

Handbuch ArchiCrypt Stega

Dok.-Nr.: ACSTG-HB-0002
Ausgabedatum: 21.05.2004
Ausgabe-Nr.: 1.2

Alle Rechte vorbehalten Weitergabe sowie Vervielfältigung dieser Unterlage, Verwertung und Mitteilung ihres Inhalts sind nur mit ausdrücklicher Zustimmung von Patric Remus erlaubt. Zuwiderhandlungen verpflichten zum Schadenersatz.

Inhalt

Teil I Einleitung	3
1 Willkommen	3
Teil II Allgemeine Informationen	3
1 Installationshinweise	3
2 Systemvoraussetzungen	3
3 Copyright	4
Teil III Bedienung	4
1 Überblick	4
2 Information	6
3 Menüleisten	7
Menü Trägerdatei	7
Menü Fenster und Dialoge	8
Menü Ansicht	8
Menü Logbuch	9
Status	9
4 Dialoge	10
Passwortdialog	10
Passwortgenerator	11
Schlüsseldiskette erstellen	13
Schlüsseldiskette einlesen	16
5 Erster Start	17
6 Beispiel	18
7 Größenverhältnisse	22
Teil IV Technischer Teil	23
1 Steganografie	23
2 Warum Verschlüsselung?	23
3 Verschlüsselung was ist das?	23
4 Eingesetzte Verfahren	24
5 Passwörter	24
6 Bewertung von Passwörtern	25

7 Sinnvoller Einsatz von Schlüsseldisketten	26
8 Angriff auf Verschlüsseltes	27
9 Hashfunktionen	28
10 Entropie	28
11 XOR	30
12 ASCII Tabelle	31
Index	32

1 Einleitung

1.1 Willkommen

Vielen Dank, dass Sie sich für ArchiCrypt Stega entschieden haben.

Reine Verschlüsselung verändert Daten so, dass Ihr Informationsgehalt nur nach Angabe eines Schlüssels zugänglich ist. Unter Steganografie versteht man Verfahren, mit denen man Informationen in Trägerinformationen derart einbinden kann, dass dieser Umstand nach außen nicht unmittelbar sichtbar wird, d.h. für Nichteingeweihte sich nur die Trägerinformationen präsentieren.

ArchiCrypt Stega verbindet die Vorzüge der Steganografie mit der Sicherheit der Kryptografie. Ein umfassender Schutz für Ihre geheimsten Informationen.

Auch der von vielen als lästig empfundene Umgang mit Passwörtern wurde von uns auf innovative Weise angegangen. Meist nutzt man Passwörter, die sehr einfach aufgebaut sind. Hat man sich ein solches Passwort gemerkt, wird es bei jeder sich bietenden Gelegenheit eingesetzt. ArchiCrypt Stega bietet Ihnen die Möglichkeit, so genannte Schlüsseldisketten einzusetzen. Dabei entfällt die Notwendigkeit, sich komplizierte Passwörter zu merken. Einfach Schlüsseldiskette einlegen und Daten ver- oder entschlüsseln. Selbstverständlich können Sie in besonders kritischen Fällen die Schlüsseldiskette mit einem Schutz versehen.

Wir wünschen Ihnen viel Spaß mit ArchiCrypt Stega

Weitere Informationen finden Sie unter www.bhv.de einsehen.

2 Allgemeine Informationen

2.1 Installationshinweise

Das Programm wird mit einer Installationsroutine geliefert, die Ihnen die Arbeit abnimmt.

Achten Sie jedoch darauf, dass Sie unter den Betriebssystemen **Windows 2000 und Windows XP** zur Installation der Software lokale Administratorrechte besitzen müssen. Sie müssen das Programm einmalig mit Administratorrechten starten.

2.2 Systemvoraussetzungen

Um ArchiCrypt Stega verwenden zu können, muss Ihr System folgende Voraussetzungen erfüllen:

- ▶ mindestens Pentium-Prozessor oder vergleichbare CPU
- ▶ mindestens 16 MB RAM; 32 MB empfohlen
- ▶ Festplatten-Platz: ca. 6 MB
- ▶ Windows 95, 98, ME, NT 4.0 oder Windows 2000 und Windows XP
- ▶ Bildschirmauflösung mindestens 640x480 bei einer Farbtiefe von mindestens 256 Farben
- ▶ Maus oder anderes Windows-kompatibles Zeigergerät

2.3 Copyright

Copyright

ArchiCrypt Stega

Copyright © 2000-2004 ArchiCrypt
Dipl.-Ing. Patric Remus
Am Brunneck 6, D-85521 Ottobrunn
Alle Rechte vorbehalten.

3 Bedienung

3.1 Überblick

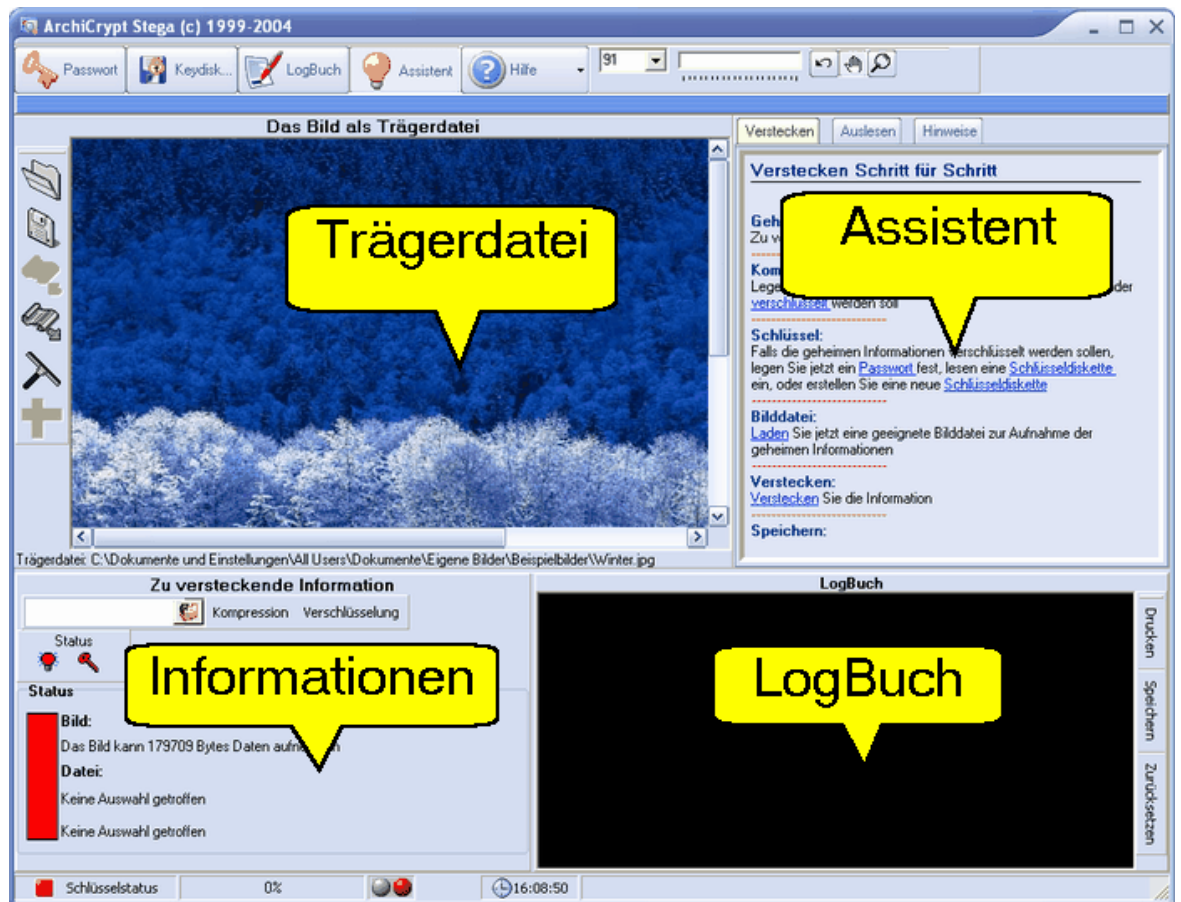
ArchiCrypt Stega

vereint die Vorzüge der Steganografie mit der Sicherheit von modernsten kryptografischen Verfahren. Durch die Steganografie werden Ihre Daten versteckt. Das heißt nur Eingeweihte wissen von der Existenz versteckter Informationen. Zusätzlichen Schutz erhalten Ihre Informationen durch eine 256 Bit Verschlüsselung. Selbst wenn es jemandem gelingen würde Ihr Versteck zu enttarnen, stünde er vor dem unlösbaren Problem, die Verschlüsselung zu brechen.

ArchiCrypt Stega bietet Ihnen die Funktionen zum Verstecken und Verschlüsseln unter einer zentralen Oberfläche.

Die wesentlichen Elemente sind:

Trägerdatei
Assistenten
Information
LogBuch
Menüleisten



Trägerdatei

Als Trägerdatei wird die Datei bezeichnet, die die zu versteckenden Informationen aufnehmen soll bzw. enthält.

Im oberen Bereich finden Sie die Anzeige für die Trägerdatei. Mittels der Trägerdatei Menüleiste können Sie eine Bilddatei laden, speichern, Informationen verstecken, auslesen, Trägerdateien säubern und an die Größe der zu versteckenden Information anpassen.

Die Ansicht der Trägerdatei können Sie mit Hilfe der Ansicht Menüleiste steuern. Sie können stufenlos zoomen und bequem in einer sehr großen Darstellung navigieren.

Assistenten

In diesem Bereich werden Sie Schritt für Schritt durch den Vorgang des Einbindens und Auslesens geheimer Informationen geleitet.

Information

Als Information werden die Daten bezeichnet, die in der Trägerdatei versteckt werden sollen. Hier finden Sie Funktionen, mit der Sie die zu versteckende Datei festlegen können und Informationen über die Kapazität der Trägerdatei und den Platzbedarf der Information. Zusätzlich können Sie Kompression und gegebenenfalls Verschlüsselung aktivieren.

LogBuch

Das LogBuch führt Buch über alle Aktionen die Sie während Ihrer aktuellen Sitzung durchführen. Sie können die Protokollierung über die Schaltfläche LogBuch an- oder abschalten.

Menüleisten

Sämtliche Funktionen und Einstellungen von ArchiCrypt Stega werden über die Menüleisten aufgerufen und eingestellt. ArchiCrypt Stega hat insgesamt 5 Menüleisten, die Sie beliebig positionieren können. Selbstverständlich merkt sich ArchiCrypt Stega die aktuellen Einstellungen.

Menüleiste Trägerdatei

Trägerdatei laden, Trägerdatei speichern, Verstecken der Information, Auslesen der Information, Säubern der Trägerdatei, Trägerdatei an Information anpassen

Menüleiste Ansicht

Trägerdatei stufenlos zoomen, letzte Änderung rückgängig machen, Handtool, Lupe

Menüleiste Fenster und Dialoge

Eingabe eines Sitzungspasswortes, Einlesen oder Erstellen einer Keydisk, Ein-/Ausschalten des LogBuchs, Hilfethemen aufrufen, Hinweise ein-/ausblenden

Menüleiste Status

Anzeige Verstecken möglich, Anzeige gültiger Sitzungsschlüssel

Menüleiste LogBuch

LogBuch drucken, LogBuch speichern, LogBuch zurücksetzen



Beachten Sie bitte, dass Trägerdateien die Informationen enthalten, unbrauchbar werden, sobald man Änderungen an ihnen vornimmt.

3.2 Information

Als **Information** werden die Daten bezeichnet, die in der Trägerdatei versteckt werden sollen. Hier finden Sie Funktionen, mit der Sie die zu versteckende Datei festlegen können und Informationen über die Kapazität der Trägerdatei und den Platzbedarf der Information. Zusätzlich können Sie Kompression und gegebenenfalls Verschlüsselung aktivieren.



Hier können Sie die zu versteckende Information festlegen (1), einstellen, ob Kompression (2) und / oder Verschlüsselung (3) vor dem Einbetten in die Trägerdatei stattfinden soll.

Sobald Sie eine Informationsdatei ausgewählt haben, wird Ihre Größe in Byte angezeigt (5a). Bei ausgewählter Kompression wird zusätzlich die Größe der komprimierten Datei angezeigt (5b). Falls Sie bereits eine Trägerdatei gewählt haben, wird hier angezeigt, wie viele Bytes die Datei

aufnehmen kann (4). Aus diesen Größenangaben wird entschieden, ob die Information in der Trägerdatei versteckt werden kann. Sie sehen dies in der Menüleiste Status sofort. Der Farbbalken (6) zeigt ebenfalls direkt an, ob die Information im Bild versteckt werden kann, oder nicht.

3.3 Menüleisten

3.3.1 Menü Trägerdatei



1. Trägerdatei laden
2. Trägerdatei speichern
3. Informationen verstecken
4. Informationen auslesen
5. Trägerdatei säubern
6. Trägerdatei anpassen

Laden und Speichern

Die Menüleiste Trägerdatei bietet Ihnen Funktionen, mit denen Sie Trägerdateien laden (1) und speichern (2) können. Als Trägerdatei können Sie Bilddateien in zahlreichen Formaten auswählen.

Zur Auswahl stehen:

JPEG Bitmap (JPG;JPEG)
CompuServe Bitmap (GIF)
TIFF Bitmap (TIF;TIFF)
PaintBrush (PCX)
Portable Network Graphics (PNG)
Windows Bitmap (BMP)
OS/2 Bitmap (BMP)
Enhanced Windows Metafile (EMF)
Windows Metafile (WMF)
Icon resource (ICO)

Verstecken

Falls Sie bereits die Datei ausgewählt haben, die Sie in der Trägerdatei verstecken möchten, und stimmen die Größenverhältnisse, können Sie mit Hilfe der Schaltfläche (3) die Daten verstecken. Falls Sie die Option "Verschlüsseln" eingeschaltet haben (siehe Information), und noch kein gültiges Sitzungspasswort vorhanden ist (siehe Status), werden Sie jetzt zur Eingabe eines Passwortes aufgefordert (siehe Passwortdialog).

Auslesen

Falls Sie sicher sind, dass in der geladenen Trägerdatei Informationen versteckt sind, geben Sie zunächst ein eventuell verwendetes Passwort ein, oder lesen Sie die notwendige Schlüsseldiskette ein (siehe Menü Fenster und Dialoge). ArchiCrypt Stega bietet Ihnen jetzt einen Dialog an, in dem Sie das Zielverzeichnis einer eventuell enthaltenen Information festlegen können. Jetzt liest ArchiCrypt Stega die Daten aus, und schreibt Sie in das angegebene Zielverzeichnis. Es wird auch immer ein Passwort abgefragt, unabhängig von dem Umstand, ob tatsächlich eine Verschlüsselung vorgenommen wurde.



WICHTIG:

Keine Hinweise auf enthaltene Daten durch ArchiCrypt Stega

ArchiCrypt Stega gibt keinerlei Rückkopplung über enthaltene Daten oder fehlerhafte Passwörter. Würde ArchiCrypt Stega anzeigen, dass Daten enthalten sind, oder bei Angabe eines falschen Passwortes eine Fehlermeldung anzeigen, könnte jeder, der im Besitz der ArchiCrypt Stega Software ist, zumindest die Anwesenheit versteckter Daten nachweisen. Falls die Datei Daten enthält und das optionale Passwort oder die

Schlüsseldiskette korrekt sind, wird im LogBuch ein Eintrag mit dem Namen der extrahierten Datei ausgegeben. Schließlich können Sie den Erfolg natürlich daran erkennen, dass die Datei in dem von Ihnen festgelegten Verzeichnis abgelegt wurde. Das auf den ersten Blick wenig benutzerfreundliche Verhalten der Software dient also lediglich Ihrem Schutz.

Säubern

Dieser Befehl (beseitigt alle Spuren aus einer Trägerdatei. Sie können den Befehl unabhängig von tatsächlich enthaltener Information aufrufen, da auch hier kein Hinweis auf enthaltene Daten gegeben werden soll (siehe oben)).

Anpassen

Falls die Trägerdatei nicht genügend Platz bietet, um die Informationen die Sie verstecken möchten aufzunehmen, können Sie mit dieser Funktion die Trägerdatei anpassen. Der zur Vergrößerung eingesetzte Filter ist sehr leistungsfähig, Sie sollten jedoch darauf achten, das Sie die Trägerdatei nicht zu stark vergrößern. (siehe auch Größenverhältnisse)

3.3.2 Menü Fenster und Dialoge



Die Schaltfläche **Passwort** ruft den Passwortdialog auf. Hier können Sie ein neues Passwort eingeben, oder mit Hilfe des Passwortgenerators ein neues Passwort nach bestimmten Vorgaben erstellen lassen.

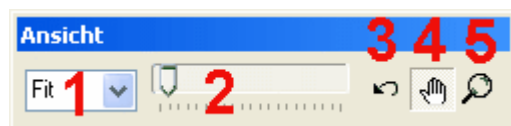
Die Schaltfläche **Keydisk** ruft den Dialog zum Einlesen und Erstellen von Keydisks/Schlüsseldisketten auf. Hier können Sie eine neue Schlüsseldiskette, auch Keydisk genannt, erstellen, oder eine bereits vorhandene Schlüsseldiskette einlesen.

Die Schaltfläche **LogBuch** schaltet das LogBuch ein oder aus. Falls die LogBuchfunktion eingeschaltet ist, ist die Schaltfläche hell hinterlegt (siehe Schaltfläche Hinweise).

Über die Schaltfläche **Hilfe** erreichen Sie ein Untermenü, mit dem Sie sich Hilfethemen anzeigen lassen können.

Die Schaltfläche **Assistent** schaltet die Assistenten an und aus.

3.3.3 Menü Ansicht



Mit Hilfe dieser Menüleiste können Sie die Ansicht der aktuell geladenen Trägerdatei beeinflussen. Im Auswahllistenfeld (1) können Sie verschiedene festvorgegebene Zoomfaktoren für die Ansicht der Trägerdatei auswählen. **Fit** passt die Darstellung so ein, dass der verfügbare Platz zur Darstellung optimal ausgenutzt wird, **100** zeigt die Trägerdatei in Originalgröße.

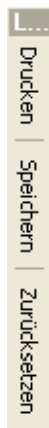
Mit Hilfe der Trackbar (2) können Sie die Trägerdatei stufenlos von 1 bis 2000 zoomen.

Durch betätigen der Schaltfläche **Rückgängig machen** (3), können Sie die letzte Aktion aufheben. Insbesondere Größenänderungen und das Einlagern von Daten kann auf diese Weise rückgängig gemacht werden.

Falls die Trägerdatei in der aktuellen Darstellung nicht in den Anzeigebereich passt, können Sie den angezeigten Bildausschnitt mit Hilfe der Scrollbalken verschieben, oder alternativ das Handsymbol (4) nutzen. Klicken Sie bei eingeschaltetem Handsymbol (hell hinterlegte Schaltfläche), auf den Bildausschnitt, halten Sie die linke Maustaste gedrückt und verschieben Sie jetzt die Maus. Der Bildausschnitt bewegt sich jetzt mit.

Falls Sie die Lupenfunktion (5) gewählt haben, können Sie die Trägerdatei mit der linken Maustaste anklicken, um hineinzuzoomen, und die rechte Maustaste, um herauszuzoomen.

3.3.4 Menü Logbuch



Sie können den Inhalt des Logbuchs speichern, ausdrucken oder zurücksetzen.

3.3.5 Status



Die Farbe des Schlüssels gibt an, ob zur Zeit ein gültiger Schlüssel geladen ist. Dabei kann es sich um ein eingegebenes Passwort oder um einen von einer Keydisk eingelesenen Schlüssel handeln.

Rot gibt an, Schlüssel ungültig, **grün** zeigt an, dass der Schlüssel gültig ist.

Die Farbe der Glühbirne gibt an, ob es möglich ist, die ausgewählte Information in der Trägerdatei zu verstecken.



Gelb gibt an, dass weder Informationsdatei, noch eine Trägerdatei festgelegt wurde.



Rot bedeutet entweder:

Trägerdatei wurde noch nicht festgelegt

Maßnahme: Laden Sie eine Trägerdatei

Informationsdatei wurde noch nicht festgelegt

Maßnahme: Laden Sie die Informationsdatei

Trägerdateikapazität nicht ausreichend zur Aufnahme der Informationsdatei

Maßnahme: Schalten Sie die Kompression ein (siehe Information)

Maßnahme: Passen Sie die Größe der Trägerdatei an (siehe Trägerdatei anpassen)

Maßnahme: Wählen Sie eine andere, ausreichend große Trägerdatei



Grün bedeutet, das die ausgewählte Information in der Trägerdatei versteckt werden kann.

3.4 Dialoge

3.4.1 Passwortdialog

Aufruf über:

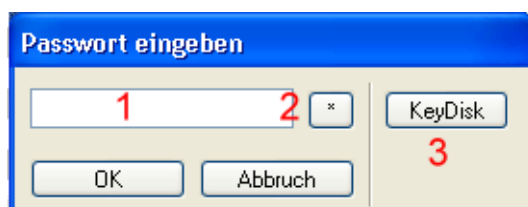
- Menüleiste Fenster und Dialoge

Es gibt zwei verschiedene Dialoge. Der Dialog zur Eingabe eines Passwortes falls eine verschlüsselte Information aus einer Trägerdatei ausgelesen, oder in diese eingelagert werden soll, und den Dialog, zur Festlegung eines neuen Passwortes für die Sitzung. Beachten Sie bitte das gesonderte Kapitel über Passwörter im technischen Teil. ArchiCrypt Stega bietet einige Besonderheiten an, um Ihre Daten umfassend zu sichern.

Sie haben es wahrscheinlich bemerkt. Sichere Passwörter haben die unangenehme Eigenschaft, dass Sie meist kompliziert sind. Man kann sie sich kaum merken. Daher wurde eine **Schnittstelle zur 1&1 Passwortverwaltung** integriert. Schlüsseldaten und Passwörter die Sie in der Passwortverwaltung mit einer Schlüsseldiskette oder einem einzigen Passwort schützen und sicher verwahren, werden dadurch ohne Tipparbeit sicher(verschlüsselt) an ArchiCrypt Stega übertragen. Der Einsatz der Passwortverwaltung ist dann sinnvoll, wenn Sie mit verschiedenen Passwörtern, Schlüsseldisketten und Benutzerdaten umgehen.

Mit ArchiCrypt Stega können Sie spezielle Zeichen in Passwörtern nutzen. Wenn Sie ein solches Zeichen eingeben wollen, leiten Sie das Zeichen bei der Eingabe durch das Zeichen \$ ein. Schreiben Sie dahinter den 2-teiligen Hex Code (siehe ASCII-Tabelle). Z.B. bedeutet: \$28 das Zeichen (.Wenn Sie das \$ Zeichen eingeben möchten, geben Sie \$\$ ein. (siehe auch Passwörter im technischen Anteil)

1. Eingabe eines Passwortes zur Entschlüsselung

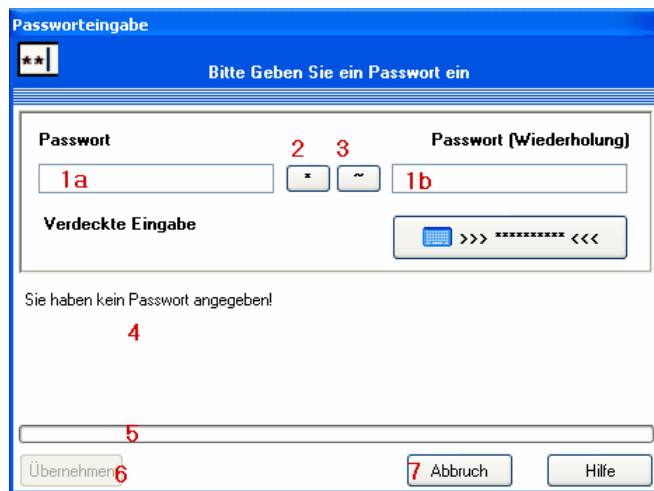


[verdeckte Eingabe des Passwortes]

Geben Sie in das Eingabefeld 1 das zum Entschlüsseln notwendige Passwort ein, betätigen Sie anschließend die <RETURN> Taste oder die Schaltfläche OK. Wenn Sie das Passwort im

Klartext sehen möchten, betätigen Sie die Schaltfläche **2**. Handelt es sich um eine Datei, die mit einer Schlüsseldiskette verschlüsselt wurde, können Sie über die Schaltfläche "KeyDisk" **3**, den Dialog zum Einlesen einer Schlüsseldiskette aufrufen.

2. Eingabe eines Passwortes zur Verschlüsselung



Der Dialog bietet die übliche Möglichkeit, das Passwort (**1a**) anzugeben. Die zweite Eingabe (**1b**) stellt sicher, dass Sie sich bei der ersten Eingabe nicht vertippt haben.

Über die Schaltfläche **2** können Sie die **Eingabe des Passwortes** in den Klartextmodus und zurück schalten.

Schaltfläche **3** ruft den Dialog für den Passwortgenerator auf.

Im Feld **4** wird in Verbindung mit der Anzeige bei **5** eine Bewertung Ihres Passwortes vorgenommen. Die Bewertung beruht auf einem mathematischen Verfahren, welches im technischen Teil beschrieben ist.

Nachdem Sie in die beiden Passwordeingabefelder das gleiche Passwort eingegeben haben, bzw. ein generiertes Passwort übernommen wurde, können Sie durch Betätigen der Schaltfläche Übernehmen **6**, das Passwort für Ihre Ver- und Entschlüsselungen nutzen. Alle ab diesem Zeitpunkt durchgeführten Ver- und Entschlüsselungen werden mit diesem Passwort durchgeführt.

Mit der Abbruch Schaltfläche **7** können Sie den Eingabevorgang abbrechen und zur ArchiCrypt Stega zurückkehren.

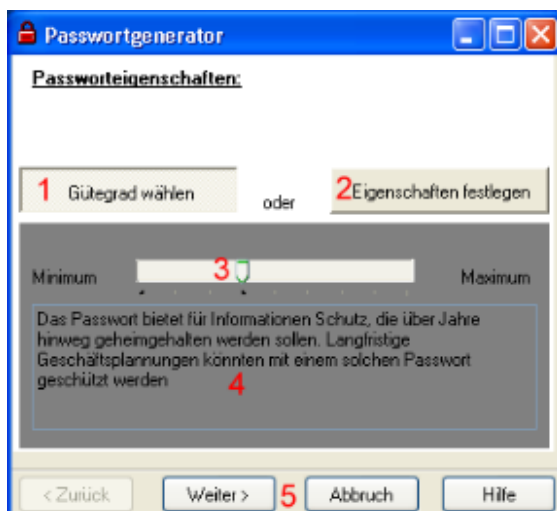
3.4.2 Passwortgenerator

Aufruf über:

- Passwortdialog

(siehe auch Passwörter, Bewertung von Passwörtern und Angriff auf Verschlüsseltes)
Der wizardbasierte Passwortgenerator generiert automatisch Passwörter nach verschiedenen Kriterien.

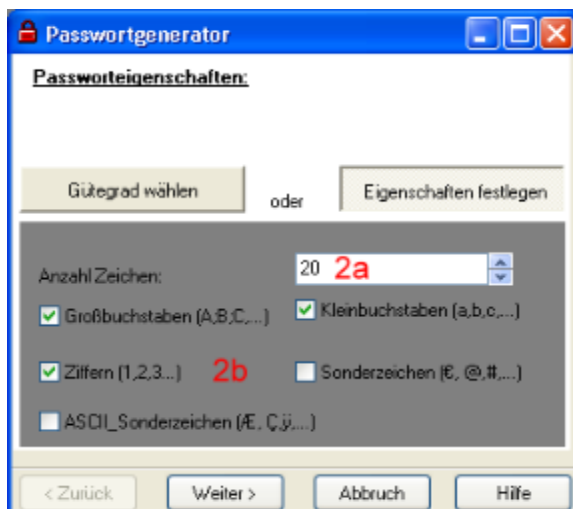
Schritt 1:



Durch die Schaltfläche **Gütegrad 1** gelangen Sie zu einem Wizard, mit dem Sie Passwörter erstellen können, die bestimmten Anforderungen genüge leisten.

Wenn Sie den Schieberegler **3** bewegen, sehen Sie, wie sich die Bewertung im Feld 4 ändert. Wählen Sie einen passenden Gütegrad und betätigen Sie die Schaltfläche Weiter.

Über die Schaltfläche **Eigenschaft festlegen 2**, übernehmen Sie die Kontrolle über das Passwort und gelangen zu einem alternativen Wizard.



Hier können Sie festlegen, wie viele Zeichen Ihr Passwort lang sein soll, ob es Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen oder ASCII_Sonderzeichen(nichtdruckbare) enthalten soll. Das Wort **soll** ist hierbei wichtig.

Betätigen Sie Schaltfläche **Weiter**.

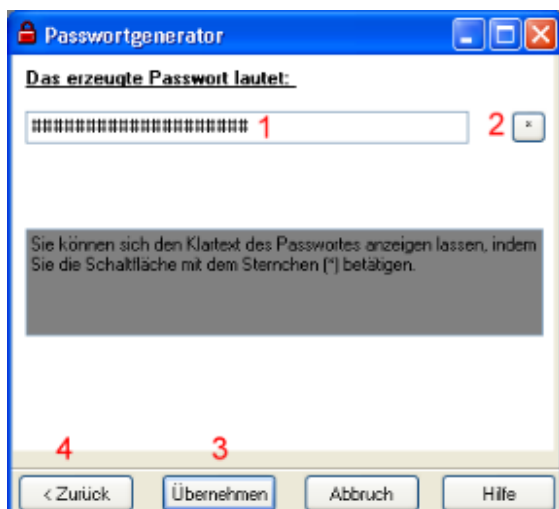
Schritt 2:

Im zweiten Schritt geht es darum Zufallsdaten zu sammeln. Bewegen Sie dazu bitte den Mauszeiger über dem Dialogfeld.

Der Fortschrittsbalken, dessen aktuelle Position mit einem roten Kreis gekennzeichnet ist, gibt an, wieviel Daten noch zu sammeln sind.



Nachdem genügend zufällige Daten vorhanden sind, schaltet die Ansicht um und das generierte Passwort wird in **1** angezeigt.



Mit der Schaltfläche **2** können Sie sich das Passwort im Klartext anzeigen lassen. Wollen Sie etwas an den Einstellungen ändern, betätigen Sie die Zurück Schaltfläche **4**, entspricht das Passwort Ihren Vorstellungen, betätigen Sie die Schaltfläche Übernehmen **3**.

3.4.3 Schlüsseldiskette erstellen

Aufruf über:

- Menüleiste Fenster und Dialoge

(siehe auch Schlüsseldiskette laden)

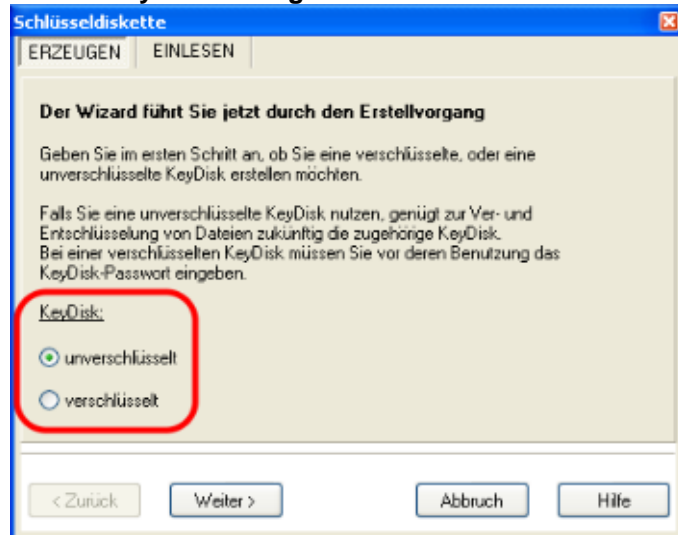
Es gibt zwei verschiedene **Arten von Schlüsseldisketten (KeyDisk)**. Eine Art ist die Schlüsseldiskette, die den Schlüssel offen, also unverschlüsselt enthält.

Die zweite Variante ist eine verschlüsselte Schlüsseldiskette. Das heißt zum Ver- und Entschlüsseln von Dateien benötigen Sie die Schlüsseldiskette und das zugehörige Passwort.

Einige Hinweise über den Umgang mit Schlüsseldisketten erhalten Sie im technischen Anteil.

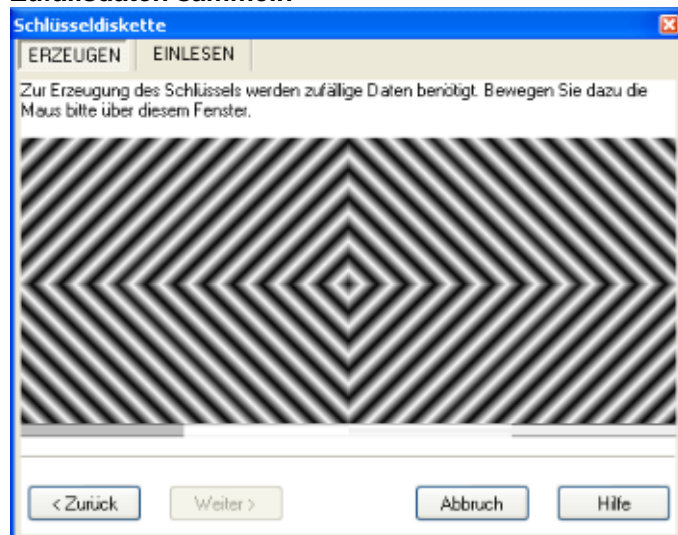
Das Erstellen erfolgt mit Hilfe eines Wizards:

Schritt 1 (beide Arten): Art der KeyDisk festlegen



Wählen Sie hier aus, welche Art von Schlüsseldiskette Sie erstellen möchten. Betätigen Sie anschließend die Weiter Schaltfläche.

Schritt 2 (beide Arten): Zufallsdaten sammeln



Zur Generierung des Schlüssels werden Zufallsdaten benötigt. Bewegen Sie den Mauszeiger über dem Dialogfenster.

Schritt 3 (nur verschlüsselte KeyDisk): Passwort festlegen

Nachdem genügend Zufallsdaten gesammelt wurden, erscheint automatisch der Dialog zur

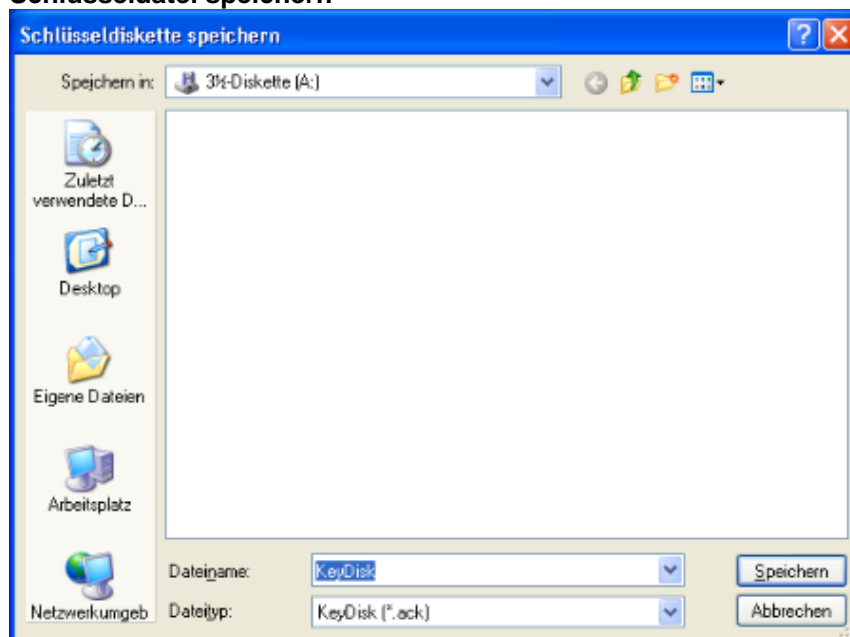
Passworteingabe.

Schritt 4 (nur verschlüsselte KeyDisk): Zeitliche Gültigkeit festlegen



In diesem Schritt können Sie angeben, ob der Schlüssel unbegrenzt, oder innerhalb zeitlicher Grenzen gültig ist. Beachten Sie bitte, dass es sich hierbei nicht um einen tatsächlichen Schutz handelt. ArchiCrypt Stega muss zur Ermittlung des Datums auf das Betriebssystem zugreifen. Ist dort ein falsches Datum eingestellt, erkennt ArchiCrypt Stega dies nicht. Diese Option macht lediglich dann Sinn, wenn man sich oder andere vertrauenswürdige Personen daran erinnern möchten, von Zeit zu Zeit den Schlüssel zu wechseln.

Schritt 5 (beide Arten): Schlüsseldatei speichern

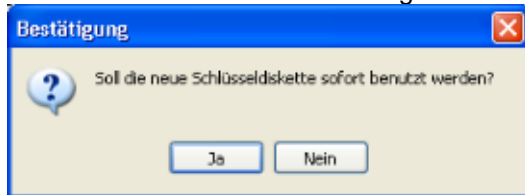


Der Dialog zum Speichern der Schlüsseldatei wird aufgerufen. Obwohl es möglich ist, sollten Sie auf keinen Fall die Schlüsseldatei auf einer Ihrer Festplatten speichern. Nutzen Sie eine Diskette oder ein anderes Wechselmedium wie z.B. einen USB-Stick.

Schritt 6 (beide Arten optional):

Nutzen der Schlüsseldiskette

Nachdem Sie die Schlüsseldatei gesichert haben erscheint der Dialog:



Beantworten Sie die Frage mit **Ja**, arbeiten Sie ab diesem Zeitpunkt mit dem Schlüssel von der Schlüsseldiskette. D.h. alle Dateien, die Sie ab jetzt verschlüsseln, können nur noch mit der Schlüsseldiskette entschlüsselt werden. Wenn Sie die Frage mit **Nein** beantworten, arbeiten Sie mit dem bisherigen Passwort oder der Schlüsseldiskette weiter.

Die erstellte Schlüsseldiskette können Sie jederzeit wie in "Schlüsseldiskette einlesen" beschrieben, eingelesen und genutzt werden.

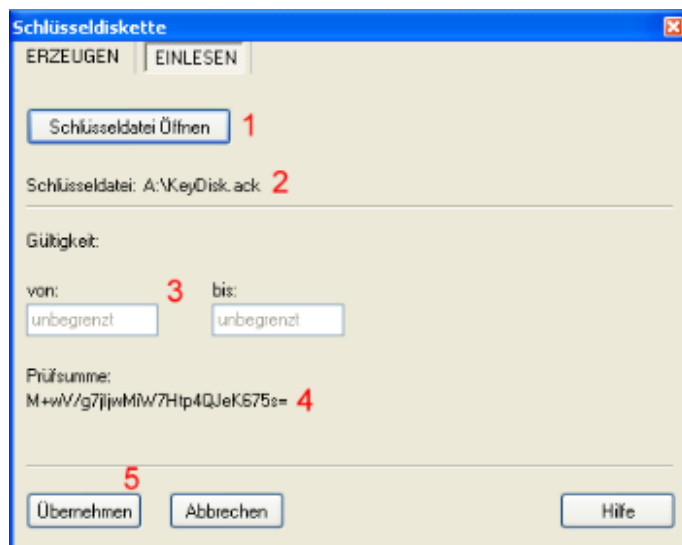
In der Passwortverwaltung verwaltete Schlüsseldisketten können ohne Medium und ohne Tipparbeit an ArchiCrypt Stega übertragen werden.

3.4.4 Schlüsseldiskette einlesen

Aufruf über:

- Menüleiste Fenster und Dialoge

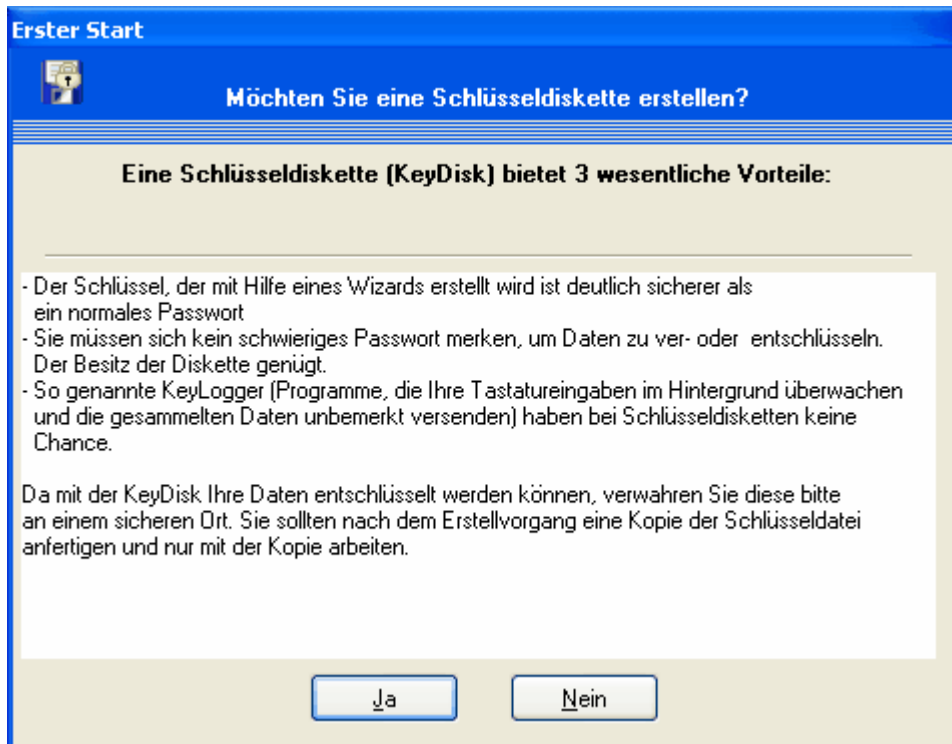
Mit dieser Funktion können Sie Schlüsseldateien laden und mit ArchiCrypt Stega verwenden.



[Dialog zum Einlesen einer Schlüsseldiskette/KeyDisk]

Mit der Schaltfläche **1** erreichen Sie den Datei Öffnen Dialog. Wählen Sie im Dialogfenster die Schlüsseldatei aus und bestätigen Sie Ihre Wahl durch das Betätigen der Schaltfläche Öffnen.

ArchiCrypt Stega bietet Ihnen beim ersten Start an, eine Schlüsseldiskette mit Ihnen zu erstellen. Sie sollten diese bequeme Art nutzen und den Anweisungen entsprechend vorgehen. Um näheres über Schlüsseldisketten zu erfahren, können Sie sich zunächst unter Schlüsseldiskette erstellen, oder unter sinnvoller Einsatz von Schlüsseldisketten informieren.



Falls Sie die Frage mit "Ja" beantworten, also eine Schlüsseldiskette erstellen möchten, wird der Wizard für das Erstellen von KeyDisks aufgerufen.

Weitere Hinweise über die Bedienung des Programmes finden Sie unter Beispiele.

3.6 Beispiel

Im Nachfolgenden sind 2 Beispiele aufgeführt, die das grundsätzliche Arbeiten mit ArchiCrypt Stega aufzeigen sollen.

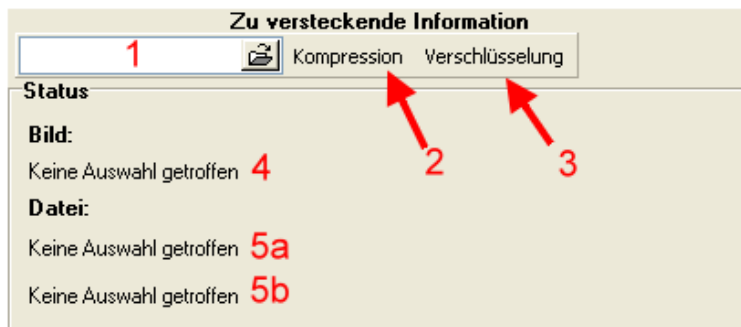
1. Verstecken einer Informationsdatei in einer Trägerdatei
2. Auslesen einer Information, die mit Passwort geschützt ist

1. Verstecken einer Informationsdatei in einer Trägerdatei

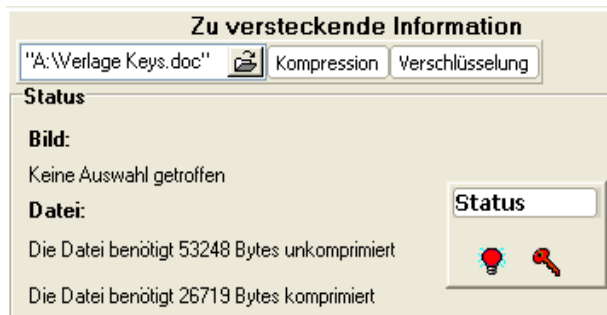
Wir wollen die Information nicht nur verstecken, sondern auch mit einer Keydisk/Schlüsseldatei verschlüsseln. Um die Trägerdatei besser auszunutzen, soll die Informationsdatei komprimiert werden.

Schritt 1:

Wir wählen zunächst die Informationsdatei aus (1):

**Schritt 2:**

Jetzt schalten wir Kompression und Verschlüsselung ein

**Schritt 3:**

Jetzt wählen wir eine geeignete Trägerdatei aus.



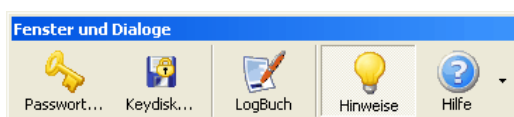
Mit (1) öffnen wir den Dialog zur Auswahl einer Trägerdatei. Falls die Trägerdatei genügend Kapazität zur Aufnahme der Informationsdatei hat, sollten Sie jetzt folgendes Bild sehen.



Falls die Glühbirne nicht grün ist, finden Sie hier geeignete Hinweise.

Schritt 4:

Jetzt lesen wir eine Schlüsseldiskette/Keydisk ein:



Betätigen Sie dazu die Schaltfläche Keydisk... und lesen Sie eine Schlüsseldiskette ein. Falls Sie weitergehende Informationen benötigen, sehen Sie unter Schlüsseldiskette einlesen oder Schlüsseldiskette erstellen nach.

Jetzt sollte sich folgendes Bild zeigen:

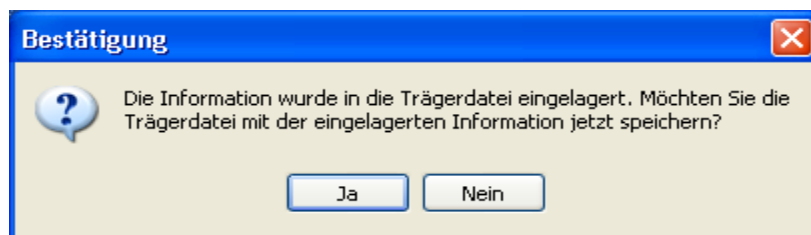


Der Status zeigt an, dass die Informationsdatei jetzt in der Trägerdatei versteckt werden kann.

Schritt 5:

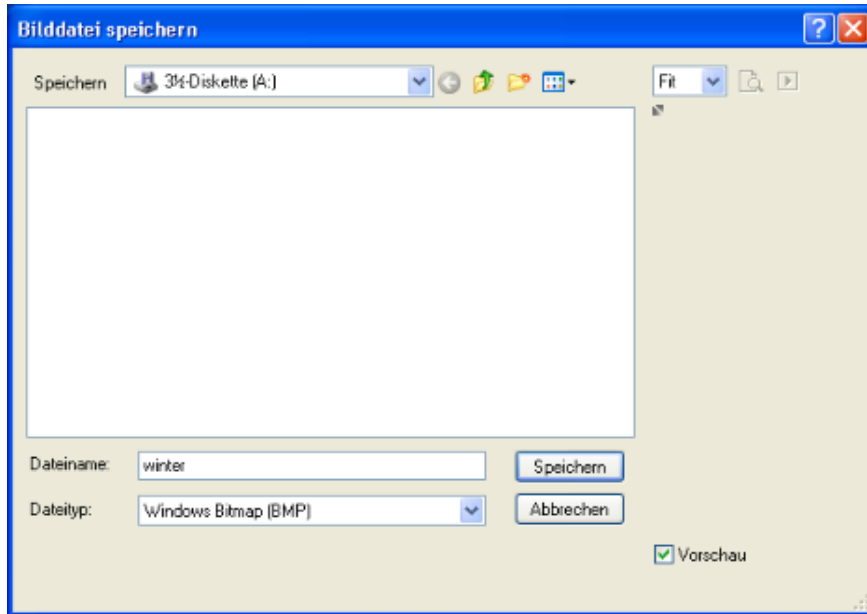


Wir verstecken die Informationsdatei indem wir die Schaltfläche (3) betätigen. Falls der Vorgang erfolgreich war, sehen Sie jetzt die folgende Meldung:



Schritt 5:

Um die Trägerdatei zu speichern betätigen Sie die Schaltfläche Ja und geben der Datei im Dialog einen geeigneten Namen.



Durch Auswahl der Schaltfläche Speichern, wird die Datei im gewählten Verzeichnis abgelegt.

2. Auslesen einer Information, die mit Passwort geschützt ist

In diesem 2ten Beispiel wollen wir eine Information die mit Passwort geschützt ist aus einer Trägerdatei auslesen.

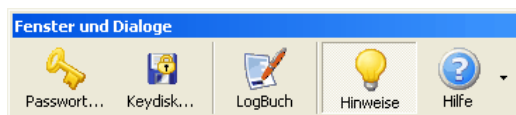
Schritt 1:

Öffnen Sie die Trägerdatei, die die Informationen enthält, welche Sie auslesen möchten. Betätigen Sie dazu Schaltfläche **1**

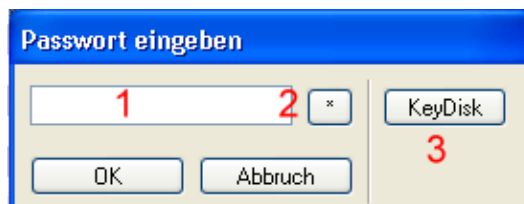


Schritt 2:

Geben Sie jetzt das Passwort ein, mit welcher die Information vor dem Einlagern zusätzlich verschlüsselt wurde. Rufen Sie dazu den Dialog zur Eingabe des Passwortes (Schaltfläche **Passwort...**) auf (siehe auch Fenster und Dialoge).



und geben dieses in das Eingabefeld (**1**) ein (siehe auch Passwortdialog).



**WICHTIG:**

Es wird grundsätzlich ein Passwort erwartet, unabhängig davon, ob die Daten beim Verstecken verschlüsselt wurden oder nicht. Falls die Daten beim Verstecken nicht verschlüsselt wurden, betätigen Sie die Schaltfläche **Abbruch.**

Schritt 3:

Die Statusanzeige:



Die Glühbirne sollte Rot oder grün sein, der Schlüssel muss grün sein.

Betätigen Sie jetzt die Schaltfläche (4) zum Auslesen der Informationsdatei



In einem Dialog müssen Sie jetzt ein Zielverzeichnis angeben, in welches die Information gespeichert werden soll.

Falls es sich um die korrekte Trägerdatei gehandelt hat und das Passwort korrekt war, wird die enthaltene Informationsdatei im Zielverzeichnis gespeichert. Wenn Sie das Logbuch eingeschaltet haben, erhalten Sie einen Hinweis auf die erfolgreiche Extraktion.

WICHTIG:

Beachten Sie bitte, dass ArchiCrypt Stega aus Sicherheitsgründen keine Indikatoren hat, die anzeigen, ob eine Trägerdatei tatsächlich Informationen enthält. Es erfolgt auch kein Fehlerhinweis auf ein eventuell fehlerhaftes Passwort.

3.7 Größenverhältnisse

Die Trägerdatei und die Informationsdatei sollten hinsichtlich Ihrer Größe geeignet ausgewählt werden. Es ist sicherlich klar, dass ein Bild, welches zum Beispiel 20 Kilobyte groß ist, keine Datei aufnehmen kann, die selbst 20 Kilobyte groß ist.

Das Trägerbild sollte ca. um den Faktor 8 größer sein, als die zu versteckende Datei. Durch spezielle Verfahren können Sie bei ArchiCrypt Stega allerdings etwas von dieser Vorgabe abweichen. ArchiCrypt Stega erlaubt es, Daten vor dem Verstecken zu komprimieren. Eine mächtige Filterfunktion erlaubt es Ihnen auch, die Trägerdatei innerhalb physikalischer Grenzen so zu vergrößern, dass die Aufnahmekapazität gesteigert und die Klarheit des Bildes annähernd erhalten bleibt. Da nicht jede Datei gleich gut komprimiert werden kann, kann man an dieser Stelle keine allgemeingültige Aussage über die Größe machen. Sie sollten ein wenig experimentieren.

4 Technischer Teil

4.1 Steganografie

Steganografie bedeutet so viel wie "verdecktes Schreiben" und bezeichnet die Wissenschaft vom Verstecken von Daten.

Steganografische Verfahren oder Algorithmen betten vertrauliche Nachrichten in andere, umfangreichere Nachrichten (Trägermedien) ein. Durch das Einbetten in ein Trägermedium entsteht ein so genanntes Steganogramm, aus dem der Empfänger die Nachricht wieder extrahieren kann.

Ein Angreifer soll Steganogramme und Trägermedien aber möglichst nicht erkennen können, so dass er weder die vertrauliche Nachricht erfährt noch den Umstand, dass etwas eingebettet wurde.

Die Einbettung, der Umstand also, dass etwas eingebettet wurde, kann mit speziellen Verfahren nachgewiesen werden (statistische und visuelle Verfahren). Aus diesem Grund verknüpft ArchiCrypt Stega Steganografie mit Kryptografie (Verschlüsselung).

4.2 Warum Verschlüsselung?

Weil es wirklich niemanden etwas angeht, was Sie an Daten auf Ihrer Festplatte haben. Weder Ihren Mann/Ihre Frau, noch den Sohn/Tochter/Vater oder den Internetprovider, den Anbieter Ihres Mailservers, den Hacker, Ihren Konkurrenten oder den Staat.

Jedes Dokument auf Ihrer Festplatte gibt einem Außenstehenden tiefen Einblick in Ihre Privatsphäre. Versicherungsart, -nummer, Bankverbindungen, Finanzdaten, Kundendaten, Firmeninterna, Liebesbriefe, Bilder etc.

Sobald die Verbindung zum Internet aufgebaut ist, besteht die nicht zu unterschätzende Chance, dass nicht nur Sie Zugriff auf Ihre Daten haben. Die bequeme Möglichkeit Dokumente und beliebige Dateien als Anhang einer Email zu versenden ist grandios und birgt gleichzeitig ungeheure Gefahren. Im privaten Bereich kann es um die eigene Existenz gehen, im beruflichen Alltag um eine Firma. Schnell ist die "Senden Schaltfläche" betätigt und das Dokument im unkontrollierbaren digitalen Raum.

Sensible Daten, sollten während einer Surfession nicht unverschlüsselt auf Ihrem Rechner sein. Gelangen verschlüsselte Daten in unbefugte Hände, kann dieser nichts damit anfangen, sofern Sie gewisse Grundregeln einhalten.

Man sollte sich allerdings darüber im Klaren sein, dass es eine absolute Sicherheit nicht gibt. Auch die besten und ausgefeiltesten Tools können an diesem Umstand nichts ändern.

Verspricht Ihnen ein Hersteller etwas anderes, ist er unseriös.

4.3 Verschlüsselung was ist das?

Verschlüsselungsverfahren sind immer dann gefordert, wenn es darum geht, vertrauliche Informationen über unsichere Informationskanäle zu übertragen. Die Information wird dabei vor der Übertragung vom Sender verschlüsselt und nach der Übertragung vom Empfänger der Information entschlüsselt.

Man unterscheidet dabei grundsätzlich zwei Verfahren. Das **symmetrische Verfahren**, bei welchem Sender und Empfänger den gleichen Schlüssel nutzen und das **asymmetrische Verfahren**, bei dem man für das Ver- und Entschlüsseln unterschiedliche Schlüssel nutzt. Bei asymmetrischen Kryptographie-Techniken wird mit einem öffentlich zugänglichen, nicht geheimen Code, dem so genannten öffentlichen Schlüssel („public key“) und einem privaten Schlüssel („private key“) gearbeitet.

Eine Kombination aus beiden Verfahren wird als **Hybrid-Codierung** bezeichnet.

Kryptologie ist wörtlich die „Wissenschaft der Verschlüsselung“ und basiert auf mathematischen Algorithmen, die man heutzutage in Software umsetzt.

Im alten Rom wurde ein extrem simples Verfahren verwendet, welches darin bestand, jeden Buchstaben „X“ der Nachricht durch einen anderen Buchstaben zu ersetzen, der sich aus einem bestimmten Abstand „X+n“ zu dem Original ergibt. So wurde z. B. aus einem „A“ ein „C“, aus „B“ ein „D“, aus „C“ ein „E“, usw. Diese Methoden sind noch schwächer als die s.g. XOR-Verschlüsselung.

4.4 Eingesetzte Verfahren

ArchiCrypt Stega setzt zur Verschlüsselung das sehr bekannte Verfahren Blowfish ein. Blowfish ist frei verfügbar und neben AES der wahrscheinlich am besten untersuchte symmetrische Verschlüsselungsalgorithmus, der bisher keine Schwachstellen zeigt. Nähere Informationen erhalten Sie, indem Sie in einer der zahlreichen Suchmaschinen im Internet den Begriff Blowfish eingeben, oder direkt zur Internetseite seines Erfinders wechseln:

- [Blowfish](#) - Bruce Schneier

Das Verfahren ist als Referenzimplementierung in der Programmiersprache C frei verfügbar.

siehe auch **Steganografie**

4.5 Passwörter

Passwörter werden meist als Schlüssel oder als Ausgangspunkt für eine Schlüsselberechnung genutzt. Sie sind quasi der Schlüssel zum Schloß, welches unsere Daten vor unbefugtem Zugriff schützt. Es ist sicher einleuchtend, dass es auf zwei Dinge ankommt. Die Methode (Algorithmus) die zur Ver- und Entschlüsselung genutzt wird und das Passwort müssen sicher sein. Was nutzt die beste Methode wenn Sie als Passwort den Buchstaben A wählen. Was nutzt das beste Passwort, wenn Sie als Methode eine XOR-Verknüpfung wählen.

Wörter, die Sie auf keinen Fall als Passwort benutzen sollten:

Sie sollten keinesfalls Geburtsdaten, Namen, Hobbies, Lieblingsverein, usw. Die Passwörter entstammen in diesen Fällen Ihrem sozialen Umfeld. Einem Angreifer der sich über Ihre Lebensumstände, Ihre Vorlieben etc. informiert, fällt es leicht auf die Lösung zu kommen.

Wörterbücher:

Vermeiden sollten Sie auch lexikalische Begriffe. Ein Wörterbuch enthält um die 120.000 Einträge. Für einen Angreifer ist es leicht die 120.000 Wörter mit Hilfe eines Computers in wenigen Sekunden zu testen. Um aus diesem Fundus dennoch zu schöpfen, müssten Sie ein Passwort bilden, welches aus ca. acht Einzelworten mittlerer Länge besteht (siehe auch Bewertung von Passwörtern).

Zahlen als Passwort:

Zahlen sind verlockend. Aber höchst gefährlich, wenn man das Passwort ausschließlich aus Ziffern aufbaut. Geben Sie in ArchiCrypt Stega ein Passwort ein und achten Sie auf die Bewertung (siehe Passworteingabe). Um ein einigermaßen sicheres Passwort zu erhalten müssen Sie sich sehr viele Ziffern merken. Leider sind es 77 Ziffern, die sich merken müssen, um ein Maximum an Sicherheit aus ArchiCrypt Stega herauszuholen.

Um dennoch die Sicherheit der Methoden zu nutzen, wurde eine **Schnittstelle zur 1&1 Passwortverwaltung** geschaffen. Schlüsseldaten und Passwörter die Sie in der Passwortverwaltung mit einer Schlüsseldiskette oder einem einzigen Passwort schützen und sicher verwahren, werden dadurch ohne Tipparbeit sicher(verschlüsselt) an ArchiCrypt Stega übertragen.

Zeichen der Tastatur als Passwort:

Wir haben dann 26 Groß- und 26 Kleinbuchstaben, 10 Ziffern und 42 Sonderzeichen zur Verfügung. Sie müssen sich nur noch ca. 38 Zeichen merken. Es ist allerdings schwierig, sich solche Monstren zu merken. Man kann eigene Methoden zur Passwortgenerierung entwickeln. Man schreibt sich einen genügend langen Satz auf, den man sich gut merken kann. Darunter eine Ziffernfolge die man sich merken kann. Vom Satz behalten Sie nur noch die Anfangsbuchstaben der Einzelworte bei. Alle 2 oder drei Buchstaben schreiben Sie jetzt eine Ziffer im Wechsel mit einem beliebigen Sonderzeichen auf. Merken müssen Sie sich diese Monstren allerdings immer noch. Abhilfe schafft gegebenenfalls die Schlüsseldiskette.

Sichere Passwörter:

Ein für ArchiCrypt Stega mit Blowfish sicheres Passwort (genauer gesagt ein Schlüssel) besteht aus 32 zufälligen Zeichen aus dem ASCII-Bereich (siehe ASCII-Tabelle). Zur Speicherung eines Zeichens wird ein Byte verwendet. Bekanntlich besteht ein Byte aus 8 Bit. Mit diesen 8 Bit kann man 2^8 verschiedene Zeichen erzeugen. Das sind 256. Genau aus diesen 256 Zeichen besteht die ASCII-Tabelle, die zahlreiche Zeichen enthält, die Sie nicht auf Ihrer Tastatur finden. Wie wir oben gesehen haben, können Sie über die Tastatur lediglich 104 Zeichen nutzen. Einem Angreifer machen Sie so das Leben leicht, da er sich auf diese Zeichen beschränken kann. Mit der speziellen Möglichkeit bei ArchiCrypt Stega, können Sie den gesamten Bereich der ASCII-Tabelle nutzen.

4.6 Bewertung von Passwörtern

Das Passwort kann Zeichen aus einem bestimmten Vorrat nutzen. Der Vorrat hat dabei eine begrenzte Zahl an Zeichen. Die Bewertung des Passwortes folgt dabei dem folgenden Schema:

Länge des Passwortes * log(Anzahl Möglicher Werte)

wobei Log der Logarithmus zur Basis 10 ist.

Wählen Sie zum Beispiel ein Passwort der Länge 10, welches lediglich aus Ziffern besteht, erhalten Sie einen Wert von

$$10 * \log(10) = 10$$

ArchiCrypt Stega hat die verfügbaren Zeichen in Gruppen aufgeteilt:

- Gruppe Großbuchstaben
- Gruppe Kleinbuchstaben

- Gruppe Ziffern
- Gruppe Sonderzeichen (auf Tastatur verfügbar)
- Gruppe ASCII Zeichen (nicht auf Tastatur) (hierzu siehe auch ASCII-Tabelle und Passwörter)

Während Ihrer Eingabe wird jetzt geprüft, aus welcher Menge Ihrer Zeichen stammen und wie lange das eingegebene Passwort ist. Die Texte, die Sie als Bewertung vorfinden, stammen aus "[Angewandte Kryptographie](#)" von Bruce Schneier

Die Aussagen beziehen sich auf Informationstypen, Informationen, die nach einem bestimmten Zeitraum Ihre Geheimhaltungsbedürftigkeit verlieren. Für die unterschiedlichen Informationstypen, werden jetzt Mindestschlüssellängen gefordert. Das Ergebnis obiger Gleichung wird nun mit genau dieser Mindestforderung verglichen. Die Schlüssellänge ist nur dann ein Maß, mit dem man verschiedene Verschlüsselungsalgorithmen vergleichen kann, wenn alle Methoden optimale Methoden sind. D.h. die beste Variante die Methode zu knacken muss die **Brute Force** Methode sein. (siehe auch Angriff auf Verschlüsseltes)

4.7 Sinnvoller Einsatz von Schlüsseldisketten

Was ist eine Schlüsseldiskette?

Eine Schlüsseldiskette steht stellvertretend für ein beliebiges Wechselmedium. Nehmen Sie den Begriff Diskette bitte keinesfalls wörtlich!! Eine Diskette zu nutzen ist, wegen der Anfälligkeit, sogar gefährlich. Eigentlich ist der Schlüssel bzw. die Schlüsseldatei nur 256 Byte groß und belegt auf der Diskette nur 1 Kilobyte.

Beim Erstellen der Schlüsseldiskette werden Zufallsdaten gesammelt. Um wirklich zufällige Daten zu erhalten, ist Ihre Mithilfe erforderlich. Die Bewegungen des Mauszeigers liefern Werte, aus denen mit Hilfe bestimmter mathematischer Verfahren geeignete Zufallsdaten gesammelt werden. Der Computer selbst ist nicht in der Lage, wirklich zufällige Daten zu erzeugen. Sie würden sich auch beschweren, wenn es anders wäre. Ein vorhersagbares Verhalten ist Grundvoraussetzung für einen produktiven Einsatz des Rechners.



Tipp: Nehmen Sie den Begriff Schlüsseldiskette nicht zu wörtlich! Selbstverständlich können Sie die Datei, welche den Schlüssel enthält (ca. 1 Kilobyte groß), auch auf einem USB-Stick, einer CD/DVD oder anderen Medium ablegen. Da Disketten sehr anfällig gegenüber Umwelteinflüssen sind, sollten Sie auch unbedingt auf ein Alternativmedium zurückgreifen.

Für wen eignet sich eine Schlüsseldiskette?

Schlüsseldisketten sind besonders für all jene geeignet, die es leid sind, sich Passwörter zu merken oder diese umständlich einzutippen.

Besonders gut geeignet ist diese Methode auch für kleinere Teams, die miteinander kommunizieren und Daten austauschen. Dazu sollte bei einem der ersten Meetings der Besprechungspunkt Datenaustausch mit auf die Tagesordnung gesetzt werden. Für jeden Teilnehmer sollte jetzt eine Diskette mit identischem Schlüssel bereit liegen. Ein paar einleitende Worte über die Wichtigkeit des sicheren Datenaustausches und den richtigen Umgang mit der Schlüsseldiskette schließen diesen Punkt ab.

Wie sollte man mit der Schlüsseldiskette umgehen?

Lassen Sie die Diskette bitte nur so lange im Laufwerk, bis Sie den Dialog zum Einlesen der Schlüsseldatei verlassen haben.

Fertigen Sie bitte von jeder Schlüsseldiskette Sicherungskopien an. Wird Ihre Schlüsseldiskette versehentlich überschrieben, sind alle damit verschlüsselten Daten verloren.

Verwahren Sie die Disketten (Backup und Original) an einem sicheren Ort auf.

4.8 Angriff auf Verschlüsseltes

Zuverlässige Kryptographie-Verfahren sollten fast unmöglich zu knacken sein. Der Aufwand für einen hochwertigen Algorithmus muss im Übrigen nicht unbedingt höher sein als für eine weniger effektive Lösung. Verfolgt man keine besondere Strategie, um einen Code zu knacken, muss man notfalls jede erdenkliche Kombinationen durchprobieren, bis man zufällig (siehe auch Entropie)-irgendwann die Lösung findet. Mit steigender Codelänge wächst zwar die benötigte Rechenzeit exponentiell, doch alle 18 Monate verdoppelt sich gemäß **Moore'schen Gesetz** die Performance der jeweils aktuellen Rechner. Für einen 56-Bit-Schlüssel benötigt man bereits ein Computernetzwerk. 64- bis 80-Bit-Schlüssel sind vorerst nur von wenigen Staaten und Institutionen zu knacken, so dass man einen 128-Bit-Schlüssel zurzeit als sicher einstuft.

Aus der Länge des Schlüssels kann man nur ableiten, wie viele Versuche ein potentieller Angreifer im ungünstigsten Fall unternehmen muss um den Code zu brechen. In der Regel werden sehr viele solche Kombinationen durchgerechnet, bevor der Code gebrochen ist. Eine Methode, die sich mittels Brute-Force innerhalb einer Woche knacken lässt, kann auch schon zufällig nach drei oder vier Tagen, in Ausnahmefällen auch innerhalb eines Tages - aber nur mit sehr niedriger Wahrscheinlichkeit - entschlüsselt sein. Wie man sieht, ist die bloße Länge des Schlüssels nicht der einzige Garant für hohe Sicherheit. Wurde der Schlüssel aus einer Zufallssequenz abgeleitet und wurde diese Sequenz nur „pseudo“-zufällig erzeugt, so kann auch ein vergleichsweise langer Schlüssel brechbar sein, wenn sich die Regel, nach der er errechnet wurde, ermitteln lässt. ArchiCrypt Stega nutzt daher Ihre Mausbewegungen zur Erzeugung eines **Zufallszahlenpools**.

Ein kryptografisches Verfahren gilt als sicher, wenn die beste Methode ohne Schlüssel an die Daten zu gelangen die s.g. Brute-Force-Methode ist. D.h. man testet jeden möglichen Schlüssel.

Im Falle von ArchiCrypt Live wird die besonders sichere AES Implementierung mit einer 256 BIT Schlüssellänge. Im schlechtesten Fall muss ein Angreifer 2^{256} verschiedene Schlüssel testen, bis er den richtigen Schlüssel findet.

Dies ergibt ca. $1,1579208923731619542357098500869e+77$ verschiedene Schlüssel. Geht man davon aus dass ein Rechner 1000000 (1 Million) Schlüssel pro Sekunde durchtesten kann, bleiben

$1,1579208923731619542357098500869e+71$ Sekunden

$1,9298681539552699237261830834781e+69$ Minuten

$3,2164469232587832062103051391302e+67$ Stunden

$1,3401862180244930025876271413043e+66$ Tage

$3,6717430630808027468154168254911e+63$ Jahre

Sie sehen also, dass es recht lange dauern kann, bis man auf diese Art an die geheimen Informationen kommt.

Es gibt auch interessante Berechnungen darüber, ob die Masse der Erde ausreicht ($E=m \cdot C^2$), um die bei den Berechnungen nötigen Energiemengen aufzubringen.

4.9 Hashfunktionen

Eine **Hashfunktion** ist eine Funktion, die eine Eingabe beliebiger Länge erhält und einen Funktionswert, den so genannten Hashwert liefert. Dieser Hashwert hat eine vorgegebene Länge. Die Funktion die bei ArchiCrypt Stega zum Einsatz kommt heißt SHA 1 (Secure Hash Algorithm 1) und liefert einen Hashwert der Länge 160 Bit.

Im kryptographischen Umfeld kommen nur Hashfunktionen zum Einsatz mit denen es möglich ist, einen Hashwert zu einer Eingabe zu ermitteln. Eine Berechnung der Eingabe aus dem Hashwert hingegen ist unmöglich. (Diese Eigenschaft wird auch als **Einweg-Eigenschaft** bezeichnet, Funktionen mit dieser Eigenschaft als **Einweg-Hashfunktionen**.)

Die Anforderungen reichen weiter: Die Funktion muß öffentlich sein, d.h. jeder muss Zugriff auf die Funktion haben. Weiterhin soll es unmöglich sein, 2 unterschiedliche Eingabewerte zu finden, die den gleichen Hashwert liefern. Da die Hashwerte genutzt werden, um Identitäten zu überprüfen, wäre es sonst nicht mehr möglich, eindeutig zu identifizieren.

ArchiCrypt Stega setzt diese Funktion für verschiedene Zwecke ein. Der erste Einsatzfall ist die Aufbereitung der Zufallsdaten die bei der Generierung von Passwörtern und Schlüsseldisketten gesammelt werden. Der zweite Einsatz kommt bei der Identifikation von Passwörtern zum Einsatz. ArchiCrypt Stega muss es auf irgendeine Art schaffen, festzustellen, ob ein bestimmtes Passwort geeignet ist, eine bestimmte Datei zu entschlüsseln. Das Passwort mit der Datei zu speichern, ist eine denkbar schlechte Methode. Das Passwort verschlüsseln und dann mit der Datei speichern? Woher dieses Passwort nehmen? Wenn man vor dem Entschlüsseln das Passwort auf Richtigkeit hin untersucht, kann man dies anhand eines gespeicherten Hashwertes für das Passwort tun. Die Eigenschaften wie oben erläutert, erlauben dies. Die Wahrscheinlichkeit, dass zwei Passwörter zum gleichen Hashwert führen liegt bei $1: 2^{160}$. Sie brauchen einen speziellen Rechner, um Zahlen dieser Dimension berechnen zu können.

4.10 Entropie

Die Entropie einer Datei ist ein Maß für den Informationsgehalt.
Die Entropie wird in bit/char (sprich Bit pro Zeichen) angegeben.

Informationsgehalt:

Für die Berechnung des Informationsgehaltes betrachtet man die Wahrscheinlichkeitsverteilung der Zeichen in einer Datei. Man geht davon aus, dass die einzelnen Bytes der Datei stochastisch unabhängig voneinander sind und mit gleicher Wahrscheinlichkeit in der Datei auftreten.

Der Informationsgehalt einer Nachricht $N[I]$ ist definiert:

$$\text{Informationsgehalt}(N[I]) := \log_2(1/P[I]) = -\log_2(P[I]).$$

$P[I]$ ist dabei die Wahrscheinlichkeit, mit der die Nachricht $N[I]$ in der Datei auftritt. \log_2 bezeichnet den Logarithmus zur Basis 2.

Der Informationsgehalt hängt damit ausschließlich von der Wahrscheinlichkeitsverteilung ab. Der semantische Inhalt geht dabei nicht in die Berechnung ein.

Da der Informationsgehalt einer seltenen Nachricht höher als der einer häufigen Nachricht ist, wird in der Definition der Kehrwert der Wahrscheinlichkeit verwendet.

Der Informationsgehalt zweier unabhängig voneinander ausgewählter Nachrichten ist gleich der Summe der Informationsgehalte der einzelnen Nachrichten.

Entropie

Mit der Definition des Informationsgehaltes kann nun die mittlere Information berechnet werden.

Für die Mittelwertbildung werden die einzelnen Nachrichten mit der Wahrscheinlichkeit ihres Auftretens gewichtet.

$$\text{Entropie}(P[1], P[2], \dots, P[r]) := -(P[1] * \log(P[1]) + P[2] * \log(P[2]) + \dots + P[r] * \log(P[r]))$$

Man kann das etwas verständlicher wie folgt beschreiben:

Die Entropie gibt die Unsicherheit als Anzahl der notwendigen Ja / Nein-Fragen zur Klärung einer Nachricht oder eines Zeichens an. Hat ein Zeichen eine sehr hohe Auftrittswahrscheinlichkeit, so hat es einen geringen Informationsgehalt. Dies entspricht etwa einem Gesprächspartner, der regelmäßig mit "ja" antwortet. Antworten, die sehr selten auftreten, haben einen hohen Informationsgehalt.

In diesem Zusammenhang sind die Extremwerte interessant:

Ein Dokument, welches nur Ziffern enthält, kann im schlechtesten Fall 0 bit/char Entropie besitzen, ein Dokument, in welchem alle Ziffern mit gleicher Wahrscheinlichkeit auftreten kann die Entropie im Höchstfall $\log_2(10) = 3,3219$.

Für uns ist noch von Interesse, welche maximale Entropie in Dateien auftreten kann. Unsere Dateien sind aus Bytes aufgebaut. Also 8 Bit. Mit diesen 8 Bit kann man 256 verschiedene Zeichen darstellen (siehe auch ASCII_Tabelle).

Die Entropie für solche Dokumente beträgt mindestens 0 bit/char und höchstens 8 bit/char, falls in der Datei alle Zeichen gleich häufig vorkommen.

Entropie einer Datei

Die Entropie einer vorliegenden Datei kann also relativ leicht ermittelt werden. Man ermittelt für eine gegebene Datei, wie oft jedes Zeichen vorkommt.

[das war schon immer so, man glaubt es kaum, aber es stimmt.](#)

```
a      := 6
b      := 2
c      := 1
d      := 1
e      := 4
h      := 1
i      := 2
k      := 1
l      := 1
m      := 6
n      := 2
o      := 2
r      := 3
s      := 6
t      := 3
u      := 2
w      := 1
```

Anschließend setzt man die Werte in obige Gleichung ein erhält man einen Entropiewert von 3,2682.

Wobei $P[a] = 6 / 58$, $P[b] = 2 / 58$ usw.

Verschlüsselte Dokumente kann man eventuell am Entropiewert erkennen. Je näher dieser Wert am Maximum liegt, desto größer ist die Wahrscheinlichkeit, dass es sich um eine verschlüsselte Datei handelt. Man kann diese Methode dazu nutzen, abzuschätzen, ob ein Angriff auf eine Datei erfolgreich war. Man testet verschiedene Passworte und nimmt das Ergebnis als Klartext, bei welchem der Entropiewert am geringsten ist.

Auf der anderen Seite sollte ein Verschlüsselungsverfahren immer Daten liefern, die einen fast maximalen **Entropiewert** besitzen. In unserem Fall also bei 7,99 und höher.

4.11 XOR

Dieses Verfahren können Sie selbst auf einem Blatt Papier nachvollziehen. Der Schlüssel für dieses Verschlüsselungsverfahren besteht aus einer Folge von Bits (siehe auch Passwörter).

Der Schlüssel wird bitweise mit den Bits des Klartextes mittels exklusivem Oder (**XOR**) verknüpft. Der Schlüssel selbst wird dabei zyklisch verwendet. D.h. Sind die Bits des Schlüssels aufgebraucht, beginnt man erneut beim ersten Schlüsselbit. Die Entschlüsselung geschieht durch erneute Anwendung der Verknüpfung mit XOR. Dies ist eine Eigenschaft der XOR-Verknüpfung, die in der Fachsprache mit Involution bezeichnet wird.

Es gilt $((A \text{ XOR } B) \text{ XOR } B) = A$ für alle Wahrheitswerte A und B.

Das exklusive Oder ermittelt aus zwei Wahrheitswerten (FALSCH=0 und WAHR=1) einen neuen Wahrheitswert.

In der nachfolgenden Wahrheitstabelle ist dies aufgeführt:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Falls beide Werte gleich sind, wird also 0 = FALSCH geliefert. Falls genau ein Wert WAHR ist, liefert die Verknüpfung 1 = WAHR.

Beispiel:

Klartext:	1	0	1	1	0	0	1	0
Schlüssel:	1	0	0	0	1	1	1	1
Ergebnis:	0	0	1	1	1	1	0	1

Um aus dem Verschlüsselungsergebnis erneut den Klartext zu erhalten, wenden wir erneut die XOR-Operation unter Verwendung des Schlüssels an.

Ergebnis:	0	0	1	1	1	1	0	1
Schlüssel:	1	0	0	0	1	1	1	1
Klartext:	1	0	1	1	0	0	1	0

Kennt man das am häufigsten vorkommende Zeichen im Klartext, so ist die Ermittlung des Schlüssels und somit auch des Klartextes möglich.

4.12 ASCII Tabelle

ASCII Tabelle

Diese ASCII Tabelle enthält alle 256 ASCII Zeichen. In der ersten Spalte steht der dezimale Wert (Dez), in der zweiten der hexadezimale Wert (Hex) und in der dritten das Zeichen, sofern darstellbar. Die Hex Angabe ist wichtig um in ArchiCrypt Stega spezielle Zeichen in Passwörtern nutzen zu können. Damit können Sie Zeichen nutzen, die sich nicht auf Ihrer Tastatur befinden. Wenn Sie ein solches Zeichen eingeben wollen, leiten Sie das Zeichen bei der Eingabe durch das Zeichen \$ ein. Schreiben Sie dahinter den 2-teiligen Hex Code. Z.B.bedeutet: \$28 das Zeichen (.Wenn Sie das \$ Zeichen eingeben möchten, geben Sie \$\$ ein.

Oct	Dec	Hex	Name
000	0	0x00	NUL
001	1	0x01	SOH, Control-A
002	2	0x02	STX, Control-B
003	3	0x03	ETX, Control-C
004	4	0x04	EOT, Control-D
005	5	0x05	ENQ, Control-E
006	6	0x06	ACK, Control-F
007	7	0x07	BEL, Control-G
010	8	0x08	BS, backspace, Control-H
011	9	0x09	HT, tab, Control-I
012	10	0x0a	LF, line feed, newline, Control-J
013	11	0x0b	VT, Control-K
014	12	0x0c	FF, form feed, NP, Control-L
015	13	0x0d	CR, carriage return, Control-M
016	14	0x0e	SO, Control-N
017	15	0x0f	SI, Control-O
020	16	0x10	DLE, Control-P
021	17	0x11	DC1, XON, Control-Q
022	18	0x12	DC2, Control-R
023	19	0x13	DC3, XOFF, Control-S
024	20	0x14	DC4, Control-T
025	21	0x15	NAK, Control-U
026	22	0x16	SYN, Control-V
027	23	0x17	ETB, Control-W
030	24	0x18	CAN, Control-X
031	25	0x19	EM, Control-Y
032	26	0x1a	SUB, Control-Z
033	27	0x1b	ESC, escape
034	28	0x1c	FS
035	29	0x1d	GS
036	30	0x1e	RS
037	31	0x1f	US
040	32	0x20	space

Index

- " -

"Angewandte Kryptographie" von Bruce Schneier 25

- A -

Administratorrechte 3
 Algorithmus 24
 Anwesenheit versteckter Daten 7
 Anzeige gültiger Sitzungsschlüssel 4
 Anzeige Verstecken möglich 4
 Art der KeyDisk festlegen 13
 Arten von Schlüsseldisketten 13
 asymmetrische Verfahren 23
 Auslesen der Information 4

- B -

Bewertung Ihres Passwortes 10
 Brute Force 25
 Brute-Force 27

- D -

Dialog zum Einlesen einer Schlüsseldiskette/KeyDisk 16

- E -

Eigenschaft festlegen 11
 Ein-/Ausschalten des LogBuchs 4
 Eingabe des Passwortes 10
 Eingabe eines Passwortes zur Entschlüsselung 10
 Eingabe eines Passwortes zur Verschlüsselung 10
 Eingabe eines Sitzungspasswortes 4
 Einlesen oder Erstellen einer Keydisk 4
 Einweg-Eigenschaft 28
 Einweg-Hashfunktionen 28
 Entropie 28
 Entropie einer Datei 28
 Entropiewert 28

Erster Start 17
 Extremwerte 28

- F -

Für wen eignet sich eine Schlüsseldiskette? 26

- G -

Größe 22
 Gütegrad 11

- H -

Handtool 4
 Hashfunktion 28
 Hilfethemen aufrufen 4
 Hinweise ein-/ausblenden 4
 Hybrid-Codierung 23

- I -

Informationsgehalt 28
 Installation 17

- K -

Keine Hinweise auf enthaltene Daten durch
 ArchiCrypt Stega 7
 KeyDisk 13, 17
 Kompression ein-/ ausschalten 4

- L -

Länge des Schlüssels 27
 letzte Aktion aufheben 8
 letzte Änderung Rückgangig machen 4
 LogBuch drucken 4
 LogBuch speichern 4
 LogBuch zurücksetzen 4
 Lupe 4

- M -

MARS 24
 Methode 24
 Mooreschen Gesetz 27

- O -

offene Eingabe des Passwortes 10

- P -

Passwort festlegen 13

Passwörter erstellen 11

- R -

RC6 24

Rechte eines lokalen Administrators 17

Rijndael 24

Rückgängig machen 8

- S -

Säubern der Trägerdatei 4

Schlüsseldatei speichern 13

Schnittstelle zu ArchiCrypt Safe 10, 24

Serpent 24

Steganografie 3

Steganographische Verfahren 23

symmetrische Verfahren 23

- T -

Trägerdatei an Information anpassen 4

Trägerdatei laden 4

Trägerdatei speichern 4

Trägerdatei stufenlos Zoomen 4

Trägerinformationen 3

Twofish 24

- V -

verdeckte Eingabe des Passwortes 10

Verschlüsselung aller Dateien in einem Verzeichnis
18

Verschlüsselung aller Dateien in einem Verzeichnis
mit KeyDisk 18

Verschlüsselung ein-/ ausschalten 4

Verschlüsselung einer Einzeldatei 18

Verschlüsselung einer Einzeldatei mit einer KeyDisk
18

Verschlüsselungsverfahren 23

Verstecken der Information 4

- W -

Was ist eine Schlüsseldiskette? 26

Wie sollte man mit der Schlüsseldiskette umgehen?
26

Wörter 24

die Sie auf keinen Fall als Passwort benutzen
sollten 24

- X -

XOR 30

- Z -

Zahlen als Passwort 24

Zeitliche Gültigkeit festlegen 13

Zoomen 4, 8

Zu versteckende Datei laden 4

Zufallsdaten 28

Zufallsdaten sammeln 13

Zufallssequenz 27

Zufallszahlenpool 27