie für die Freischaltung eine aktive Internetverbindung haben müssen.

Nach der Freischaltung können Sie Random Crypt für das Internet sperren. So können Sie sicher sein, dass keinerlei Daten zu Ihren Verschlüsselungen versendet werden.
Random Crypt benötigt nur zu Freischaltungszwecken eine Internetverbindung. Wenn das Programm zwischendurch eine Internetverbindung aufbauen will, handelt es sich nicht um eine Version von uns. Aus diesem Grund verzichten wir auch auf automatische Updatefunktionen.

Beim Kauf von Random Crypt wird Ihre E-Mail-Adresse gespeichert und wenn in Ihrem Zeitraum der Freischaltung ein Update verfügbar ist, benachrichtigen wir Sie per Mail. Zu weiteren Zwecken wird Ihre E-Mail-Adresse nicht verwendet.

Nach dem Klick auf den Button erschein folgendes Fenster:



Kopieren Sie hier Ihren Freigabecode hinein, den Sie mit der Mail zum Kauf erhalten haben. Bewahren Sie den Freigabecode gut auf. Wenn Sie den Computer wechseln und die Verbindung mit dem Computer trennen möchten, benötigen Sie den Freigabecode.

Bestätigen Sie die Freischaltung und sofort können Sie Random Crypt benutzen. Wenn Sie den Zugang zum Internet für Random Crypt sperren möchten, dann können Sie das nun tun.

Datenschlüssel erstellen

Bei der gesamten Verschlüsselung dreht es sich immer wieder um den Datenschlüssel. Er ist die wichtigste Komponente der Verschlüsselung und verdient besonderer Beachtung.
Wie Sie den Datenschlüssel generieren hängt stark davon ab, wie Sie Random Crypt benutzen wollen.

Random Crypt selbst ist auch vor Entschlüsselungsversuchen mit Quantencomputern geschützt. Es gibt aber einen Angriffspunkt und das ist die Erzeugung des Datenschlüssels.

Datenschlüssel durch Generierungscode erzeugen

Wenn Sie den Datenschlüssel durch einen Generierungscode erstellen, dann ist Ihr Chiffrat nur so gut geschützt wie stark Sie den Generierungscode erdacht haben. Je länger er ist und je mehr Sonderzeichen und Zahlen Sie benutzen, desto sicherer ist Ihr Chiffrat. Generell sollten Sie diese Methode nur verwenden, wenn Sie die Chiffrate an mehreren Orten verwenden müssen und keinen USB-Stick mit herumtragen möchten. Sonst bieten sich sicherere Methoden zur Erzeugung des Datenschlüssels an.

Datenschlüssel durch eine Datei erzeugen

Random Crypt bietet Ihnen die Möglichkeit, einen Datenschlüssel durch Verwendung einer beliebigen Datei (größer als 100 Kilobyte) zu erzeugen. Es eignet sich jede Art von Datei dazu, um einen Datenschlüssel zu erzeugen. Sie muss nur groß genug sein. Wenn die Datei aus welcher der Schlüssel stamm, nicht verändert wird, können Sie durch diese Datei immer wieder denselben Datenschlüssel erzeugen. Das heißt das solange die ursprüngliche Datei existiert, müssen Sie den Datenschlüssel nicht speichern. Diese Variante ist sehr sicher und gleichzeitig flexibel, wenn Sie von mehreren Computern auf das Chiffrat zugreifen möchten.

Datenschlüssel mit dem Zufallsgenerator erstellen

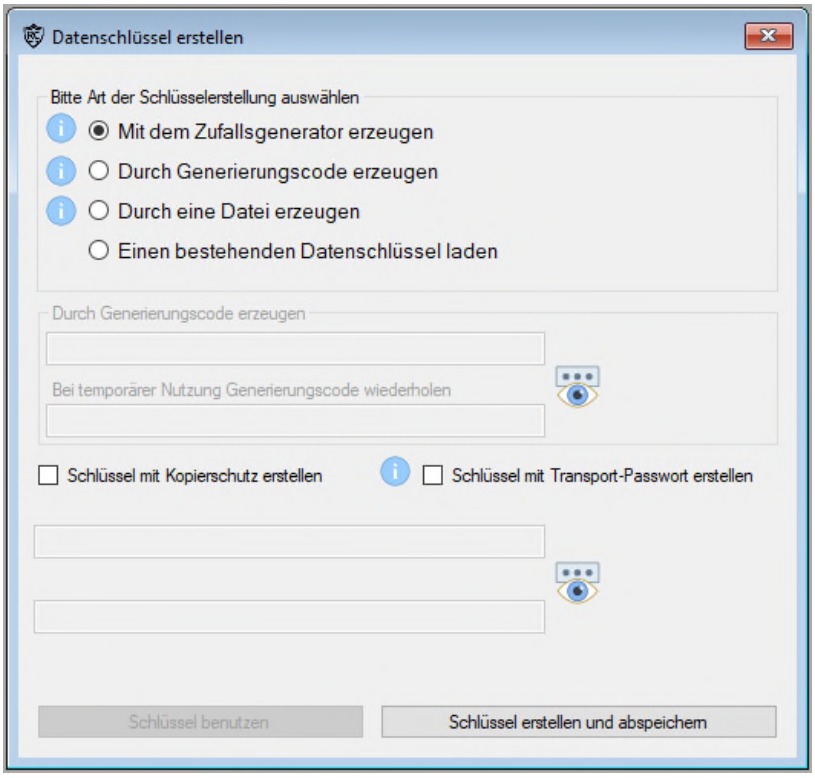
Auch wenn der Datenschlüssel in dieser Variante mit mathematisch errechneten Pseudozufallszahlen erzeugt wird, ist diese Variante doch die Sicherste. Die Pseudozufallszahlen erzeugen nicht den Inhalt des Datenschlüssels, sondern deren Anordnung im Datenschlüssel. Der Inhalt ist in jedem Datenschlüssel gleich. Es sind 256-mal die Zahlen von 0 bis 255. Doch wie diese Zahlen angeordnet werden, dass macht den Datenschlüssel aus. Es gibt über $259 * 10^{157.823}$ Varianten. Das ist eine Zahl mit 157823 Nullen am Ende. Das ist eine ausreichende Menge um alle Quantenrechner der Welt bis zum Ende der Existenz unseres Universums rechnen zu lassen.
Diesen Datenschlüssel müssen Sie vor Verwendung unbedingt auf einem geeigneten Medium speichern.
Er ist ja nur 65 Kilobyte groß und findet Platz auf jedem USB-Stick.
Achten Sie darauf, dass Sie diesen Datenschlüssel nicht verlieren, denn er lässt sich kein zweites Mal generieren!

Für alle Datenschlüssel gilt, wenn Sie Ihn verlieren, oder nicht mehr wissen wie Sie ihn generiert haben, können Sie die Chiffrate nicht mehr wieder dechiffrieren.
Auch wir können das nicht!

Bedienung des Formulars „Datenschlüssel erzeugen“

Nach dem Start des Programms sehen Sie links in der Auswahlleiste dieses Symbol. Das sagt Ihnen, dass Sie bevor Sie mit dem Ver- oder Entschlüsseln von Dateien beginnen können, einen Datenschlüssel erzeugen, oder laden müssen.

Klicken Sie dafür auf dieses Symbol in der Auswahlleiste links. Dadurch öffnet sich folgendes Fenster:



Die drei Arten um einen Datenschlüssel zu generieren haben wir schon weiter oben beschrieben.
Hier noch die Erklärung zu den beiden zusätzlichen Optionen „Schlüssel mit Kopierschutz erstellen“ und „Schlüssel mit Transportpasswort erstellen“

Schlüssel mit Kopierschutz erstellen

Diese Option können Sie wählen, wenn Sie vermeiden möchten, dass ein auf einem USB-Stick gespeicherter Datenschlüssel von dem USB-Stick auf einen anderen USB-Stick oder ein anderes Medium gespeichert und unerlaubt verwendet wird. Dabei verhindert der Kopierschutz nicht das Kopieren des Datenschlüssels. Der Kopierschutz bewirkt, dass die Kopie auf einem anderen Speichermedium als dem Original USB-Stick funktioniert. Probieren Sie es mal aus. Wenn Sie den USB-Stick kopieren möchten, müssen Sie den Datenschlüssel erst einladen mit dem Button „Einen bestehenden Datenschlüssel laden“ und dann auf einem anderen USB-Stick speichern. Dabei können Sie auch diesen USB-Stick mit einem Kopierschutz versehen.

Schlüssel mit Transportpasswort erstellen

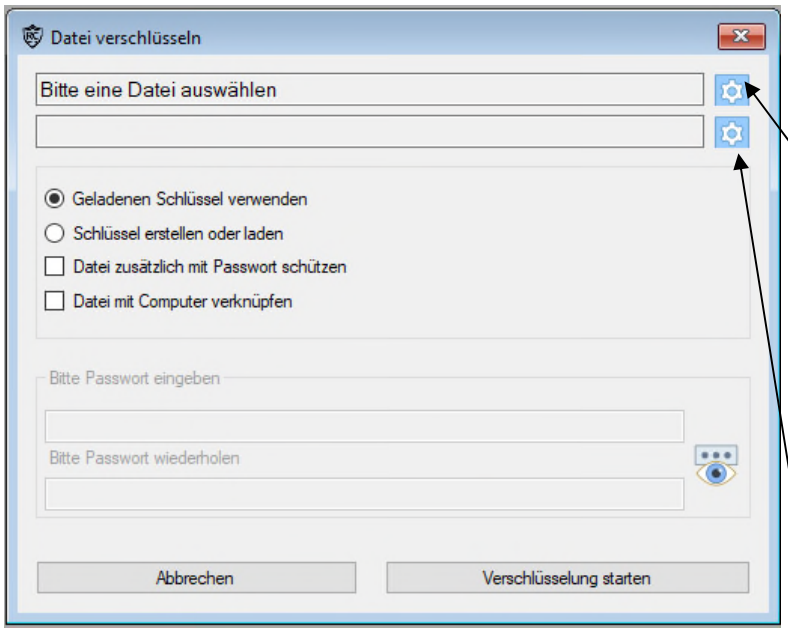
Für ganz besondere Zwecke können Sie den USB-Stick für den Transport von einem Computer zum anderen mit einem Passwort versehen, welches für die Benutzung des Schlüssels eingegeben werden muss. Erst dann können Sie mit dem Schlüssel vorher chiffrierte Dokumente wieder dechiffrieren.

Wenn Sie den Schlüssel gerade erzeugt haben, müssen Sie noch bestimmen, ob er nur verwendet werden soll, oder ob er auch gespeichert werden muss. Bei Verwendung eines mit dem Zufallsgenerator erzeugten Schlüssel ist die Verwendung ohne Speichern nicht freigegeben.

Wenn Sie den Datenschlüssel zum Abschluss mit „Schlüssel benutzen“ oder mit „Schlüssel erstellen und abspeichern“ bestätigt haben, dann erscheint links in der Auswahlleiste dieses Symbol. Random Crypt ist nun bereit.

Bedienung des Formulars Dateien chiffrieren

Um einzelne Dateien zu verschlüsseln, klicken Sie dieses Symbol an. Es öffnet sich dann folgendes Fenster:



Datei auswählen, welche Sie chiffrieren möchten.

Dazu klicken Sie auf das weiße Zahnrad am rechten oberen Rand. In der Dialogbox können Sie nun die Datei auswählen.

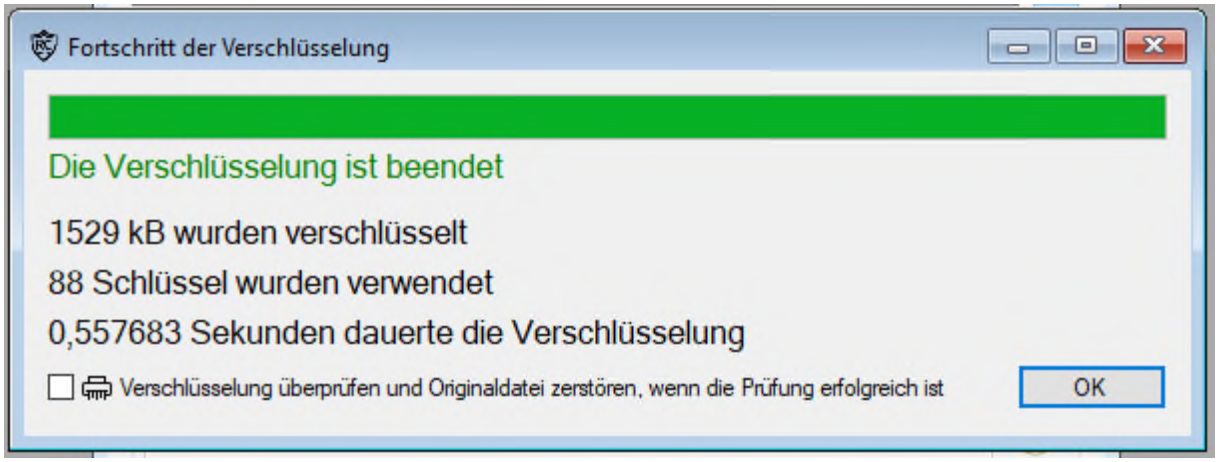
Das Chiffrat hat automatisch die gleiche Bezeichnung wie das Original, aber mit der Endung .yrc

Standartmäßig ist der Pfad für das Chiffrat eingestellt wie beim Original. Sie können Namen und Pfad des Chiffrats hier ändern.

Wenn Sie „Schlüssel erstellen oder laden“ anklicken, kommen Sie wieder auf das Formular für den Datenschlüssel.
Sie können zum Datenschlüssel eine Datei noch zusätzlich mit einem Passwort verschlüsseln. Diese Option ist hilfreich, wenn Sie untergeordnete Dateien auf Ihrem Computer haben, die auch von anderen geöffnet werden sollen, welche den gleichen Datenschlüssel haben.

Eine weitere Option ist es, dass Sie die verschlüsselte Datei mit dem Computer verknüpfen.
Das bedeutet, dass die Datei nur auf dem Rechner dechiffrieren können, auf dem sie chiffriert wurde. Da Computer erfahrungsgemäß mal kaputt gehen, wird beim ersten Mal wo Sie diese Funktion nutzen, für den Fall das Ihr Computer einen Defekt hat, eine Datei mit dem Namen C_Hash.txt erzeugt. **Bewahren Sie diese Datei gut an einem sicheren Ort auf.** Falls Ihr Computer nicht mehr funktioniert und Sie ein an den Computer verknüpftes Chiffrat wieder dechiffrieren wollen, können Sie mit Hilfe der C_Hash.txt Datei den defekten Computer auf einem anderen Computer simulieren.

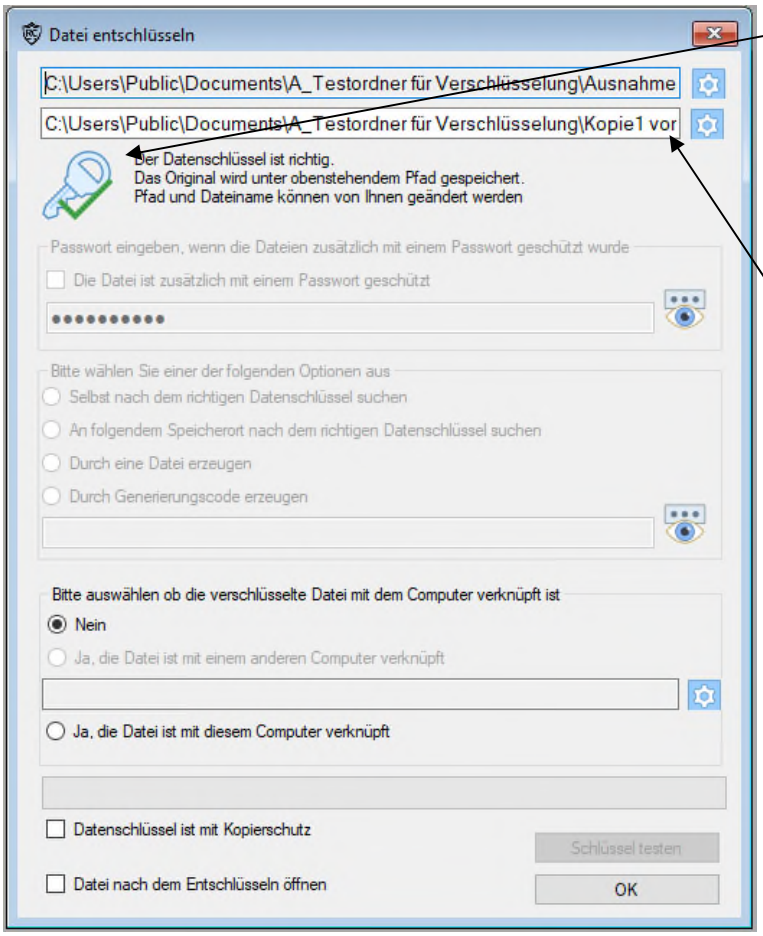
Nach erfolgreicher Chiffrierung einer Datei erscheint folgendes Fenster:



Hier erhalten Sie Informationen zur Chiffrierung der Datei. In diesem Fall wurden rund 1,5 Mb chiffriert. Wie Sie lesen können wurden dafür 88 Schlüssel verwendet. Was bedeutet das? Random Crypt chiffriert in unterschiedlich großen Blöcken. Wie groß ein Block ist wird durch die Originaldatei bestimmt. Es gibt keine feste Blockgröße. Für jeden Block wird ein neuer Schlüssel basierend auf dem vorherigen generiert. Um die maximale Sicherheit in der Verschlüsselung zu erreichen, wird mit dem Schlüssel den Sie verwenden, nicht ein einziges Byte chiffriert. Ihr Schlüssel wird nur dazu verwendet, den nächsten Schlüssel zu generieren. Wie der nächste Schlüssel dabei aufgebaut ist, ist rein zufällig. Das macht Random Crypt so besonders.
Wenn Sie mit dem gleichen Schlüssel Millionen Mal die gleiche Datei chiffrieren, dann erhalten Sie Millionen unterschiedliche Chiffrate. Und alle können mit dem einen Schlüssel wieder zum Original zurück dechiffriert werden. Das alle Chiffrate unterschiedlich sind, liegt einfach daran, dass kein Schlüssel ein zweites Mal verwendet wird. Die Zahl der möglichen Schlüsselvarianten ist einfach viel zu hoch. Testen Sie es einfach mal aus.
Unten rechts im Fenster haben Sie noch die Möglichkeit das Original nach dem chiffrieren zu vernichten. Dafür überprüft Random Crypt Byte für Byte ob die Verschlüsselung korrekt ist und überschreibt das Original danach mehrfach mit zufällig erzeugten Byte, bevor die Originaldatei gelöscht wird. Eine derart behandelte Datei lässt sich nicht wieder herstellen, auch nicht mit speziellen Programmen.

Bedienung des Formulars Dateien dechiffrieren

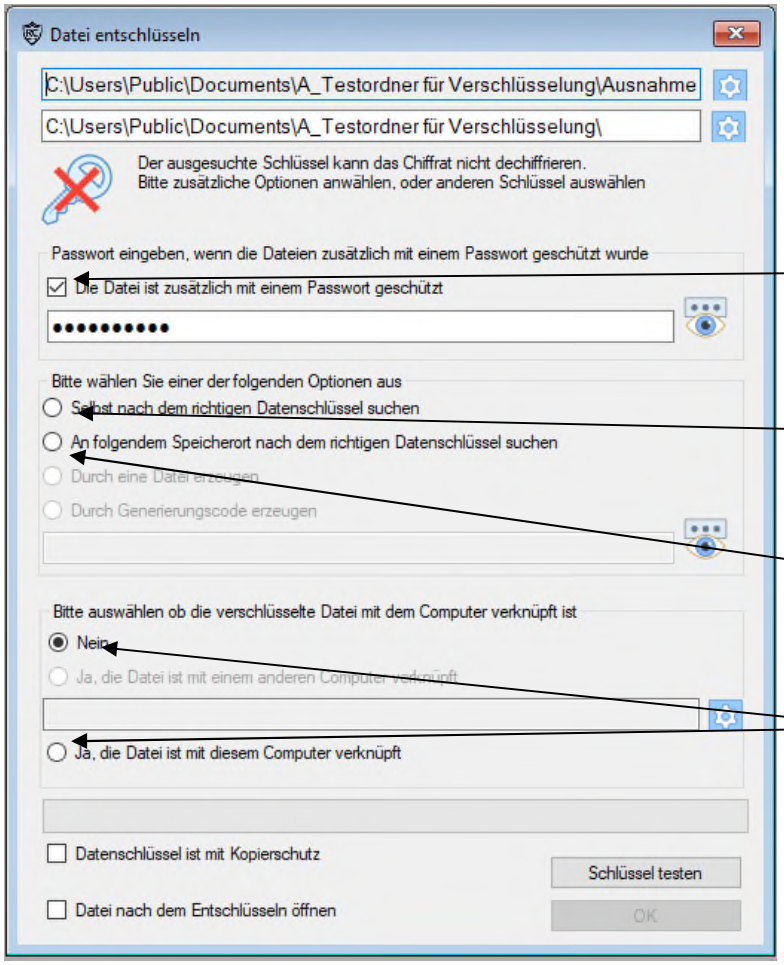
Wenn Sie hier klicken erscheint das Auswahlfenster mit dem Sie eine chiffrierte Datei auswählen können um Sie zu dechiffrieren. Nach der Bestätigung der Auswahl erscheint folgendes Fenster:



Dieses Symbol zeigt Ihnen an, ob die Datei mit dem verwendeten Schlüssel dechiffriert werden kann. Wenn es mit einem grünen Häkchen versehen ist, dann ist der geladene Schlüssel richtig und Sie können die Datei dechiffrieren.
Den Pfad und den Namen der Datei können Sie hier noch ändern.
Haben Sie keine Sorge, wenn erst einmal gesagt wird, dass der Schlüssel nicht richtig ist.
Dann erscheint das Formular wie auf der nächsten Seite dargestellt.

Sie können dann weitere Optionen für die Datei eingeben, ob sie mit einem Passwort geschützt ist, oder ob die Datei mit dem Computer verknüpft wurde.
Nach den Änderungen der Optionen können Sie testen, ob die Datei nun entschlüsselt werden kann.

Vielleicht haben Sie ja auch den falschen Schlüssel geladen. Im Formular können Sie einen anderen gespeicherten Schlüssel auswählen und laden.
Wenn das Chiffrat nicht mit einem Passwort geschützt und auch nicht mit dem Computer verknüpft ist, dann können Sie einen Speicherort auswählen, auf dem Sie Datenschlüssel gespeichert haben. Random Crypt findet dann selbstständig den passenden Schlüssel, wenn dieser sich an dem angegebenen Speicherort befindet.

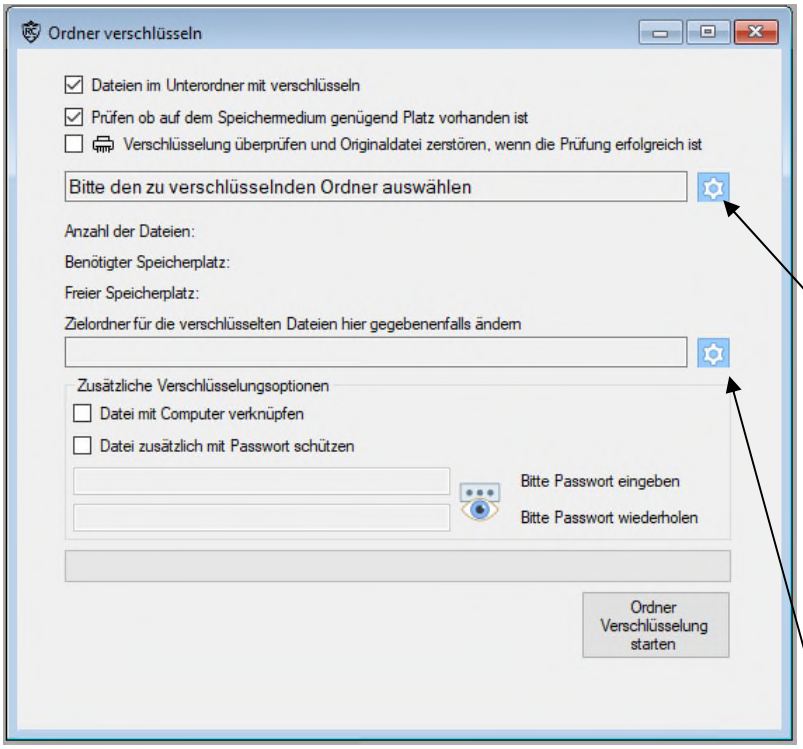


Hier sehen Sie das Formular, wenn der Schlüssel in der ausgewählten Form das Chiffrat nicht entschlüsseln kann.
Falls Sie das Chiffrat zusätzlich mit einem Passwort versehen haben, dann klicken Sie hier und geben das Passwort ein.
Sie können auch nach einem anderen Schlüssel suchen. Wenn Sie hier klicken dann müssen Sie selbst entscheiden, welches der richtige Schlüssel ist. Wenn Sie den Button hier klicken, dann können Sie den Pfad auswählen, an dem Random Crypt nach dem passenden Schlüssel suchen soll.
Hier wählen Sie aus, ob das Chiffrat mit dem Computer verknüpft ist.
Zum Abschluss noch auf „Schlüssel testen“ klicken.

Wenn der Schlüssel dann das Chiffrat dechiffrieren kann, dann sieht das Formular wie ein Bild weiter oben aus und sie können die Datei dechiffrieren.
Es ist im Chiffrat nicht gespeichert, welcher Schlüssel benötigt wird, um das Chiffrat zu dechiffrieren. Für die Überprüfung des Schlüssels auf das Chiffrat wird ein Algorithmus verwendet, der erkennen kann, ob der Schlüssel in der Lage ist das Chiffrat zu dechiffrieren. Dafür wird der Anfang dechiffriert und der Algorithmus erkennt, ob die Dechiffrierung korrekt ist. Es könnte also theoretisch möglich sein, dass ein Schlüssel als falsch positiv bewertet wird. Dieser Fall ist aber extrem unwahrscheinlich. Falsch negativ ist aber nicht möglich.

Bedienung des Formulars Ordner verschlüsseln

Wenn Sie auf diesen Button im Auswahlfeld klicken, öffnet sich das Formular für die Chiffrierung von Dateien in einem Ordner. Dies sieht dann wie folgt aus:



Die Bedienung der Elemente wie sie schon in dem Formular Dateiverschlüsselung beschrieben sind, wird hier nicht erneut erklärt. Bitte lesen Sie dazu die Verschlüsselung von Dateien.
Zuerst wählen Sie bitte hier den Ordner aus, den Sie chiffrieren möchten. Sie können auch auswählen, ob Dateien in den Unterordnern mit chiffriert werden sollen. Wenn Sie die Auswahl des Ordners durchgeführt haben, wird im Formular die Anzahl der Dateien, der benötigte Speicherplatz und der freie Speicher angezeigt.

Wenn nicht genug Speicherplatz vorhanden ist, oder Sie die Chiffrate woanders speichern möchten, dann wählen Sie hier einen anderen Speicherplatz aus.
Sie können wie bei einzelnen Dateien auch hier die Originale nach der Chiffrierung und Überprüfung der Chiffrierung von Random Crypt zerstören lassen.

Dazu ein wichtiger Hinweis!

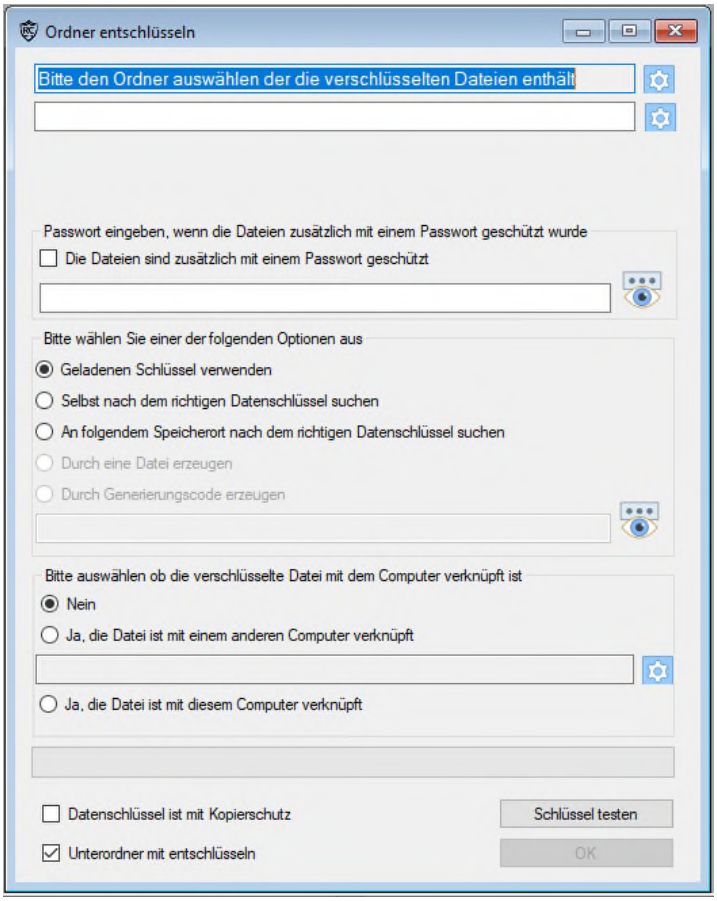
Zerstören Sie nur Dateien in Ordnern, die nicht für Ihr Betriebssystem wichtig sind. Am Besten handeln Sie, wenn Sie nur Ordner verschlüsseln und deren Inhalt zerstören, die Sie selbst erzeugt haben. Wir übernehmen ausdrücklich keine Haftung für Originaldateien, die Sie nach dem chiffrieren zerstört haben, welche für Betriebssystem oder Programme notwendig sind und diese nach der Zerstörung der Dateien nicht mehr fehlerfrei funktionieren. Auch wenn Sie die Dateien wieder herstellen können, indem Sie die Chiffrate wieder dechiffrieren, könnte der zeitweise Verlust dieser Dateien zu ungewünschtem Verhalten Ihres Computers führen.

Weitere Hinweis!

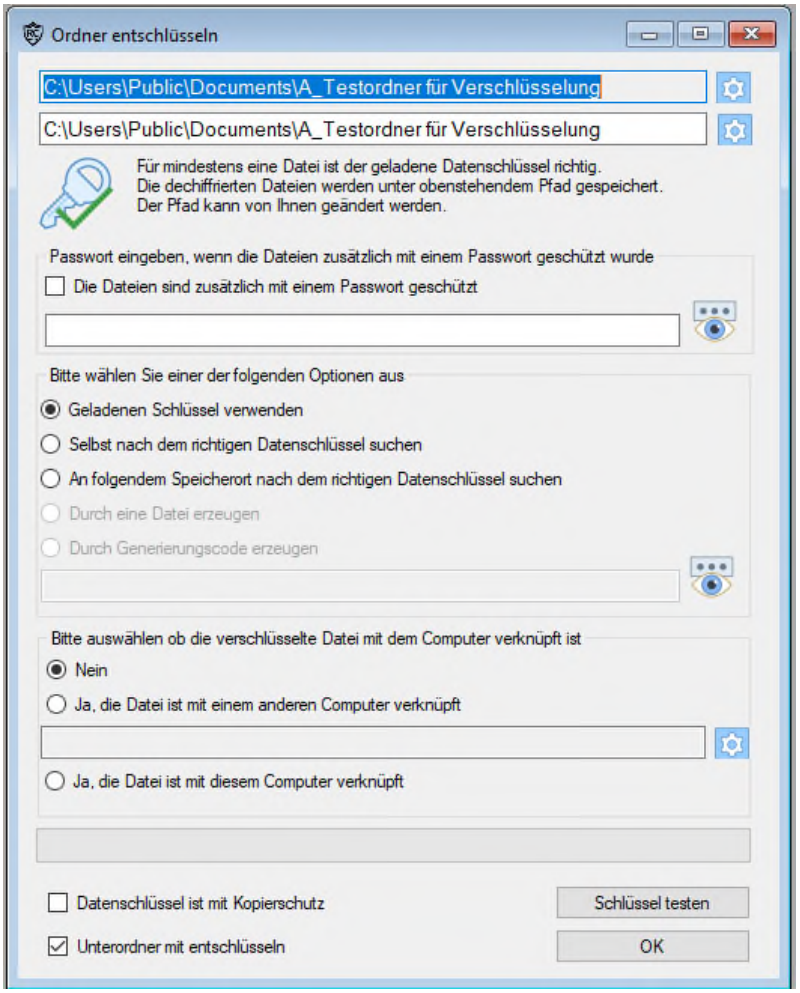
Manche Antiviren Programme sehen in dem durch Random Crypt ausgelöste Zerstörung von Dateien ein verdächtiges Verhalten. Mit Recht. Schadsoftware kann sich ebenso verhalten. In diesem Fall müssen Sie im Antivirenprogramm Random Crypt dieses Verhalten erlauben, wenn Sie die automatische Zerstörung der Originaldateien nach der Verschlüsselung wünschen. Bei der Zerstörung einer einzelnen Datei reagieren Antivirenprogramm in der Regel nicht so empfindlich.

Bedienung des Formulars Ordner entschlüsseln

Wenn Sie diesen Button im Auswahlfeld klicken, öffnet sich das Formular für die Dechiffrierung von Dateien in einem Ordner. Dies sieht dann wie folgt aus:



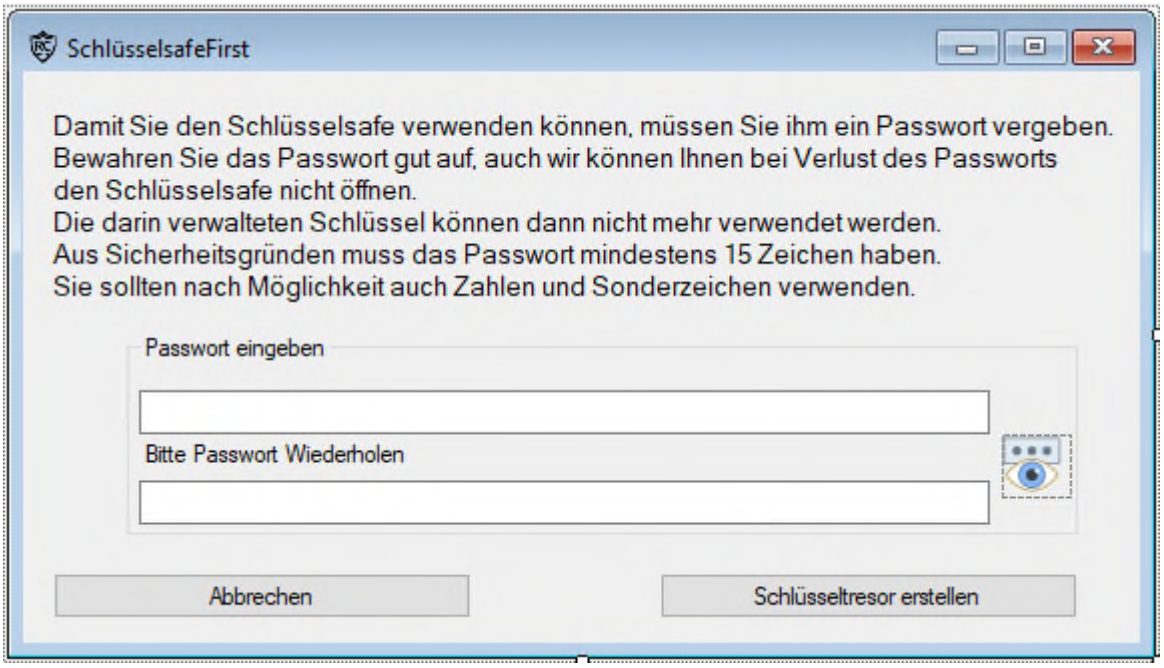
Hier können Sie den entsprechenden Ordner auswählen und wenn Sie möchten einen anderen Zielordner, in denen die Dateien entschlüsselt werden.
Außerdem können Sie wie bei dem Formular zur Dechiffrierung einzelner Dateien ein Passwort für die Chiffrate eingeben. Zusätzlich können Sie angeben, ob die Dateien mit dem Computer verknüpft sind.
Nachdem Sie die Informationen angegeben haben, können Sie testen, ob der geladene Schlüssel Dateien in dem Ordner dechiffrieren kann. Wenn dies der Fall ist, verändert sich das Formular zu folgendem Bild.



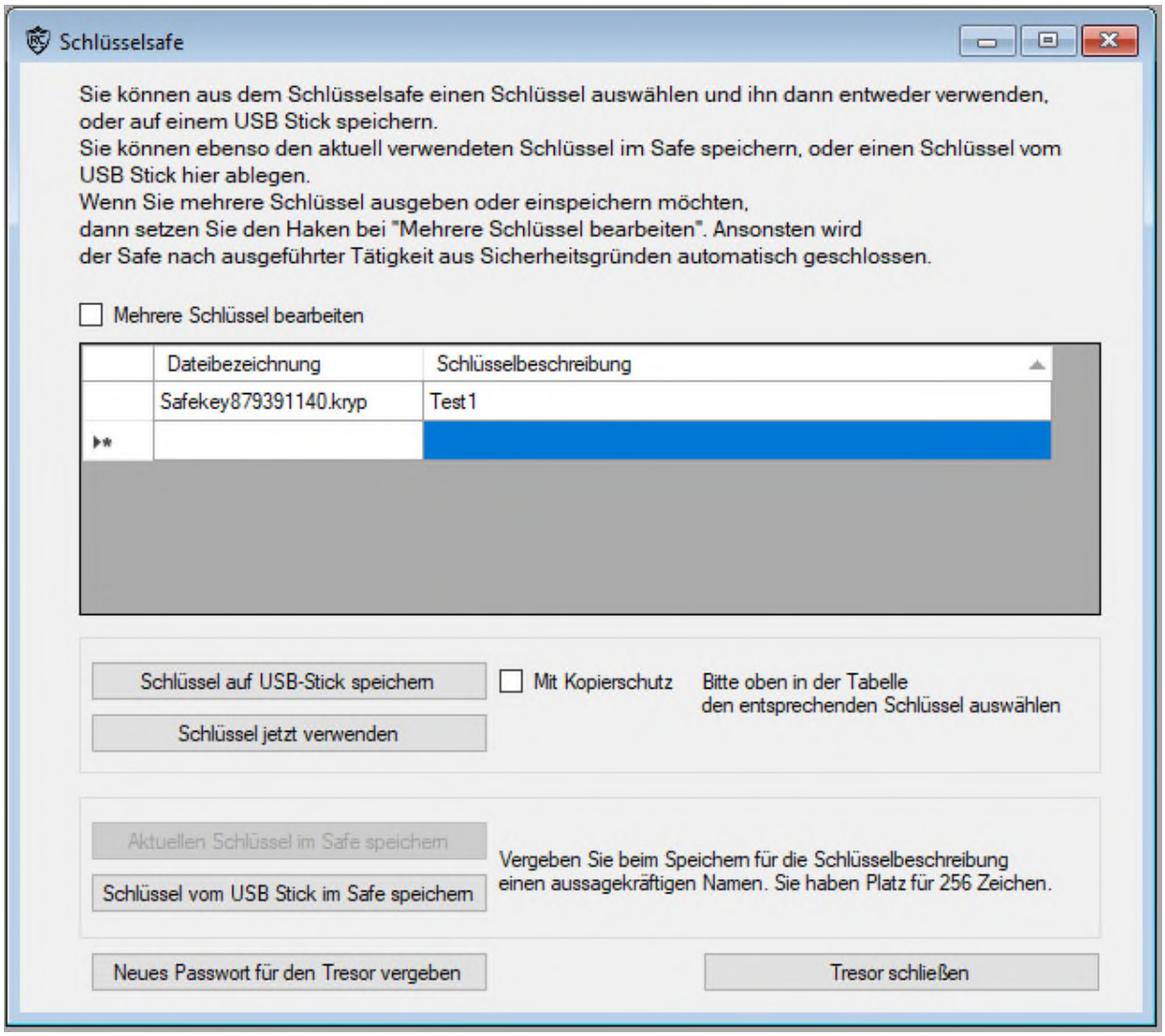
Wenn Sie den Schlüssel mit dem grünen Haken sehen können, bedeutet das, das mindestens eine Datei in dem Ordner mit diesem Schlüssel dechiffriert werden kann.
Dateien, welche nicht mit dem Schlüssel dechiffriert werden können, werden auch nicht zur Dechiffrierung aufgerufen.
Wenn Sie keinen anderen Zielordner angegeben haben, werden die Dateien im Ordner mit den Chiffraten gespeichert. Sie werden unter ihrem Originalnamen gespeichert. Wenn diese Datei schon vorhanden ist, wird die dechiffrierte Datei mit dem Zusatz Kopie versehen. Die vorhandene Datei wird nicht überschrieben.

Bedienung des Formular Schlüsselsafe

Wenn Sie auf dieses Symbol klicken erscheint beim ersten Mal folgendes Formular:



Da Sie in dem Schlüsselsafe eine unbegrenzte Zahl an Schlüssel aufbewahren können, ist der Anspruch an das Passwort etwas höher. Hier müssen Sie mindestens 15 Zeichen eingeben.
Das Passwort kann später auch geändert werden.
Das Passwort was Sie verwenden bewirkt, dass die darin enthaltenen Schlüssel durch das Passwort neu generiert werden. Diese neu generierten Datenschlüssel werden dann in dem Ordner Safe gespeichert. Mit diesen Schlüsseln kann keine Datei dechiffriert werden. Erst wenn Sie den Safe mit Ihrem Passwort öffnen, wird der ursprüngliche Schlüssel wieder hergestellt, wenn Sie ihn im Safe auswählen und kann verwendet werden. Wenn Sie Random Crypt beenden, existiert der richtige Schlüssel nicht mehr.
Der Safe ist für Nutzer gedacht, welche zum Beispiel in einem Unternehmen an mitarbeitende Personen einen Schlüssel herausgeben, (am besten mit Kopierschutz) und wenn der Schlüssel nicht greifbar ist, kann aus dem Safe der Schlüssel wieder generiert werden.
Wenn Sie das Passwort 2 eingegeben und bestätigt haben, öffnet sich der Tresor und folgendes Formular erscheint:



In diesem wurde zur einfacheren Erklärung schon ein Schlüssel gespeichert. Die Bezeichnung Safekey im Namen des Schlüssels zeigt, dass es sich hier um einen im Safe eingelagerten Schlüssel handelt. Schlüssel mit der Bezeichnung Safekey können von Random Crypt nur verwendet werden, wenn sie aus dem geöffneten Safe heraus verwendet werden.
Normalerweise schließt sich der Safe aus Sicherheitsgründen sofort, nachdem Sie eine Tätigkeit durchgeführt haben. Zum Beispiel einen Schlüssel auswählen um damit ein Dokument zu chiffrieren. Wenn Sie aber beispielsweise mehrere Schlüssel nacheinander auf USB-Stick speichern möchten, dann müssen Sie oben im Formular bei „Mehrere Schlüssel bearbeiten“ ein Häkchen setzen.
Dann bleibt der Safe solange geöffnet, bis Sie ihn selbst schließen, oder Random Crypt beenden.