

Handbuch ArchiCrypt Pro

Dok.-Nr.: ACPRO-HB-0001

Ausgabedatum: 06.09.2002

Ausgabe-Nr.: 1.0

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	4
1 Willkommen	4
Teil II Allgemeine Informationen	5
1 Installationshinweise	5
2 Systemvoraussetzungen	5
Teil III Bedienung	5
1 Überblick	5
2 Hauptmenü	6
3 Dateimanager	9
4 Personalisierer	10
Überblick	10
Überschrift	10
Logo	11
Text	11
Selfdecryptor	12
Selfdecryptor	12
Selfdecryptor beim Empfänger.....	13
5 Schnellbefehle und Wizards	14
Schnellbefehle.....	14
Wizards	15
Überblick	15
Wizard Verschlüsselung.....	15
Wizard Entschlüsselung.....	16
Wizard Selfdecryptor.....	17
6 Satellite	18
Überblick	18
Satellite einrichten und starten	19
Listeneinträge erstellen und bearbeiten.....	20
Ansehen der Logdatei	21
Anwendungsgebiete und Einsatz des Satellite.....	21
7 Silent Modus	23
8 Dialoge	23
Dialog zur Angabe eines Schlüssels	23
Passwortdialog.....	24

Verdeckte Eingabe	26
Passwortgenerator.....	26
Schlüsseldisketteerstellen	28
Schlüsseldisketteeinlesen	31
Einstellungen	32
9 Archive	33
Anzeige des Archivinhalts.....	33
Arbeit mit Archiven.....	34
10 Log Bereich	35
Arbeit mit dem Log Bereich	35
Aufbau der Logdateien.....	35
Kontextmenü des Log Bereichs	36
11 Statusleiste	36
12 Kurzhilfe	37
13 Fortschrittsanzeige	37
Die Fortschrittsanzeige.....	37
14 Zusammenarbeit mit MS Windows-Explorer	39
Zusammenarbeit mit MS Windows-Explorer.....	39
15 Erster Start	39
16 Beispiele	39
17 Tastaturkürzel	41
Teil IV Umgang mit der Software	42
1 Umgang mit der Software	42
Teil V Technischer Teil	43
1 Warum Verschlüsselung?	43
2 Verschlüsselung was ist das?	43
3 Eingesetzte Verfahren	44
4 Passwörter	45
5 Bewertung von Passwörtern	46
6 Sinnvoller Einsatz von Schlüsseldisketten	46
7 AES	47
8 Angriff auf Verschlüsseltes	48
9 Hashfunktionen	48
10 Entropie	49
11 XOR	50
12 ASCII Tabelle	51

1 Einleitung

1.1 Willkommen

Vielen Dank, dass Sie sich für ArchiCrypt entschieden haben.

Ich freue mich, Ihnen mit ArchiCrypt ein Tool an die Hand zu geben, mit dem Sie Ihre sensiblen Daten mit den besten zur Zeit verfügbaren Methoden der Kryptografie schützen können.

Jedes Dokument auf Ihrem Rechner enthält Informationen, die nicht für jeden zugänglich sein sollten. Finanzdaten, Kundendaten, Firmeninterna, Liebesbriefe, Bilder, Email-Adressen, Videos etc. Geben Sie den Dateien absolut beliebige Bezeichnungen, ArchiCrypt stellt nach Angabe des Passwortes die Originalbezeichnung, die Dateieigenschaften und bei Bedarf eine bestimmte Verzeichnisstruktur wieder her.

Kommunikation und Datenaustausch via Email ist bequem und wird vielfach genutzt. Genau in diesem Moment sind Ihre Daten jedoch für jeden, der es darauf anlegt, lesbar. Die Funktionsweise der Private-Key Public-Key Verschlüsselung, die in diesem Zusammenhang oft genannt wird, ist den wenigsten Leuten klar oder in der Anwendung schlicht zu umständlich. Außerdem setzt diese Methode auf der Empfängerseite immer eine bestimmte Software voraus. An dieser Stelle kommt der Selfdecryptor zum Einsatz, der nicht nur für die Sicherheit Ihrer Daten sorgt, sondern gleichzeitig durch die Nutzung als Werbefläche, ein äußerst wirksames Marketinginstrument darstellt.

Ganz neu in Version 6 ist ArchiCrypt Satellite. Mit dem Satellite können Sie bis zu 30 Verzeichnisse festlegen, die ständig überwacht werden. Treffen neue Dateien ein, werden zuvor festgelegte Aktionen ausgeführt. Vom einfachen Livebackup bis hin zum automatisierten Erstellen selbstentschlüsselnder Dateien.

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 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. Auch die verdeckte Eingabe von Passwörtern, die dem leidigen Keyloggerproblem zu Leibe rückt, wurde integriert.

Neben diesen offensichtlichen Neuerungen gibt es zahlreiche kleinere Verbesserungen, bei deren produktivem Einsatz wir Ihnen viel Erfolg wünschen.

Die neusten Entwicklungen können Sie wie gewohnt unter www.ArchiCrypt.com einsehen.

Dipl.-Ing. Patric Remus

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 NT**, **Windows 2000** und **Windows XP** zur Installation der Software lokale Administratorrechte besitzen müssen.

Hinweise für Administratoren:

ArchiCrypt erstellt auf dem lokalen Rechner den Registry Schlüssel `HKEY_CLASSES_ROOT\.%$%`. Dadurch wird der von ArchiCrypt genutzte Dateityp `.%$%` mit der Anwendung verknüpft. Um auf diesen Schlüssel schreibend zuzugreifen, benötigt man lokale Administratorrechte.

2.2 Systemvoraussetzungen

Um ArchiCrypt 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 98, ME, NT 4.0 (SP 6), Windows 2000 und Windows XP
- ▶ Bildschirmauflösung mindestens 800x600 bei einer Farbtiefe von mindestens 256 Farben
- ▶ Maus oder anderes Windows-kompatibles Zeigegerät

3 Bedienung

3.1 Überblick

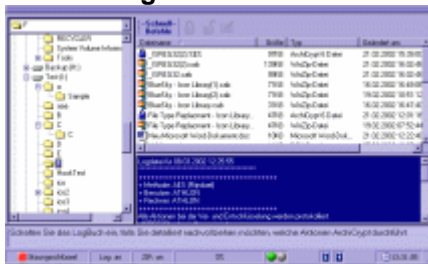
ArchiCrypt ist eine Verschlüsselungssoftware, die die zur Zeit besten und sichersten Verschlüsselungsverfahren einsetzt, um Ihre Daten gegen unbefugten Zugriff abzusichern. Um mit der Software verantwortungsvoll zu arbeiten, sollten Sie sich zunächst das Kapitel Umgang mit der Software durchlesen.

ArchiCrypt präsentiert sich nach dem Start in einer Ihnen sicher bekannten Dateimanageransicht. Die Ansicht orientiert sich hinsichtlich des Aufbaus und der Bedienung sehr stark am Windows-Explorer.

Der **Dateimanager** ist die Zentrale für alle manuellen Ver- und Entschlüsselungen. Für diese Aufgaben stehen Ihnen die **Schnellbefehle** oder aber die **Wizards** zur Verfügung, mit deren Hilfe Sie Dateien ver- und entschlüsseln, sowie selbstentschlüsselnde Dateien erstellen können.

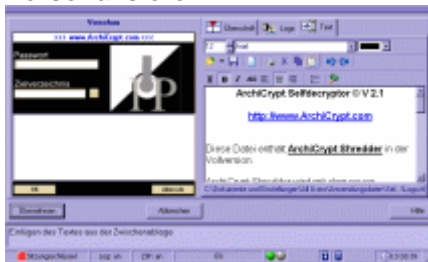
Neben dem **Dateimanager** bietet ArchiCrypt den **Personalisierer** zur Anpassung selbstentschlüsselnder Dateien und den **Satellite**, der Verzeichnisse überwachen und bei Eintreffen neuer Dateien Aktionen nach Ihren Vorgaben durchführen kann.

Dateimanager



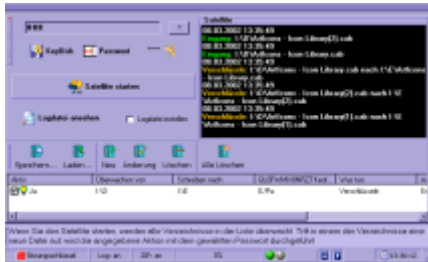
(siehe Dateimanager)

Personalisierer



(siehe Personalisierer)

Satellite



(siehe Satellite)






3.2 Hauptmenü

Das **Hauptmenü** ist in die Bereiche

- **Datei**
- **Ansicht**
- **Wechseln zu**
- **Schlüssel**
- **Tools**
- **Hilfe**

unterteilt.

Datei

	Verschlüsseln	Strg+Alt+V
	Entschlüsseln	Strg+Alt+E
	Selfdecryptor	Strg+Alt+S
	Einstellungen	Strg+Alt+O
	Beenden	Strg+Alt+X

Das Menü **Datei** bietet folgende Funktionen an:






Verschlüsseln, Entschlüsseln, Aufruf des **Selfdecryptors**, Änderung der **Einstellungen** (Verschlüsselungsmethode) und schließlich **Beenden** der Anwendung.

Die Ver- und Entschlüsselungsfunktionen sind nur dann verfügbar, wenn Sie im Dateimanager Dateien oder Ordner ausgewählt haben.

Ansicht

Das Menü **Ansicht** enthält zwei Untermenüs. Ein Menü zur Steuerung der Ansicht im **Dateimanager**(Dateifenster) und ein Untermenü **Menüleisten**.

Dateifenster

	Große Symbole
	Kleine Symbole
	Liste
	Details
	Detail mit Gitternetz

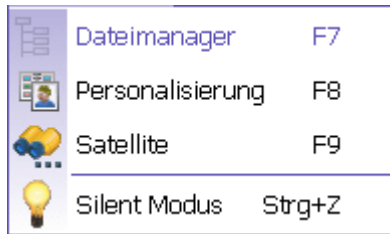
Menüleisten

	Wizards
	Sitzungs-Schlüssel
	Hilfe
	Menütext zeigen

Über dieses Untermenü steuern Sie, welche Menüleiste sichtbar ist, und welche nicht. Im Beispiel sind alle verfügbaren Menüleisten sichtbar. **Bedenken Sie, dass die Verfügbarkeit mancher Menüleiste bei bestimmten Aktionen unverzichtbar ist.**

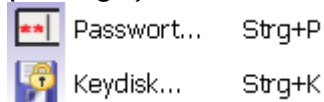
Durch Auswahl des Punktes **Menütext zeigen**, werden in den Menüleisten nicht nur Symbole angezeigt, sondern auch die Bezeichnungen.

Wechseln zu



Mit diesem Menü können Sie zu den verschiedenen Hauptansichten von ArchiCrypt wechseln. Silent Modus schaltet ArchiCrypt in den unsichtbaren Modus. (siehe auch Silent Modus)

(Sitzungs-)Schlüssel



Über den Eintrag **Passwort** erreichen Sie den Passwortdialog, in dem Sie ein neues Passwort eingeben, oder ein neues Passwort nach Ihren Vorgaben erstellen lassen können.

Der Menüpunkt **KeyDisk** öffnet den Dialog Schlüsseldiskette. In diesem Dialog können Sie eine neue Schlüsseldiskette erstellen, oder eine vorhandene laden.

Der so festgelegte Schlüssel wird nicht automatisch verwendet. Er steht vielmehr an den Stellen zur Verfügung, an denen die Möglichkeit besteht, den Sitzungsschlüssel als aktuellen Schlüssel zu verwenden.

Tools



Zip-Archive

Falls Sie diese Option eingeschaltet haben, werden die Inhalte von ZIP-Archiven angezeigt. Gleichzeitig stehen Ihnen zahlreiche Funktionen zur Bearbeitung des Archivs zur Verfügung. (siehe auch Arbeit mit Archiven)

LogBuch

Schalten Sie diese Option ein, wenn ArchiCrypt alle Aktionen protokollieren soll. (siehe auch Arbeit mit dem LogBereich)

Online News



(siehe Schnellbefehle)

Wizards



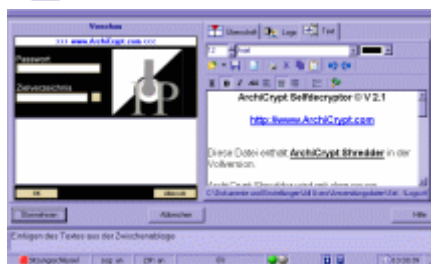
(siehe Wizards)

Während die Schnellbefehle mit verschiedenen Voreinstellungen arbeiten und nur wenige Angaben erfordern, bietet der jeweilige Wizard deutlich mehr Spielraum. Der Wizard führt Sie dabei durch den Erstellprozess und macht Sie auf mögliche Fehler aufmerksam.

Die Aktionen, die Sie während der Arbeit mit ArchiCrypt durchführen, werden im Logbuch protokolliert. Sie können diese Funktion im **Hauptmenü -> Tool -> LogBuch** ein- oder ausschalten. Weitere Informationen über das LogBuch erhalten Sie unter Arbeit mit dem Log Bereich.

3.4 Personalisierer

3.4.1 Überblick



Der **Personalisierer** teilt den Bildschirm in 2 Bereiche auf.

Den linken Teil, in dem eine Vorschau des Dialoges angezeigt wird, wie ihn der Empfänger einer selbstentschlüsselnden Datei sieht, und in den rechten Bereich, in dem Sie das Aussehen des Dialogs festlegen.

Das Anpassen des Dialoges ist in 3 Punkte aufgeteilt:

Überschrift, Logo und Text

Wenn Sie Ihre Eingaben abgeschlossen haben, können Sie diese durch Betätigen der Schaltfläche **Übernehmen**, akzeptieren.

(siehe auch Selfdecryptor und Selfdecryptor beim Empfänger)

3.4.2 Überschrift

Auf der Seite **Überschrift** gibt es 2 Eingabefelder.

Das Eingabefeld **Überschrift**, in dem Sie den Text festlegen, der im Dialog als Überschrift angezeigt werden soll und das Eingabefeld **Verknüpfte Internetadresse**.

1. Eingabefeld Überschrift

Alles was Sie in das Feld **Überschrift** eingeben, wird zeitgleich im Vorschaufenster angezeigt. Der

Text kann beliebig gewählt werden, achten Sie jedoch darauf, keinen zu langen Text zu wählen.

2. Verknüpfte Internetadresse

Die **Verknüpfte Internetadresse** gibt an, welche Internetadresse aufgerufen wird, wenn der Empfänger der selbstentschlüsselnden Datei auf die Überschrift klickt.

Die Adresse kann eine bestimmte Internetseite bezeichnen, zu einem FTP-Server gehören, oder eine Emailadresse repräsentieren.

- Adressen von Internetseiten geben Sie bitte mit führendem **http//**: an; also etwa <http://www.ArchiCrypt.com>.
- Adressen von FTP Servern bitte mit vorangestelltem **ftp//**, also etwa <ftp://ftp.uni-stuttgart.de>
- Emailadresse leiten Sie bitte mit der Zeichenfolge **mailto**: ein; also <mailto:Info@ArchiCrypt.com>

Man kann der Emailadresse auch einen Betreff und einen kurzen Text beifügen.

Beispiel:

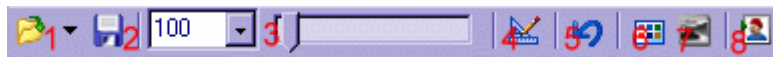
[mailto:Info@ArchiCrypt.com? subject=ArchiCrypt 6&body=Ich würde mir nachfolgende Features wünschen:](mailto:Info@ArchiCrypt.com?subject=ArchiCrypt%206&body=Ich%20w%C3%BCrde%20mir%20nachfolgende%20Features%20w%C3%BCnschen)

Hinter **subject=** steht der Text, der als Betreff in der Mail auftritt. Die Angabe hinter **body=** ist der Text, der als eigentlicher Meldungstext im Emailprogramm auftaucht. Der eigentliche Text (hinter Body=), ist auf ca 240 Zeichen begrenzt. Ein Zeilenumbruch muss mit der Zeichenfolge %0D%0A angegeben werden.

3.4.3 Logo

Auf der Seite **Logo** können Sie die anzuzeigende Grafik festlegen und diese mit einigen Basisfunktionen an Ihre Bedürfnisse anpassen.

Es werden Ihnen folgende Funktionen angeboten:



1. Laden einer Grafik
2. Speichern der Grafik
3. Festlegen des Zoomfaktors
4. Anpassen der Größe
5. Letzte Aktion rückgängig machen
6. Kontrast, Farb- und Helligkeitswerte festlegen
7. Grafik in ein Graustufenbild umwandeln
8. Verschiedene Grafikfilter und Effekte

3.4.4 Text

Auf der Seite **Text** finden Sie einen Texteditor, mit dem Sie einfach formatierte Texte rasch erstellen können. Der Funktionsumfang des Editors ist dabei an die Fähigkeiten des Dialogs der sich selbstentschlüsselnden Datei angepasst.

Um mehr über die Funktion einer Schaltfläche zu erfahren, bewegen Sie den Mauszeiger über die entsprechende Schaltfläche und warten bis Ihnen ein Kurzhinweis angezeigt wird.



3.4.5 Selfdecryptor

3.4.5.1 Selfdecryptor

Das Ergebnis des Erstellvorganges einer selbstentschlüsselnden Datei ist der so genannte Selfdecryptor

Der Selfdecryptor ist High Tech. Als Selfdecryptor wird der Teil bezeichnet, der auf der Empfängerseite dafür sorgt, dass die Daten nur dann zugänglich werden, wenn ein zuvor vereinbartes Passwort eingegeben wird. Neben dem Vorteil, dass **auf der Empfängerseite keinerlei zusätzliche Programme zur Entschlüsselung** benötigt werden, hat der Selfdecryptor weitere herausragende Eigenschaften.

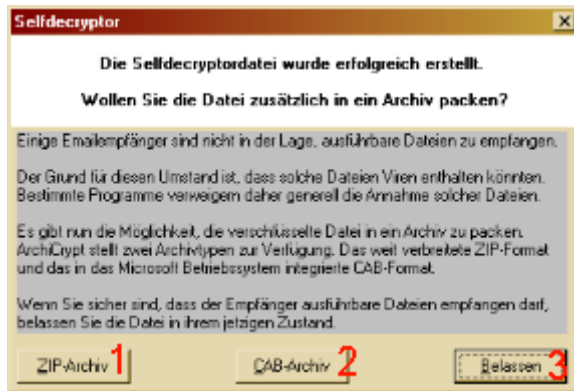
Der Selfdecryptor ist personalisierbar. (siehe auch Personalisieren des Selfdecryptors) Das heißt, Sie legen das Aussehen des Selfdecryptors fest. Damit wird Ihren Kommunikationspartnern nicht nur verdeutlicht, dass Ihnen der Begriff Datensicherheit kein Fremdwort ist, sondern Sie haben gleichzeitig die Möglichkeit, auf innovative Weise Werbung zu betreiben. Angenehmer Nebeneffekt bei der Verwendung des Selfdecryptors ist die Tatsache, dass die zu versendenden Daten komprimiert (also in ihrer Größe verkleinert) werden. Je nach enthaltenen Daten sparen Sie so bis zu 95%.

Der Selfdecryptor schafft es, dank der systemnahen Umsetzung, mit 40 KByte alle die Funktionen (Entschlüsselung, Dekompression, Darstellung der Grafik und des Werbetextes und Bereitstellung der Bedienoberfläche) bereitzustellen. (Zum Vergleich: Ein absolut leeres MS Word Dokument hat einen Platzbedarf von ca. 18KByte).

Vorgehen beim Erstellen einer Selfdecryptor Datei:

Wählen Sie wie bei einer normalen Verschlüsselung Dateien oder ein Verzeichnis aus. Betätigen Sie anschließend die Schnellbefehlstaste oder rufen Sie den Wizard auf. (siehe auch Selfdecryptor beim Empfänger)

Nachdem der Selfdecryptor fertiggestellt ist, können Sie im nachfolgenden Dialog auswählen, ob der Selfdecryptor in ein ZIP-Archiv **1** oder ein CAB-Archiv **2 gepackt**, oder als ausführbare Datei **3** belassen werden soll.

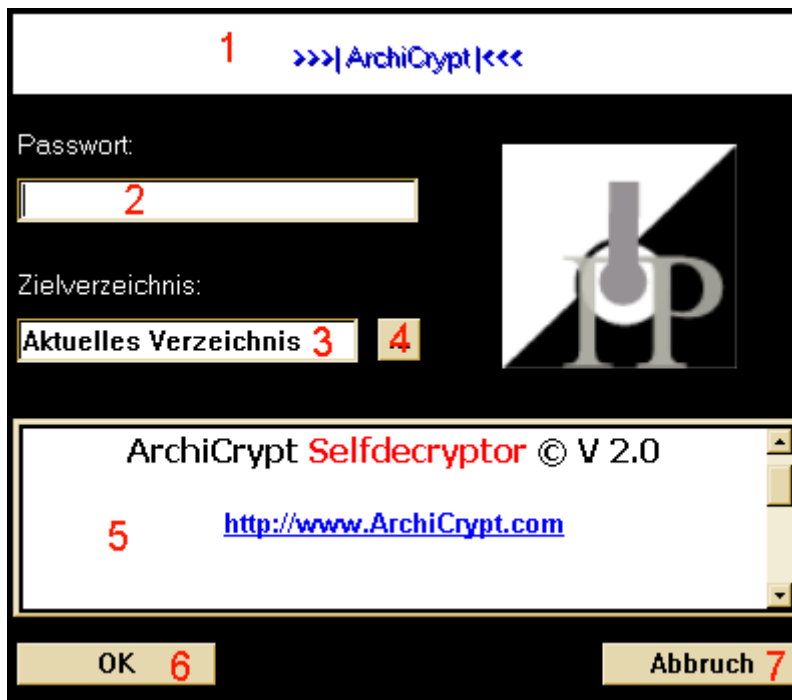


(siehe auch Selfdecryptor beim Empfänger).

3.4.5.2 Selfdecryptor beim Empfänger

Nachdem Sie den Selfdecryptor erstellt haben, können Sie das erstellte Programm an den Empfänger weiterleiten.

Die nachfolgende Grafik zeigt die interaktiven Elemente des Selfdecryptors.



1) Mausklick auf den Kopfzeilenbereich verzweigt zur im Personalisierer angegebenen Internetadresse.

2) In das Eingabefeld muss das Passwort eingegeben werden, welches Sie zur Verschlüsselung benutzt haben.

Tipp: *Um Ihre Passwörter effektiv und sicher zu verwalten empfiehlt sich der Einsatz von ArchiCrypt Safe.*

3,4) Der Empfänger kann ein Verzeichnis in das Eingabefeld eingeben oder über die Schaltfläche 4, einen Dialog zur Verzeichniswahl aufrufen. Selfdecryptor gibt als Empfehlung vor, die Dateien in das aktuelle Verzeichnis zu entschlüsseln.

5) Ein hinsichtlich der Werbewirksamkeit sehr wichtiges Interaktionselement. Der Empfänger kann Internetadressen (Email, http, ftp,...) anklicken, die verknüpfte Anwendung wird aufgerufen und es wird zur Adresse verzweigt. Die Anzahl der Adressen ist fast beliebig.

6) Hat der Empfänger kein Passwort angegeben, wird der Selfdecryptor geschlossen. Hat der Empfänger ein falsches Passwort angegeben, wird ihm die Meldung Prüfsummenfehler angezeigt und der Selfdecryptor wird geschlossen. Hat der Empfänger das korrekte Passwort angegeben, werden die Daten in das unter 3,4 festgelegte Verzeichnis entschlüsselt.

3.5 Schnellbefehle und Wizards

3.5.1 Schnellbefehle

Mit Hilfe der Schnellbefehle können Sie die 3 Basisoperationen

Verschlüsseln von Dateien



Entschlüsseln von Dateien



Erstellen selbstentschlüsselnder Dateien



durchführen.

Die Schnellbefehle arbeiten dabei mit bestimmten Voreinstellungen. Zum Beispiel werden die erstellten Dateien immer in dem Verzeichnis abgelegt, in dem sich auch die Ausgangsdatei befindet.

Um die Schnellbefehle zu nutzen, wählen Sie die zu bearbeitenden Dateien aus (Sie können auch einen Verzeichnisordner auswählen; in diesem Fall werden alle Dateien bearbeitet, die sich in diesem Ordner befinden) und betätigen Sie die zum gewünschten Schnellbefehl gehörende Schaltfläche.

Wenn Sie eine selbstentschlüsselnde Datei erstellen möchten, sollten Sie zuvor den Dialog für den Empfänger an Ihre Vorstellungen anpassen. Nutzen Sie hierzu den Personalisierer (siehe Personalisierer).

In allen Fällen erscheint der Dialog zur Angabe eines Schlüssels. (siehe Dialog zur Angabe eines Schlüssels).

Nachdem der Schlüssel festgelegt wurde und Sie die Auswahl durch Betätigen der OK Schaltfläche bestätigt haben, werden im Falle einer Ver- oder Entschlüsselung die Dateien erstellt. Wenn Sie eine selbstentschlüsselnde Datei erstellen, müssen Sie zusätzlich noch einen Namen für die Datei angeben. Den Fortgang der Aktion ersehen Sie an der Fortschrittsanzeige.

ACHTUNG

Große Dateien (> 15 - 20 Megabyte) sollten nicht in eine Selfdecryptordatei eingebunden werden.

3.5.2 Wizards

3.5.2.1 Überblick

Die **Wizards** unterstützen Sie bei der **Durchführung komplexer Arbeitsabläufe**. Im Gegensatz zu den Schnellbefehlen, die nur wenige Angaben erfordern, gleichzeitig aber relativ wenig Spielraum bieten, kann man mit den Wizards viele Spezialfunktionen nutzen.

Um einen Wizard zu nutzen, wählen Sie zunächst die Dateien aus, die Sie bearbeiten möchten. (Sie können auch einen Verzeichnisordner auswählen; in diesem Fall werden alle Dateien bearbeitet, die sich in diesem Ordner befinden). Wenn Sie eine selbstentschlüsselnde Datei erstellen möchten, sollten Sie zuvor den Dialog für den Empfänger an Ihre Vorstellungen anpassen. Nutzen Sie hierzu den Personalisierer (siehe Personalisierer).

Für jede Funktion gibt es einen eigenen Wizard, der je nach Aktion unterschiedlich viele Schritte erfordert.

Verschlüsseln von Dateien

Entschlüsseln von Dateien

Erstellen selbstentschlüsselnder Dateien

3.5.2.2 Wizard Verschlüsselung



Zum jeweils nächsten Schritt gelangen Sie, indem Sie die Schaltfläche **Weiter** betätigen.

Voraussetzung:

Dateien und / oder Verzeichnisse die verschlüsselt werden sollen, sind ausgewählt.

Schritt 1: Welche Dateien möchten Sie verschlüsseln?

*Hier werden Ihnen die Dateien angezeigt, die Sie ausgewählt haben. Um Dateien aus der Liste zu entfernen, die Sie versehentlich ausgewählt haben, markieren Sie die betroffenen Dateien mit der linken Maustaste, halten die linke Maustaste gedrückt und ziehen die Dateien über das mit Löschfeld bezeichnete schwarze Rechteck und lassen die Maustaste los. Die Dateien werden dann aus der Liste entfernt. Haben Sie Dateien versehentlich aus der Liste entfernt, betätigen Sie die Schaltfläche **Rückgängig**.*

Schritt 2: Wo möchten Sie die verschlüsselten Dateien speichern?

Sie haben hier die Möglichkeit festzulegen, in welches Verzeichnis die verschlüsselten Dateien abgelegt werden sollen.

Schritt 3: Sollen die Originaldateien gelöscht werden?

Wählen Sie hier nur dann ja, wenn Sie die Dateien nicht mehr im Klartext benötigen. Falls Sie die Dateien löschen, werden diese mit Betriebssystemmitteln gelöscht. Dies bedeutet, dass die Dateien mit Recoverytools wieder herstellbar sind.

Schritt 4a: Sollen die Dateien in eine Datei geschrieben werden?

Nur, falls Sie mehrere Dateien ausgewählt haben.

Sie können mehrere Dateien in eine einzige Datei schreiben lassen. Beim Entschlüsseln werden die ursprünglichen Datei- und Pfadangaben wieder hergestellt. Falls Sie JA auswählen, können Sie einen Namen festlegen, den diese Datei erhalten soll, oder einen zufälligen Namen durch ArchiCrypt generieren lassen.

Schritt 4b: Wie sollen Dateien benannt werden?

Die Auswahl **Falls Datei schon existiert, automatisch umbenennen** sorgt dafür, dass Dateien mit gleichem Namen nicht überschrieben werden. Haben Sie zum Beispiel eine Datei Geheim.doc und eine zweite namens Geheim.bmp, würden bei der Verschlüsselung in beiden Fällen eine Datei mit Namen Geheim.%%\$% entstehen. Es würde also die zuerst verschlüsselte Datei durch die erste wieder überschrieben. Die Einstellung verhindert dies, indem sie an den Namen der zweiten Datei eine in Klammern gesetzte Ziffer anhängt.

Gleichzeitig können Sie auch durch Auswahl von **folgende Dateieindung verwenden** festlegen, dass die verschlüsselten Dateien eine harmlose Dateieindung erhalten.

Die Auswahl **Zufallsdateiname vergeben** (nur falls nicht alle Dateien in eine einzige Datei geschrieben werden), sorgt dafür, dass jede der Dateien mit zufälligem Dateinamen abgelegt wird. Der Name wird dabei aus Buchstaben und Ziffern gebildet.

Schritt 5: Mit welchem Schlüssel sollen die Dateien bearbeitet werden?

In diesem Schritt legen Sie den Schlüssel fest, mit dem die Dateien verschlüsselt werden sollen. Sie haben 3 Möglichkeiten zur Auswahl.

1. Passworteingabe und Passwort generieren.
2. Schlüsseldiskette einlesen oder erstellen
3. Den Sitzungsschlüssel als Schlüssel für die aktuelle Verschlüsselung wählen.
(Der Sitzungsschlüssel selbst kann dabei ebenfalls ein "normales" Passwort oder eine Schlüsseldiskette sein.)

(siehe auch Dialog zur Angabe eines Schlüssels)

Zusammenfassung

In der Zusammenfassung können Sie Ihre Einstellungen nochmals überprüfen. Falls Sie feststellen, dass eine der Angaben nicht Ihren Vorstellungen entspricht, können Sie über die Schaltfläche Zurück, zum gewünschten Schritt zurückkehren, und die Änderungen vornehmen. Falls alle Einstellungen Ihren Vorstellungen entsprechen, betätigen Sie bitte die Schaltfläche **Fertigstellen**.

3.5.2.3 Wizard Entschlüsselung

Zum jeweils nächsten Schritt gelangen Sie, wenn Sie die Schaltfläche **Weiter** betätigen.

Voraussetzung:

Dateien und / oder Verzeichnisse die entschlüsselt werden sollen, sind ausgewählt.

Schritt 1: Welche Dateien möchten Sie entschlüsseln?

Hier werden Ihnen die Dateien angezeigt, die Sie ausgewählt haben. Um Dateien aus der Liste zu entfernen, die Sie versehentlich ausgewählt haben, markieren Sie die betroffenen Dateien mit der linken Maustaste, halten die linke Maustaste gedrückt und ziehen die Dateien über das mit Löschfeld bezeichnete schwarze Rechteck und lassen die Maustaste los. Die Dateien werden dann aus der Liste entfernt. Haben Sie Dateien versehentlich aus der Liste entfernt, betätigen Sie

die Schaltfläche **Rückgängig**.

Schritt 2: Wo möchten Sie die entschlüsselten Dateien speichern?

Sie haben hier die Möglichkeit festzulegen, in welches Verzeichnis die entschlüsselten Dateien abgelegt werden sollen.

Gleichzeitig können Sie festlegen, dass beim Entschlüsseln die Verzeichnisstruktur wiederhergestellt wird, die beim Verschlüsseln der Dateien vorlag.

Schritt 3: Sollen die Originaldateien gelöscht werden?

Wählen Sie hier nur dann ja, wenn Sie die Dateien nicht mehr in verschlüsselter Form benötigen.

Schritt 4: Mit welchem Schlüssel sollen die Dateien bearbeitet werden?

In diesem Schritt legen Sie den Schlüssel fest, mit dem die Dateien entschlüsselt werden sollen. Sie haben 3 Möglichkeiten zur Auswahl.

1. Passworteingabe und Passwort generieren.
2. Schlüsseldiskette einlesen oder erstellen
3. Den Sitzungsschlüssel als Schlüssel für die aktuelle Verschlüsselung wählen.
(Der Sitzungsschlüssel selbst kann dabei ebenfalls ein "normales" Passwort oder eine Schlüsseldiskette sein.)

(siehe auch Dialog zur Angabe eines Schlüssels)

Zusammenfassung

In der Zusammenfassung können Sie Ihre Einstellungen nochmals überprüfen. Falls Sie feststellen, dass eine der Angaben nicht Ihren Vorstellungen entspricht, können Sie über die Schaltfläche Zurück, zum gewünschten Schritt zurückkehren, und die Änderungen vornehmen. Falls alle Einstellungen Ihren Vorstellungen entsprechen, betätigen Sie bitte die Schaltfläche **Fertigstellen**.

3.5.2.4 Wizard Selfdecryptor



Zum jeweils nächsten Schritt gelangen Sie, wenn Sie die Schaltfläche **Weiter** betätigen.

Voraussetzung:

Dateien und / oder Verzeichnisse die verschlüsselt werden sollen, sind ausgewählt.

Schritt 1: Welche Dateien möchten Sie verschlüsseln?

Hier werden Ihnen die Dateien angezeigt, die Sie ausgewählt haben. Um Dateien aus der Liste zu entfernen, die Sie versehentlich ausgewählt haben, markieren Sie die betroffenen Dateien mit der linken Maustaste, halten die linke Maustaste gedrückt und ziehen die Dateien über das mit Löschfeld bezeichnete schwarze Rechteck und lassen die Maustaste los. Die Dateien werden dann aus der Liste entfernt. Haben Sie Dateien versehentlich aus der Liste entfernt, betätigen Sie die Schaltfläche **Rückgängig**.

Schritt 2: Wie soll die selbstentschlüsselnde Datei benannt werden? Wo soll Sie abgelegt werden?

Im oberen Eingabefeld müssen Sie einen Namen für die selbstentschlüsselnde Datei festlegen. Legen Sie dann fest, in welchem Verzeichnis die Datei abgelegt werden soll. Falls Sie keinen Pfad angeben, wird die Datei auf Ihrem Desktop abgelegt.

Schritt 3: Sollen die Originaldateien gelöscht werden?

Wählen Sie hier nur dann ja, wenn Sie die Dateien nicht mehr im Klartext benötigen. Falls Sie die Dateien löschen, werden diese mit Betriebssystemmitteln gelöscht. Dies bedeutet, dass die Dateien mit Recoverytools wieder herstellbar sind.

Schritt 4: Soll die Datei zusätzlich in ein Archiv gepackt werden?

Aufgrund der Virengefahr, die von ausführbaren Dateien ausgeht, sind zahlreiche Emailprogramme so eingestellt, dass sie Dateien mit der Endung exe abweisen. Um Ihrem Kommunikationspartner dennoch die gewünschten Dateien zukommen zu lassen, bietet der Wizard an dieser Stelle die Möglichkeit, die erstellte selbstentschlüsselnde Datei nach dem Erstellvorgang in ein ZIP- oder CAB-Archiv integrieren zu lassen. Während das ZIP-Archiv weit verbreitet und sehr bekannt ist, bietet das CAB-Format den Vorteil, das es integraler Bestandteil des Betriebssystems ist. D.h. der Empfänger benötigt tatsächlich keine Zusatzsoftware. Wählen Sie im Zweifelsfall also das CAB-Format aus.

Schritt 5: Soll die Datei versendet werden?

Wählen Sie die Option Datei nach dem Erstellen als Email versenden, wird nach dem Erstellvorgang Ihr Emailprogramm geöffnet. Die erstellte selbstentschlüsselte Datei ist der Email bereits als Anhang beigelegt.

ACHTUNG: Diese Funktion ist nur möglich, falls Sie ein Email Programm nutzen, welches den MAPI Standard unterstützt. Bekanntester Vertreter ist Outlook (und Outlook Express).

Schritt 6: Mit welchem Schlüssel sollen die Dateien bearbeitet werden?

In diesem Schritt legen Sie den Schlüssel fest, mit dem die Dateien verschlüsselt werden sollen. Sie haben 2 Möglichkeiten zur Auswahl.

1. Passworteingabe und Passwort generieren.
2. Den Sitzungsschlüssel als Schlüssel für die aktuelle Verschlüsselung wählen.
(Der Sitzungsschlüssel selbst kann dabei ebenfalls ein "normales" Passwort sein.)

(siehe auch Dialog zur Angabe eines Schlüssels)

Zusammenfassung

In der Zusammenfassung können Sie Ihre Einstellungen nochmals überprüfen. Falls Sie feststellen, dass eine der Angaben nicht Ihren Vorstellungen entspricht, können Sie über die Schaltfläche Zurück, zum gewünschten Schritt zurückkehren, und die Änderungen vornehmen. Falls alle Einstellungen Ihren Vorstellungen entsprechen, betätigen Sie bitte die Schaltfläche **Fertigstellen**.

ACHTUNG

Große Dateien (> 15 - 20 Megabyte) sollten nicht in eine Selfdecryptordatei eingebunden werden.

3.6 Satellite

3.6.1 Überblick

Im Gegensatz zum Dateimanager, der für die manuelle Ver- und Entschlüsselung von Dateien zuständig ist, dient der **Satellite** der automatisierten Bearbeitung von Dateien. Wenn Sie erfahren möchten, wie Sie den Satellite starten, fahren Sie mit dem Kapitel Satellite einrichten und starten fort.

Der Satellite benötigt für seine Arbeit eine s.g. **Überwachungsliste**. Um eine Liste zu erstellen, muß zunächst ein s.g. **Listenpasswort** festgelegt werden. Dieses Passwort hat die Funktion, alle in

der Liste enthaltenen Passwörter zu verschlüsseln. Listen können unter beliebigem Namen gespeichert werden. Um bestehende Einträge zu bearbeiten oder neue zu erstellen, nutzen Sie bitte den Dialog zum Erstellen von Listeneinträgen.

Um die Tätigkeit des Satellite nachvollziehen zu können, besteht die Möglichkeit, eine Logdatei erstellen zu lassen. In dieser Logdatei finden Sie genaue Angaben darüber, zu welchem Zeitpunkt, welche Datei mit welcher Aktion und welchem Passwort bearbeitet wurde. Jeder Eintrag in dieser **Logdatei** ist mit dem von Ihnen festgelegten Listenpasswort verschlüsselt. Zur Auswertung steht Ihnen die Funktion **Logdatei ansehen** zur Verfügung (siehe Ansehen der Logdatei).

Unter Anwendungsgebiete und Einsatz des Satellite, finden Sie Beispiele für den Einsatz des Satellite.

3.6.2 Satellite einrichten und starten

Geben Sie zunächst ein **Listenpasswort** ein. Dabei kann es sich um ein Passwort einer bestehenden, aber auch um das Passwort einer neu zu erstellenden Überwachungsliste handeln.



Bedienung und die Bedeutung der Schaltflächen: Dialog zur Eingabe eines Schlüssels

Betätigen Sie die Schaltfläche **Laden...**, um eine bestehende Überwachungsliste zu laden, oder die Schaltfläche **Neu**, um den ersten Eintrag in einer neuen Liste zu erstellen.



(siehe auch Listeneintrag erstellen)

Falls Sie die erstellte Liste zu einem späteren Zeitpunkt wiederverwenden möchten, betätigen Sie die Schaltfläche **Speichern....** Die Liste, wird dann mit den darin enthaltenen Einträgen und Passwörtern in verschlüsselter Form gespeichert. Zu diesem Zweck wird das Listenpasswort verwendet.

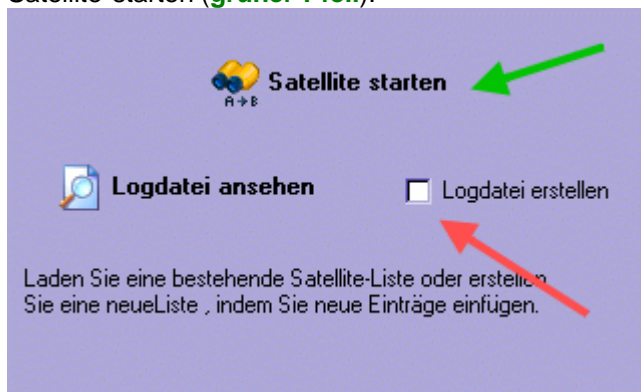
Aktiv	Überwachen von	Schreiben nach	QL0FWMX8NRZTKeof...	Was tu
<input type="checkbox"/> Nein	J:\Angebote	J:\Schmidt	E/Pa	Verschl
<input checked="" type="checkbox"/> Ja	J:\Angebote	J:\Wagner	E/Pa	Verschl
<input type="checkbox"/> Nein	J:\Verträge	J:\Müller	E/Pa	Verschl
<input checked="" type="checkbox"/> Ja	J:\Verträge	J:\Schmidt	E/Pa	Verschl
<input checked="" type="checkbox"/> Ja	J:\QS	J:\MAIL	E/Pa	Selbdec

Wählen Sie jetzt die Einträge aus, die der Satellite überwachen soll. Diese Einträge werden mit einer gelben Glühbirne gekennzeichnet. Einen Eintrag wählen Sie aus, indem Sie das Symbol in der Spalte **Aktiv** anklicken.

Um einen Eintrag zu ändern, markieren Sie diesen und betätigen die Schaltfläche **Änderung**.

Falls der Satellite alle Aktionen protokollieren soll, wählen Sie die Option **Logdatei erstellen (roter Pfeil)** aus. Der Satellite protokolliert jetzt jede einzelne Aktion inklusive verwendetem Passwort. Sie können so erstellte Logdateien nur mit ArchiCrypt einsehen (siehe Ansehen der

Logdatei). Nachdem Sie die zu überwachenden Einträge ausgewählt haben, können Sie den Satellite starten (**grüner Pfeil**).



Sie werden jetzt gefragt, ob Dateien, die sich bereits in den Verzeichnissen befinden, bearbeitet werden sollen.

Wenn Sie die Frage mit **Ja** beantworten, wird für jede Datei in einem Verzeichnis die festgelegte Aktion ausgeführt. Geben Sie **Nein** an, wird die Aktion nur bei Dateien ausgeführt, die nach dem Start des Satellite neu in ein Verzeichnis geschrieben werden.

Während der Satellite aktiv ist, empfiehlt es sich, den s.g. Silent Modus zu nutzen. Um die Performance zu steuern, können Sie unter Einstellungen bestimmte Werte festlegen, die das Zeitverhalten des Satellite beeinflussen.

3.6.3 Listeneinträge erstellen und bearbeiten

Listeneinträge werden mit dem Dialog zum Erstellen von Listeneinträgen erstellt. Sie haben im Dialog für die verschiedenen Bestandteile des Listenfeldes verschiedene Eingabe- und Auswahlfelder.

Jeder Eintrag in der Überwachungsliste hat folgende Bestandteile:

Was tun:

Aktion die bei Auftreten einer Änderung durchgeführt werden soll. Hier kann es sich um Verschlüsselung, Entschlüsselung, Selfdecryptor (Erstellen einer selbstentschlüsselnden Datei) oder um Synchronisation handeln.

Verschlüsseln: Alle Dateien die im überwachten Verzeichnis abgelegt werden, werden unter Berücksichtigung der anderen Werte mit dem festgelegten Schlüssel verschlüsselt.

Entschlüsseln: Alle Dateien die im überwachten Verzeichnis abgelegt werden, werden unter Berücksichtigung der anderen Werte mit dem festgelegten Schlüssel entschlüsselt.

Selfdecryptor: Alle Dateien die im überwachten Verzeichnis abgelegt werden, werden unter Berücksichtigung der anderen Werte mit dem festgelegten Schlüssel in eine sich selbstentschlüsselnde Datei umgewandelt.

Synchronisation: Alle Dateien die im überwachten Verzeichnis abgelegt werden, werden unter Berücksichtigung der anderen Werte kopiert.

Überwachen von:

Verzeichnis, das auf Änderungen hin untersucht werden soll

Schreiben nach:

Das Verzeichnis, in welches die jeweilige Aktion die Dateien schreiben soll

Passwort:

Prüfsumme für das Passwort, welches mit dem Eintrag verknüpft ist.

Name:

Entweder Vorgabe, falls die Datei entsprechend ihrem ursprünglichen Namen benannt werden soll. oder Zufälliger Dateiname.

KeyDisk:

Gibt an, ob für die Aktion eine Schlüsseldiskette verwendet wird.

Archiv:

Gibt an, ob nach Durchführung der eigentlichen Aktion noch ein Archiv erstellt werden soll.

Nachfolgende Tabelle gibt eine Übersicht darüber, bei welchen Aktionen welche Einstellungen bei den verschiedenen Werten möglich sind.

Was tun?	Überwachen von	Schreiben nach	Passwort	Name (Vorgabe, Zufall)	KD (KeyDisk)
Verschlüsseln	X	X	X	Vorgabe/Zufall	X
Entschlüsseln	X	X	X	Vorgabe	X
Selfdecryptor	X	X	X	Vorgabe	-
Synchronisation	X	X	-	Vorgabe	-

3.6.4 Ansehen der Logdatei

Die Schaltfläche "**Logdatei ansehen**" öffnet einen Dialog, indem Sie sich Logdateien ansehen und diese nach bestimmten Begriffen durchsuchen können. Beachten Sie bitte, dass Logdateien verschlüsselt sind, Sie also vor dem Laden das Passwort eingeben müssen, mit welchem die Überwachungsliste gesichert ist. Die Logdatei trägt auch den gleichen Namen, wie die zugehörige Überwachungsliste; lediglich die Dateiendungen unterscheiden sich.

3.6.5 Anwendungsgebiete und Einsatz des Satellite

Der Satellite bearbeitet Dateien in festgelegten Verzeichnissen automatisch nach bestimmten Vorgaben. ArchiCrypt nutzt hierzu s.g. Überwachungslisten (siehe auch Listeneintrag).

Beispiel 1: Verteilen vertraulicher Dokumente

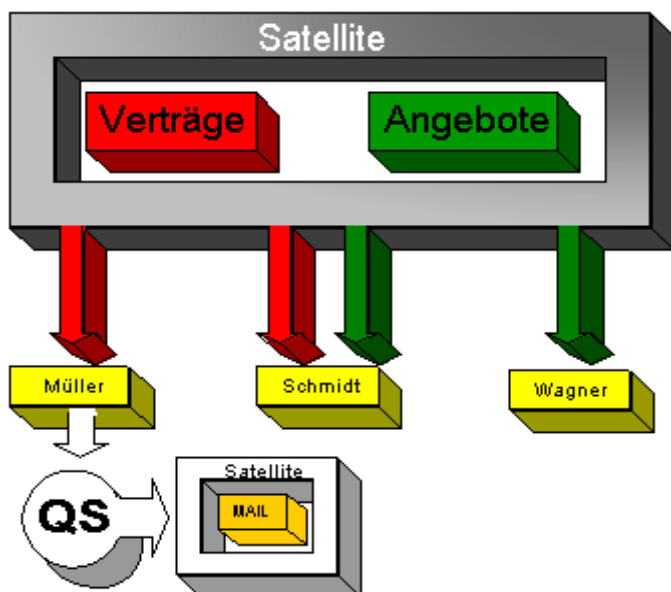
Nehmen wir an, Sie haben auf dem Server 2 Verzeichnisse, in welche von der Geschäftsführung verschiedene Dokumente eingestellt werden, die nur für bestimmte Personen zugänglich gemacht werden sollen.

Verzeichnisse:

Verträge, Angebote

Die Angestellten Müller und Schmidt sollen Zugriff auf alle Dateien im Verzeichnis Verträge

haben. Herr Schmidt soll gleichzeitig Dateien aus dem Ordner Angebote einsehen können. Herr Wagner ist nur für Angebote autorisiert. Herr Müller kontrolliert die Angebote und ist für die Weiterleitung per Email verantwortlich.



Für jede Person muß für jedes Verzeichnis, dessen Dateien für sie bestimmt sind, ein Eintrag in der Überwachungsliste erstellt werden.

Die Liste sollte wie folgt aussehen:

Was tun?	Überwachen von	Schreiben nach	Passwort	Name (Vorgabe, Zufall)	KD (KeyDisk)
Verschlüsseln	J:\Angebote	J:\Schmidt	*****	Vorgabe	Nein
Verschlüsseln	J:\Angebote	J:\Wagner	*****	Vorgabe	Nein
Verschlüsseln	J:\Verträge	J:\Müller	*****	Vorgabe	Nein
Verschlüsseln	J:\Verträge	J:\Schmidt	*****	Vorgabe	Nein
Selfdecryptor	J:\QS	J:\MAIL	*****	Vorgabe	Nein

Beispiel 2: Versenden vertraulicher Dokumente

Sie haben ein bestimmtes Dokument, welches Sie einem bestimmten Personenkreis zukommen lassen wollen. Mit jedem dieser Personen haben Sie ein Passwort vereinbart. Legen Sie für jede der Personen ein eigenes Verzeichnis an. Für jede der Personen muss ein eigener Eintrag in einer Überwachungsliste erstellt werden. Geben Sie bei Überwachen von das Verzeichnis an, in welches das zu versendende Dokument abgelegt wird. Bei Schreiben nach, das zum Empfänger gehörende Dokument und bei Passwort, das mit der Person vereinbarte Passwort.

Beispiel 3: Filesharing

Viele Programme zum Austausch von Dateien erlauben Zugriff auf den Ordner, in dem Sie

eigene Downloads ablegen. Legen Sie einen Listeneintrag an und tragen in den Feldern Überwachen von und Schreiben nach das Verzeichnis ein, in dem die Downloads abgespeichert werden. Wählen Sie ein Passwort und geben Sie die Option Dateien im überwachten Verzeichnis löschen an. ArchiCrypt verschlüsselt jetzt jede eingehende Datei und löscht anschließend die Klartextdatei. Die Datei ist jetzt für jeden, der das Passwort nicht kennt, wertlos.

Beispiel 4: FTP-Server, Web-Server

Sie betreiben eine Webserver und haben Verzeichnisse freigegeben, die für bestimmte Kunden oder Besuchergruppen Dateien erhalten. Die Dateien sollen jedoch nur von denen genutzt werden können, die zuvor ein Passwort von Ihnen erhalten haben.

Legen Sie zunächst Verzeichnisse an, in welche Sie die unverschlüsselten Dateien ablegen. Diese Verzeichnisse dürfen selbstverständlich nicht freigegeben werden. Jetzt legen Sie für jedes Verzeichnis mit Klartextdateien ein Verzeichnis an, welches die verschlüsselten Dateien aufnehmen soll. Diese Verzeichnisse können Sie zur Benutzung im FTP oder Web-Server freigeben. Richten Sie jetzt für jedes dieser Verzeichnisse einen Eintrag in einer Überwachungsliste ein. Bei Überwachen von geben Sie das Verzeichnis mit den Klartextdateien an, bei Schreiben nach, das freigegebene Verzeichnis, in welches die verschlüsselten Dateien abgelegt werden sollen.

3.7 Silent Modus

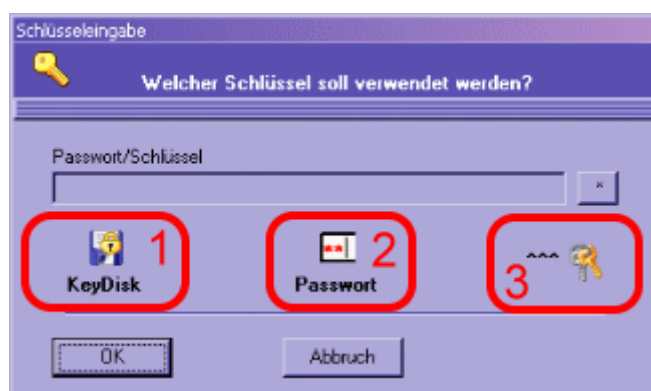
Der **Silent Modus** versteckt das ArchiCrypt Hauptfenster und zeigt ein Symbol [rote Glühbirne] im Statusbereich (Taskleiste neben der Uhr an). Sie können zum Schutz der Anwendung ein Kennwort festlegen. Dadurch wird verhindert, dass Unbefugte ungehindert Zugang zu Passwortdaten erhalten. Die Funktion ist im Zusammenhang mit dem Satellite besonders nützlich.

3.8 Dialoge

3.8.1 Dialog zur Angabe eines Schlüssels

Schlüsseleingabe

Als Schlüssel wird die Zeichenfolge bezeichnet, mit der Ihre Daten Verschlüsselt werden. Ein Schlüssel ist dabei nicht zwingend ein **Passwort**. Es kann sich alternativ auch um eine s.g. **Passphrase** (Merksatz), eine **Schlüsseldiskette** (KeyDisk) oder Ähnliches handeln.



Durch Betätigen der Schaltfläche KeyDisk (Schlüsseldiskette) wird der Dialog zum Einlesen / Erstellen einer Schlüsseldiskette aufgerufen. Die Schaltfläche 3 übernimmt einen eventuell vorhandenen Sitzungsschlüssel. Bei diesem kann es sich wiederum entweder um ein Passwort oder um eine Schlüsseldiskette handeln.

Sitzungsschlüssel



Einen Sitzungsschlüssel können Sie über die Schaltflächen der gleichnamigen Werkzeugleiste aufrufen.

- **Radiergummi** löscht einen **Sitzungsschlüssel**
- Symbol für das **Passworteingabefeld** öffnet einen Dialog zur Eingabe eines Passwortes
- **Diskettensymbol mit Schloss** öffnet den Dialog zum Einlesen / Erstellen einer Schlüsseldiskette

3.8.2 Passwortdialog

(siehe auch Dialog zur Angabe eines Schlüssels)

Es gibt zwei verschiedene Dialoge um ein Passwort einzugeben.

Der Dialog zur Eingabe eines Passwortes falls eine oder mehrere Dateien entschlüsselt werden sollen, und den Dialog, zur Festlegung eines neuen Passwortes für die ArchiCrypt Sitzung oder eine Verschlüsselung. Beachten Sie bitte das gesonderte Kapitel über Passwörter im technischen Teil.

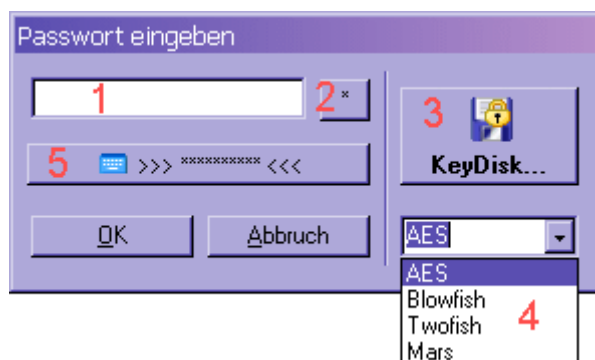
ArchiCrypt bietet einige Besonderheiten an, um Ihre Daten umfassend zu sichern.

Mit ArchiCrypt 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 ("Klammer auf". Wenn Sie das \$ Zeichen eingeben möchten, geben Sie \$\$ ein. (siehe auch Passwörter im technischen Anteil)

Eine sehr lästige Gefahr geht in der letzten Zeit von **Trojanern** (*Bezeichnung für ein Programm, das die Benutzeroberfläche eines anderen Programms nachahmt, oder vorgibt, eine bestimmte Funktion zu haben, tatsächlich jedoch Daten ausspioniert*) aus. Diese Programme protokollieren jeden Einzelnen Buchstaben den Sie eingeben und können so jedes Passwort, welches über Tastatur eingegeben wird, weiterleiten. Programme mit diesen Eigenschaften werden auch **Keylogger** genannt.

Die Keylogger haben bei ArchiCrypt keinen Erfolg, wenn Sie die s.g. verdeckte Eingabe nutzen.

1. Eingabe eines Passwortes zur Entschlüsselung



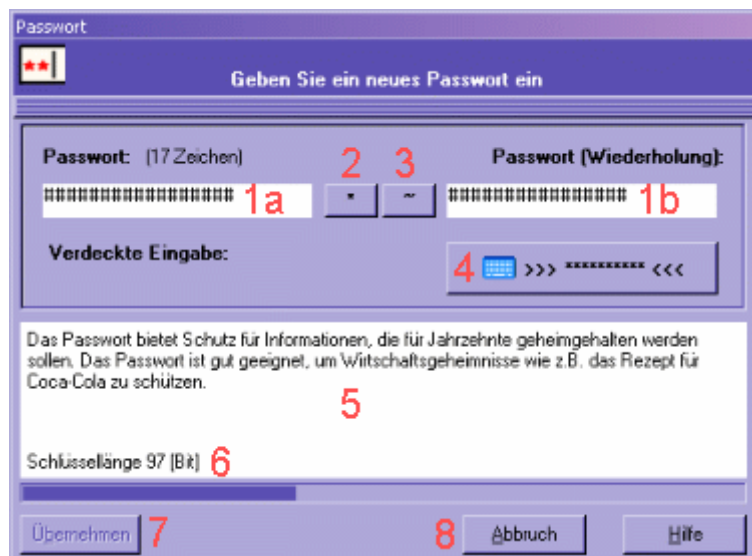
[Eingabe des Passwortes]

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.

Mit der Auswahlbox **4** können Sie, falls notwendig, die zur Verschlüsselung eingesetzte Methode auswählen. (siehe Einstellungen) Durch Betätigen der Schaltfläche **5** haben Sie die Möglichkeit, das Passwort verdeckt einzugeben. (siehe verdeckte Eingabe)

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.

Bei **4** können Sie den Dialog für die Verdeckte Eingabe aufrufen.

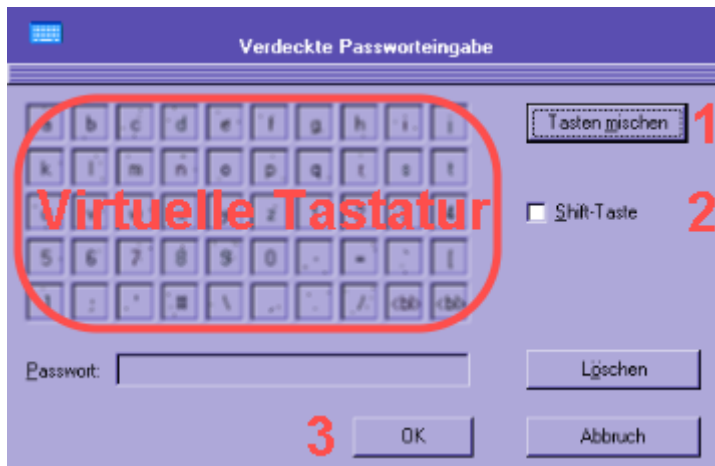
Im Feld **5** wird in Verbindung mit der Anzeige bei **6** eine Bewertung Ihres Passwortes vorgenommen. Die Bewertung beruht auf einem mathematischen Verfahren, welches im technischen Teil beschrieben ist.

Nachdem Sie in die beiden Passwordeingabefelder das gleiche Passwort eingegeben haben, bzw. ein generiertes Passwort übernommen wurde, können Sie durch Betätigen der Schaltfläche Übernehmen **7**, das Passwort für Ihre Ver- und Entschlüsselungen nutzen.

Mit der Abbruch Schaltfläche **8** können Sie den Eingabevorgang abbrechen.

3.8.3 Verdeckte Eingabe

Die **verdeckte Eingabe** unterbindet jeden Versuch, Ihr Passwort dadurch auszuspähen, dass sämtliche Tastatureingaben protokolliert werden. (siehe auch Passwortdialog)



Die virtuelle Tastatur stellt die Standardzeichen zur Verfügung. Mit Hilfe des \$ Zeichens können Sie mit Hilfe der ASCII Tabelle jedes Zeichen eingeben. Das Auswahlkästchen Shift-Taste **2** simuliert dabei die normale Shifttaste. Wenn Sie die Schaltfläche **Tasten mischen 1** betätigen, werden die Tasten in einer zufälligen Reihenfolge dargestellt. Die zufällig auf der Tastatur verteilten Punkte verhindern das gleichmäßige Abstrahlen des Monitors und damit ein Abhören.

Mit einem Klick auf die **OK 3** Schaltfläche übernehmen Sie das Passwort.

3.8.4 Passwortgenerator

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

Schritt 1:

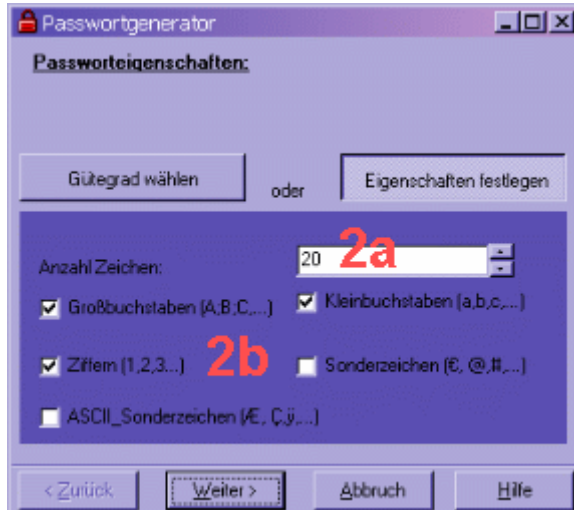


Durch die Schaltfläche **Gütegrad 1** gelangen Sie zu einem Wizard, mit dem Sie Passwörter

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.



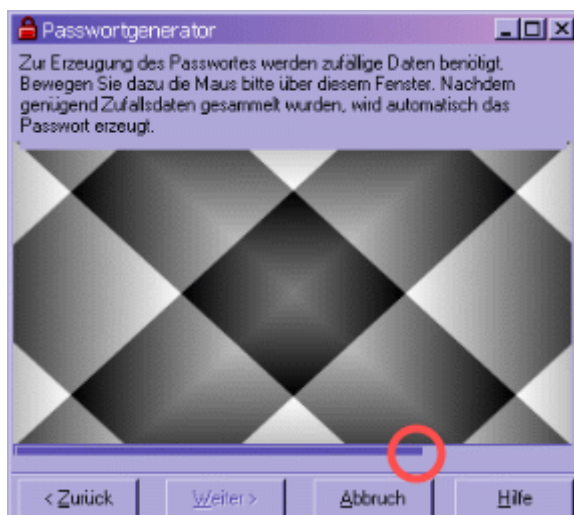
Hier können Sie festlegen, wie viele Zeichen Ihr Passwort lang sein soll, ob es Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen oder ASCII_Sonderzeichen(nichtdruckbare) enthalten soll. Das Wort **soll** ist hierbei wichtig.

Betätigen Sie Schaltfläche **Weiter**.

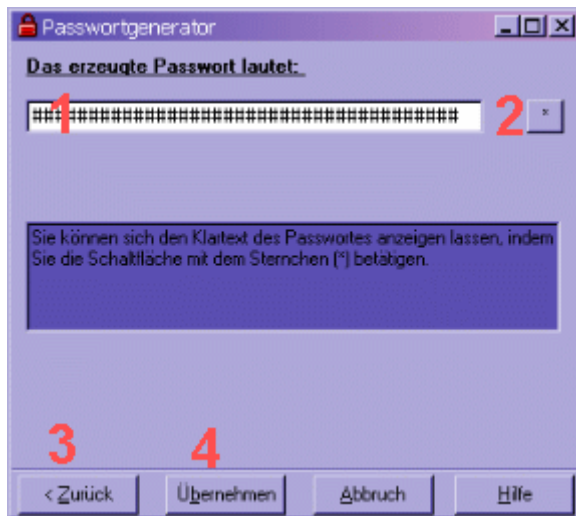
Schritt 2:

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 **3**, entspricht das Passwort Ihren Vorstellungen, betätigen Sie die Schaltfläche Übernehmen **4**.

3.8.5 Schlüsseldiskette erstellen

(siehe auch Schlüsseldiskette laden)

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

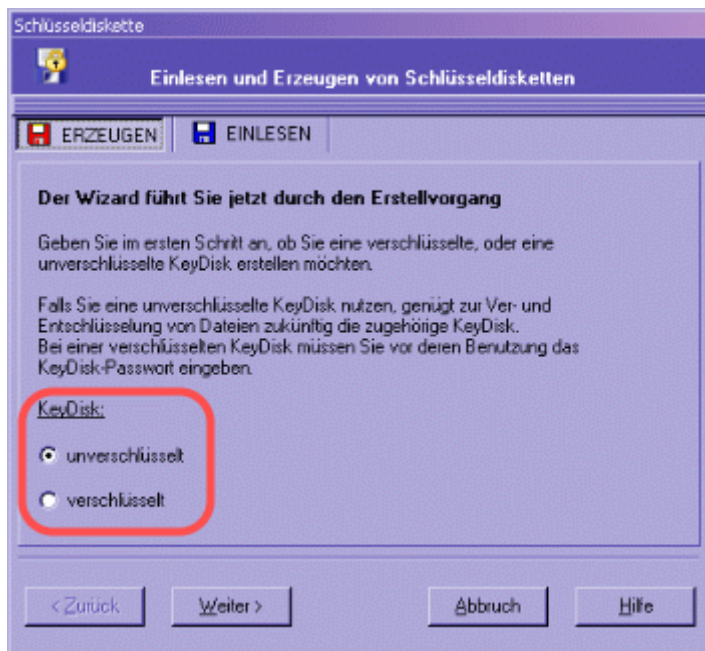
Die zweite Variante ist eine verschlüsselte Schlüsseldiskette. Das heißt zum Ver- und Entschlüsseln von Dateien benötigen Sie die Schlüsseldiskette und ein zugehöriges Passwort.

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**

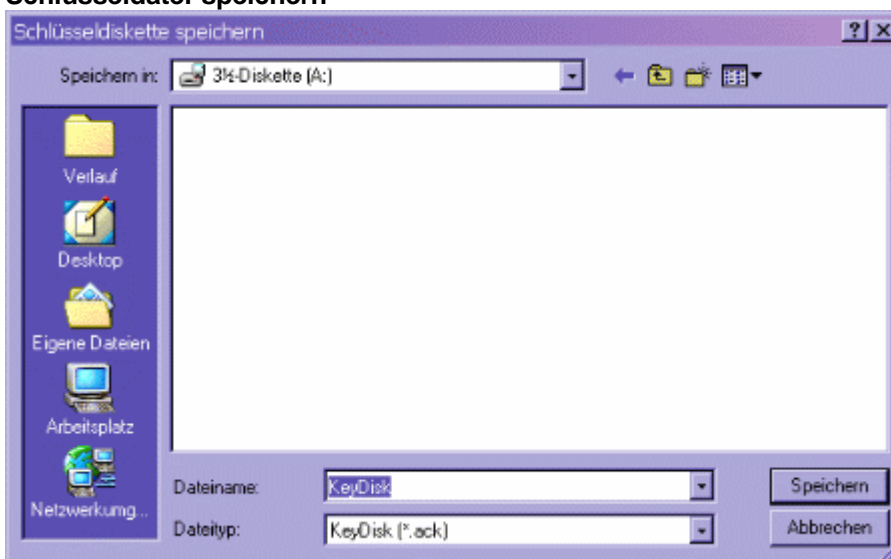
Nachdem genügend Zufallsdaten gesammelt wurden, erscheint automatisch der Dialog zur Passworteingabe.

**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 muss zur Ermittlung des Datums auf das Betriebssystem zugreifen. Ist dort ein falsches Datum eingestellt, erkennt ArchiCrypt 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.

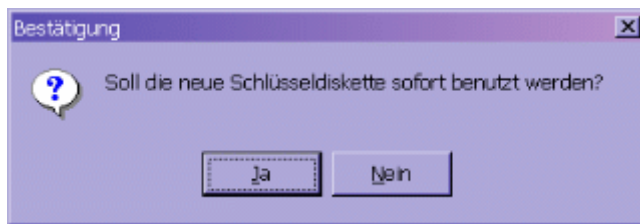
Schritt 5 (beide Arten): Schlüsseldatei speichern



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.

Schritt 6 (beide Arten optional): Nutzen der Schlüsseldiskette

Nachdem Sie die Schlüsseldatei gesichert haben erscheint der Dialog:

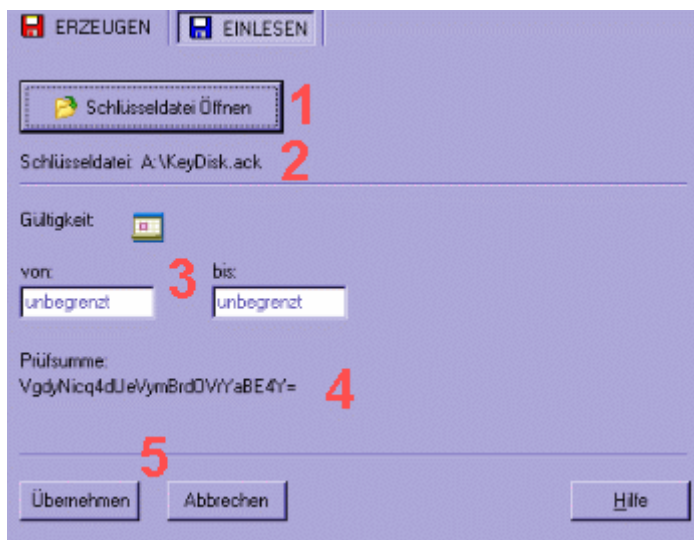


Beantworten Sie die Frage mit **Ja**, wird der Schlüssel von der Schlüsseldiskette als Sitzungsschlüssel genutzt.

Die erstellte Schlüsseldiskette können Sie jederzeit wie in "Schlüsseldiskette einlesen" beschrieben, einlesen und nutzen.

3.8.6 Schlüsseldiskette einlesen

Mit dieser Funktion können Sie Schlüsseldateien laden und mit ArchiCrypt 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.

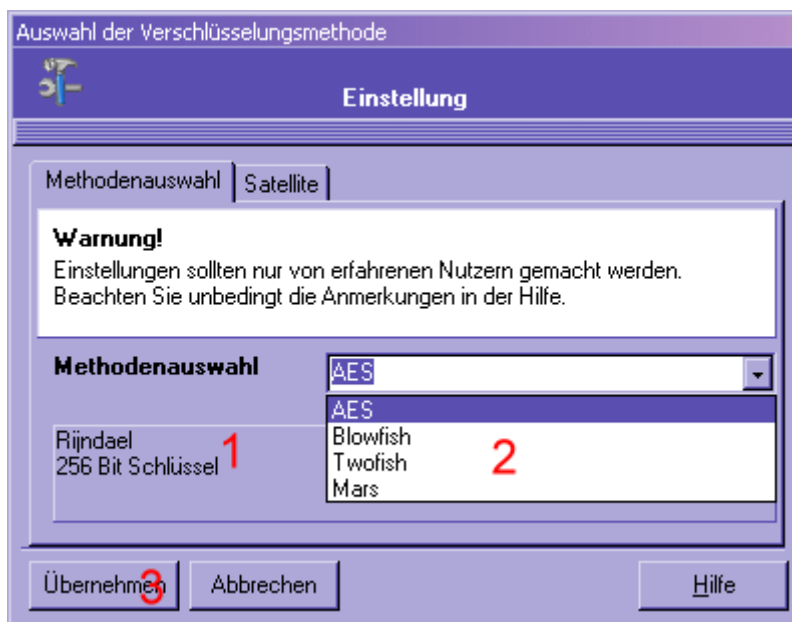
Die Schlüsseldatei **2** wird jetzt geladen und auf Gültigkeit überprüft. Falls es sich um eine kennwortgeschützte Schlüsseldiskette (siehe Schlüsseldiskette erstellen) handelt, wird zunächst das Passwort abgefragt (siehe Passwortdialog). Wenn das Passwort gültig ist wird geprüft, ob eventuell eine Gültigkeitsdauer eingegeben wurde. Die Gültigkeit wird bei **3** angezeigt. Falls die Schlüsseldatei ungültig ist, wird sie nicht geladen.

Die Prüfsumme **4** ist eine Zahl, die die Schlüsseldatei eindeutig identifiziert. D.h. anhand dieser Zahl können Sie die Schlüsseldatei identifizieren, auch wenn die Schlüsseldatei umbenannt wurde. Die Zahl läßt allerdings keinerlei Rückschlüsse auf den eigentlichen Schlüssel oder ein eventuell verwendetes Passwort zu.

Nachdem der Schlüssel geladen wurde, können Sie diesen durch Betätigen der Schaltfläche Übernehmen **5**, als Sitzungsschlüssel übernehmen.

3.8.7 Einstellungen

Wählen Sie in der Auswahlbox 2 die gewünschte Verschlüsselungsmethode aus. Bei 1 sehen Sie den Namen und die Schlüssellänge die bei dieser Methode bei ArchiCrypt zur Anwendung kommt.

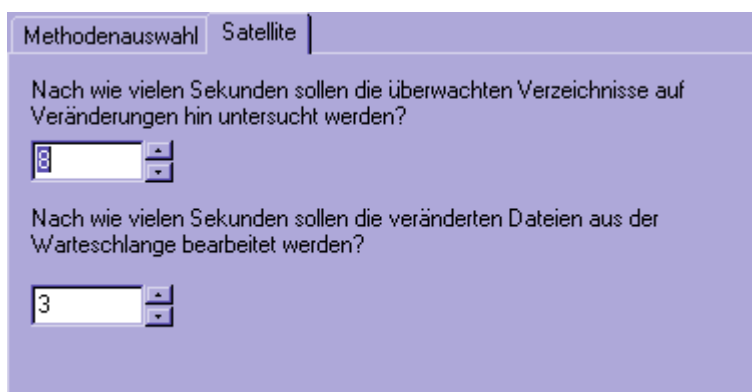


HINWEIS:

Die Einstellungen auf dieser Seite wirken sich unmittelbar auf die Sicherheit der Daten aus, die mit ArchiCrypt bearbeitet werden. Informieren Sie sich sehr genau über die Sicherheit der von Ihnen gewählten Methode. Es wurden nur Methoden in ArchiCrypt aufgenommen, die zum Zeitpunkt der Erstellung keine kryptografischen Schwachstellen aufzeigten.

Die Dateien die mit ArchiCrypt verschlüsselt werden, enthalten keinerlei Hinweis darauf, mit welchem kryptografischen Verfahren sie bearbeitet wurden. Dies bedeutet, dass Sie sich bei jeder verschlüsselten Datei neben dem Passwort, zusätzlich die Methode merken müssen.

Satellite



1. Wert

Satellite untersucht die Verzeichnisse nach bestimmten Zeitintervallen auf Veränderungen. Da es nicht damit getan ist, eine Dateigröße oder ein Datum zu vergleichen, um festzustellen, ob sich

eine Datei geändert hat, sondern umfangreiche Untersuchungen notwendig sind, können diese Operationen sehr zeitaufwendig sein, wenn sich viele Dateien in den überwachten Verzeichnissen befinden. Je niedriger der eingestellte Wert ist, um so länger befinden sich geänderte Dateien in den überwachten Verzeichnissen, ohne dass ArchiCrypt diese entdeckt und behandelt.

2. Wert

Entdeckt ArchiCrypt geänderte Dateien, fügt er diese in eine s.g. Warteschlange. Diese Warteschlange wird in bestimmten Zeitabständen daraufhin untersucht, ob sich zu bearbeitende Einträge darin befinden.

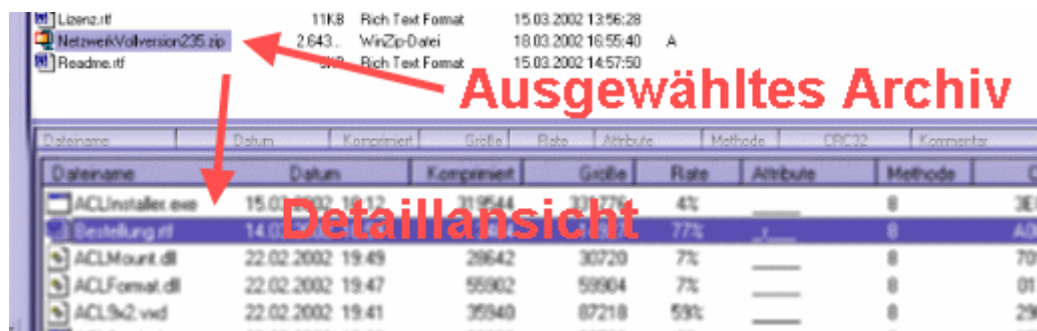
Sind beide Wert klein ≤ 2 , wird das System stark belastet, geänderte Dateien werden jedoch sofort erkannt und bearbeitet. Hohe Werte belasten das System wenig, führen jedoch dazu, dass Dateien länger unbehandelt bleiben.

3.9 Archive

3.9.1 Anzeige des Archivinhalts

ArchiCrypt ist kein Programm zum Komprimieren von Dateien, obwohl es dies ganz nebenbei erledigt. Bei jeder Verschlüsselung werden die Dateien immer auch komprimiert. Vor einer Verschlüsselung ist es oft hilfreich zu sehen, welche Dateien sich in einem speziellen Archiv befinden. Nützlich in diesem Zusammenhang sind auch Funktionen, mit denen man bestehende Archive bearbeiten kann.

Falls die entsprechende Option eingestellt ist (siehe Hauptmenü), werden die Inhalte von ZIP Archiven in der Detailansicht für Archive angezeigt.



Die im Archiv enthaltenen Dateien werden mit den Ihnen vertrauten Symbolen angezeigt. Um die **ZIP-Funktionen** aufzurufen, betätigen Sie bitte über der Detailansicht die rechte Maustaste. Es erscheint ein Kontextmenü mit Funktionen für ZIP-Archive (siehe Arbeit mit Archiven).

3.9.2 Arbeit mit Archiven

Wenn Sie den Mauszeiger über die Detailansicht für Archive bewegen und die rechte Maustaste bewegen, erscheint das nachfolgende **Kontextmenü für Archive** erscheint:

	Archiv entpacken [Pfad]	1
	Archiv entpacken [ohne Pfad]	2
	Datei(en) entpacken [Pfad]	3
	Datei(en) entpacken [ohne Pfad]	4
	Datei(en) löschen	5
	Anzeigen/Starten	6
	Installieren	7
	Fixieren	8

Die verfügbaren Funktionen sind davon abhängig, ob Sie Dateien in der Detailansicht ausgewählt haben, oder ob sich bestimmte Dateiformate im Archiv befinden.

1. Archiv entpacken [Pfad]

Sie müssen ein Zielverzeichnis angeben. Alle Dateien im Archiv werden mit enthaltenen Pfadangaben entpackt.

2. Archiv entpacken [ohne Pfad]

Wie unter 1. beschrieben, jedoch werden eventuell im Archive enthaltene Pfadangaben nicht berücksichtigt.

3. Datei(en) entpacken [Pfad]

Es werden die von Ihnen ausgewählten Dateien unter Berücksichtigung von Pfadangaben im Archiv entpackt.

4. Datei(en) entpacken [ohne Pfad]

Wie unter 3. beschrieben, jedoch werden eventuell im Archive enthaltene Pfadangaben nicht berücksichtigt.

5. Datei(en) löschen

Die von Ihnen ausgewählten Dateien werden aus dem Archiv entfernt.

6. Anzeigen/Starten

Sie müssen eine einzelne Datei auswählen und das Kontextmenü aufrufen. Die Funktion extrahiert die Datei in das temporäre Verzeichnis und ruft die mit der Datei verbundene Anwendung auf. Falls es sich um eine Anwendung handelt, wird diese gestartet.

7. Installieren

Diese Funktion ist nur dann verfügbar, wenn sich im ausgewählten Archiv eine Datei mit dem Namen Install.exe bzw. Setup.exe befindet. Dabei werden alle im Archiv enthaltenen Dateien in das temporäre Verzeichnis extrahiert und die Setup bzw. Install-Anwendung wird gestartet.

8. Fixieren

Bei ausgewählter Option bleibt das aktuell ausgewählte Archiv in der Detailansicht fixiert. Sie können jetzt beliebige Dateien im Dateimanager auswählen und diese per Drag&Drop auf die Detailansicht ziehen. Die Dateien werden dann in das Archiv eingefügt.

3.10 Log Bereich

3.10.1 Arbeit mit dem Log Bereich

Der **Log Bereich** hat zwei Funktionen. Protokollieren und Informieren. ArchiCrypt schreibt alle Vorgänge die im Zusammenhang mit der Ver- und Entschlüsselung stehen in den Log Bereich, sofern die Funktion eingeschaltet ist. Die Log Daten haben dabei einen ganz bestimmten Aufbau(siehe Aufbau der Logdateien). Spezielle Aktionen oder Zustände werden dabei in speziellen Farben dargestellt.

Die Inhalte des Log Bereichs können Sie **speichern**, **zurücksetzen** und **ausdrucken**. Die Funktionen erreichen Sie über das Kontextmenü des Log Bereichs.

Selbstverständlich können Sie **die Mitschrift/ das Protokoll um eigene Anmerkungen erweitern**.

3.10.2 Aufbau der Logdateien

Eine typische **Mitschrift** sieht wie folgt aus:

```

Logdatei für 19.03.2002 10:38:41
*****
+++++++
+ Methode: AES (Rijndael)
+ Benutzer: ATHLON
+ Rechner: ATHLON
+++++++
Alle Aktionen bei der Ver- und Entschlüsselung werden protokolliert.
ipcthrd.dcu wird komprimiert
ipcthrd.dcu Schlüsselberechnung
ipcthrd.dcu Verschlüsselung
Verschlüsselung von ipcthrd.dcu nach Dateiquellverzeichnis erfolgreich
Namenskollision >> ipcthrd <<
Kollision aufgelöst >> ipcthrd(1) <<
ipcthrd.pas wird komprimiert
ipcthrd.pas Schlüsselberechnung
ipcthrd.pas Verschlüsselung
Verschlüsselung von ipcthrd.pas nach Dateiquellverzeichnis erfolgreich
PrMemMqrTest.~dpr wird komprimiert

```

Wichtige Aktionen und Statusbegriffe werden in besonderen Farben dargestellt. Sie sollten sich die Logdatei näher betrachten, wenn Begriffe in roter Farbe dargestellt sind. Dabei kann es sich um Warnungen, Fehler oder kritische Aktionen handeln.

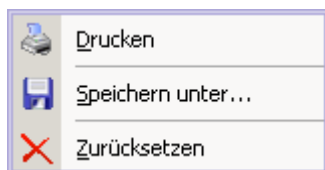
```

!WARNUNG!
Fehlerhaftes Passwort bei: I:\memtest\~$Gse7r7.doc
!HINWEIS!
Datei wurde vermutlich mit anderem Passwort oder anderer Methode verschlüsselt
!WARNUNG!
Entschlüsselung mit Fehlern vermutlich bei: I:\memtest\~$Gse7r7.doc
!HINWEIS!
Sehen Sie sich die Logdatei an

```

3.10.3 Kontextmenü des Log Bereichs

Das Kontextmenü des Log Bereichs hat folgendes Aussehen:



Drucken

Der aktuelle Inhalt des Log Bereichs wird auf Ihrem Standarddrucker ausgegeben.

Speichern unter...

In einem Dialog legen Sie den Namen und das Zielverzeichnis fest, unter dem Ihre Log Datei abgelegt werden soll.

Zurücksetzen

Alle Einträge werden entfernt.

Achtung:

Es werden auch alle von Ihnen eingegebenen Anmerkungen entfernt!

3.11 Statusleiste



Die Statusleiste gibt ständig Auskunft über verschiedene Einstellungen und Aktionen. Von links nach rechts bedeuten die verschiedenen Abschnitte:

Sitzungsschlüssel

rot : kein Schlüssel festgelegt
grün Sitzungsschlüssel verfügbar

Log

an: LogBuch ist angeschaltet
aus: LogBuch ist ausgeschaltet

ZIP

an: ZIP-Archivinhalt werden angezeigt
aus: ZIP-Archivinhalt werden nicht angezeigt

Fortschritt in Prozent

Der Fortschritt verschiedener Aktionen wird hier angezeigt

Beschäftigt

Grüne LED, wenn ArchiCrypt nicht beschäftigt ist, rote, wenn ArchiCrypt beschäftigt ist.

Pfeil nach oben:

Schriftgröße der Kurzhilfe vergrößern (Mausklick auf Symbol)

Pfeil nach unten:

Schriftgröße der Kurzhilfe verkleinern (Mausklick auf Symbol)

Aktuelle Uhrzeit

Aktuell ausgewählte Datei / Verzeichnis

3.12 Kurzhilfe

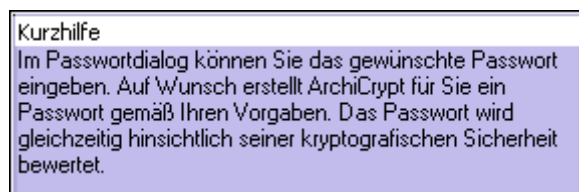
Bewegen Sie den Mauszeiger über das Bedienelement, über das Sie mehr erfahren möchten. Im Kurzhilfenfenster wird Ihnen eine knappe Hilfe präsentiert. Um eine ausführlichere Hilfe zu

erhalten, nutzen Sie die Schaltfläche **Was ist**



Dateiansicht zeigt Ihnen alle Dateien und Verzeichnisse, die sich im aktuell ausgewählten Verzeichnis befinden, oder dem Selfdecryptor zu bearbeiten.

Sie können das Kurzhilfenfenster an einer beliebigen Stelle positionieren und in der Größe ändern. Klicken Sie doppelt auf die mit dem roten Pfeil markierte schraffierte Leiste.



Um die Kurzhilfe wieder an die Ausgangsposition zurückzubringen, klicken Sie bitte auf die weiße Titelleiste.

Die Schriftgröße können Sie mit Hilfe der Pfeilsymbole in der Statusleiste verändern.

3.13 Fortschrittsanzeige

3.13.1 Die Fortschrittsanzeige

Die Fortschrittsanzeige hat neben der Funktion, den aktuellen Bearbeitungsstand zu visualisieren, die Aufgabe Ihnen eine Möglichkeit zu bieten, Aktionen abzubrechen.

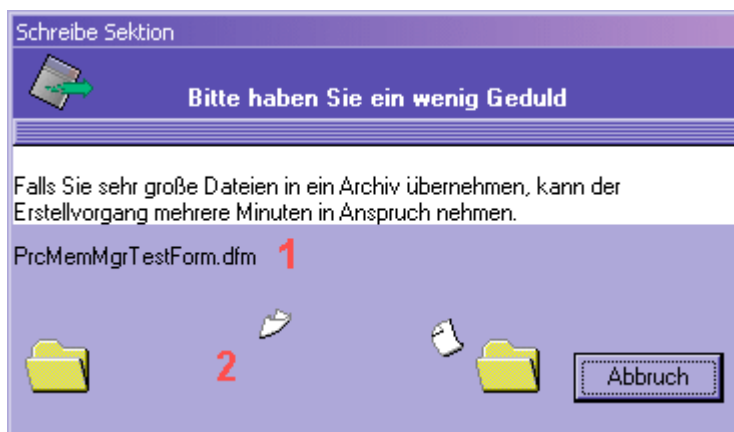
Die Fortschrittsanzeige bei "normaler" Ver-/Entschlüsselung:



Die Animation **1** zeigt an, dass ArchiCrypt arbeitet. Bei **2** wird der Name der aktuell bearbeiteten Datei angezeigt. Bei **3** können Sie den Fortschritt einer Kompression oder Dekompression sehen. Die Fortschrittsanzeige für Aktuelle Datei und Gesamt unterscheiden sich nur, wenn es sich um ein Archiv handelt. Falls ArchiCrypt mit einer Verschlüsselungsaktion beschäftigt ist, können Sie den Fortschritt bei **4** ersehen.

Falls Sie die **Aktion abbrechen** möchten, betätigen Sie die Schaltfläche "Abbruch". ArchiCrypt beendet die Arbeit dann kontrolliert.

Fortschrittsanzeige beim Erstellen von Selfdecryptor Dateien:



Der Name der aktuell bearbeiteten Datei wird bei **1** angezeigt, die Animation bei **2** zeigt, dass der Erstellvorgang noch im Gange ist. Beachten Sie bitte den Hinweis im Dialog.

ACHTUNG

Große Dateien (> 15 - 20 Megabyte) sollten nicht in eine Selfdecryptordatei eingebunden werden.

3.14 Zusammenarbeit mit MS Windows-Explorer

3.14.1 Zusammenarbeit mit MS Windows-Explorer

ArchiCrypt bietet selbst eine Oberfläche, die der des betriebssystemeigenen Datei-Explorers sehr ähnlich ist. Auch bewährte Techniken wie das s.g. Drag&Drop werden unterstützt. Die mit ArchiCrypt verschlüsselten Dateien können im normalen Windows Explorer entschlüsselt werden, sofern die Dateiendung .%\$% lautet. In diesem Fall genügt ein Doppelklick auf die Datei und es erscheint der Dialog zur Eingabe des Passwortes. Vorausgesetzt, Sie haben das richtige Passwort eingegeben, bzw. die korrekte Schlüsseldiskette angegeben, wird die Datei in das Verzeichnis entschlüsselt, in dem sich die Ausgangsdatei befindet.

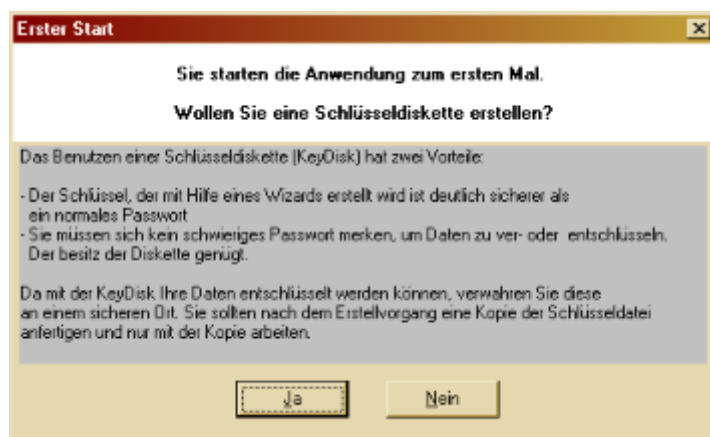
3.15 Erster Start

Nach der Installation, finden Sie den Eintrag des Programmes unter "Programme-ArchiCrypt 6"

WICHTIGER HINWEIS:

Unter Windows NT, Windows 2000 und Windows XP benötigen Sie zur Installation und für den ersten Start die Rechte eines lokalen **Administrators**. Falls Sie diese Rechte nicht besitzen, nehmen Sie bitte Kontakt mit Ihrem Administrator auf. Dieser kann Sie gegebenenfalls zusätzlich beim Erstelvorgang einer KeyDisk unterstützen und eine erste Einführung in das Programm geben.

ArchiCrypt 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 Schlüsseldiskette 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.

3.16 Beispiele

Verschlüsselung einer Einzeldatei mit einer KeyDisk:

Einstellungen:

```
+++++
+ Kein Archiv erstellen
```

+ Originaldateien erhalten
 + Zielverzeichnis ist Quellverzeichnis
 + Bei Namenskollision NACHFRAGEN (nur Verschlüsselung)
 + Sie arbeiten im Normalmodus
 ++++++

1. Legen Sie die Diskette in Ihr Diskettenlaufwerk ein.
2. Lesen Sie die Schlüsseldiskette wie unter "Schlüsseldiskette einlesen" beschrieben ein.
3. Wechseln Sie im Dateimanager in das Verzeichnis, welches die zu verschlüsselnde Datei enthält.
4. Markieren Sie die Datei im Dateimanager.
5. Lösen Sie den Verschlüsselungsvorgang über zum Beispiel die Schaltfläche der Schnellbefehle aus aus.

Verschlüsselung aller Dateien in einem Verzeichnis mit KeyDisk:

Einstellungen:

+ Kein Archiv erstellen
 + Originaldateien erhalten
 + Zielverzeichnis ist Quellverzeichnis
 + Bei Namenskollision NACHFRAGEN (nur Verschlüsselung)
 + Sie arbeiten im Normalmodus
 ++++++

Nr. 1-3 wie oben

4. Markieren Sie alle Dateien des Verzeichnisses.

HINWEIS:

Achten Sie darauf, dass keine Verzeichnisse, die sich im ausgewählten Verzeichnis befinden, mit markiert sind. Ansonsten werden darin enthaltene Dateien ebenfalls verschlüsselt.

Nr. 5 wie oben

Verschlüsselung eines Verzeichnisbaumes mit Passwort

Einstellungen:

+ Kein Archiv erstellen
 + Lösche Originaldateien
 + Zielverzeichnis ist G:\Ziel
 + Bei Namenskollision AUTOMATISCH umbenennen (nur Verschlüsselung)
 + Sie arbeiten im Expertenmodus
 + Es werden bei der Verschlüsselung zufällige Dateinamen vergeben
 + Die Datei erhält die Endung %\$\$%
 ++++++

1. Haben Sie bisher mit einem gültigen Passwort oder mit einer Schlüsseldiskette gearbeitet, müssen Sie den Passwortdialog aufrufen. Hat ArchiCrypt kein gültiges Kennwort, ruft er eigenständig den Passwortdialog auf.
2. Wählen Sie im linken Teil des Dateimanagers das Verzeichnis aus, welches hierarchisch über dem zu verschlüsselnden Verzeichnis liegt. Im rechten Teil sehen Sie jetzt das Verzeichnis, welches zu verschlüsseln ist.
3. Markieren Sie das Verzeichnis im rechten Teil des Dateimanagers.
4. Starten Sie den Verschlüsselungsvorgang.

3.17 Tastaturkürzel

Tastaturkürzel Ver-/Entschlüsselung

Start Entschlüsselung (Schnellbefehl)

<F11>

Start Entschlüsselung (Wizard)

<STRG> + <ALT> + <E>

Aufruf KeyDisk Dialog

<STRG> + <K>

Aufruf Methodenauswahl Dialog

<STRG> + <ALT> + <O>

Aufruf Passwortdialog

<STRG> + <P>

Sitzungsschlüssel löschen

<Strg> + <R>

Start Selfdecryptor (Schnellbefehl)

<F12>

Start Selfdecryptor (Wizard)

<STRG> + <ALT> + <S>

Start Verschlüsselung (Schnellbefehl)

<F10>

Start Verschlüsselung (Wizard)

<STRG> + <ALT> + <V>

Anwendung

Beenden der Anwendung

<STRG> + <ALT> + <X>

oder

<Alt> + F4

Wechseln zu

Dateimanager anzeigen

<F7>

Personalisierung anzeigen

<F8>

Satellite anzeigen

<F9>

Silent Modus einschalten

<Strg> + <Z>

Aufruf der Hilfe

<F1>

Tools

Inhalt von Zip-Archive anzeigen / ausblenden

<Strg> + <A>

Logbuch führen

<Strg> + <L>

Tastaturkürzel Dateimanager

Löschen ausgewählter Dateien in den Papierkorb

<Entf> oder

Löschen

<SHIFT> + <Entf>

oder

<STRG> + <Entf>

Kopieren

<STRG> + <C>

Ausschneiden

<STRG> + <X>

Einfügen

<STRG> + <V>

Neuen Order erstellen

<STRG> + <N>

Eintrag in Dateiansicht umbenennen

<F2>

Ansicht aktualisieren

<F5>

4 Umgang mit der Software

4.1 Umgang mit der Software

Die Software verwendet starke Verschlüsselungstechniken, die in Deutschland erlaubt, in bestimmten Ländern jedoch verboten sind. Bevor Sie das Programm mit ins Ausland nehmen, prüfen Sie zuvor, ob die in ArchiCrypt verwendeten Verfahren im Zielland erlaubt sind (siehe Eingesetzte Verfahren).

ArchiCrypt ist kein Kinderspielzeug. Verschlüsselte Daten sind unwiederbringlich verloren, wenn das Passwort nicht mehr verfügbar ist. Merken Sie sich die verwendeten Passwörter und die jeweils verwendete Methode gut. Selbst die Programmierer der Software sind nicht in der Lage verschlüsselte Daten ohne Kenntnis des Passwortes zu entschlüsseln. Bevor Sie eine Klartextdatei, die Sie verschlüsselt haben löschen, prüfen Sie auf jeden Fall zuvor die korrekte Funktionsweise der Entschlüsselung mit Ihrem Passwort.

Zum verantwortungsvollen Umgang mit der Software gehört es ebenfalls, dass man von wichtigen Daten regelmäßig Backup Dateien anlegt.

Verschlüsseln Sie keinesfalls Systemdateien oder Systemordner. Dies kann dazu führen, dass alle Daten Ihres Rechners zerstört werden.

5 Technischer Teil

5.1 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 denn Staat.

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

Sobald Sie Verbindung zum Internet aufgebaut ist, besteht die nicht zu unterschätzende Chance, das nicht nur Sie Zugriff auf die Daten im Internet haben, sondern andere, nicht ganz so gesetzestreue Zeitgenossen, 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. In meinem Berufsleben habe ich viele Mitarbeiter kennengelernt, die die eingebaute Möglichkeit von Kompressions- oder Office-Produkten nutzen. Der Krug geht eben so lange zum Brunnen bis er! Sie sagen es.

Sensible Daten, sollten während einer Surfsession nicht unverschlüsselt auf Ihrem Rechner sein. Gelangen die verschlüsselten 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.

5.2 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 eine extrem simple Verfahren verwendet, die 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.

5.3 Eingesetzte Verfahren

ArchiCrypt setzt per Voreinstellung den neuen AES (Advanced Encryption Standard) ein. Dieser Algorithmus ging aus einem Wettbewerb als Sieger hervor, der 3 Jahre andauerte und in dem die vorgestellten Methoden strengsten Untersuchungen unterzogen wurden. Man kann also davon ausgehen, das nach menschlichem Ermessen das "Knacken" des Verfahrens derart aufwendig ist, dass es auf lange Sicht nicht möglich ist.

In der Endausscheidung waren von den anfänglich 15 Verfahren noch 5 Kandidaten im Rennen. Obwohl die Verfahren von zum Teil äußerst renommierten Firmen eingebracht wurden, waren bei einigen Methoden schnell Schwachstellen und Lücken entdeckt. Dies sollte uns einmal mehr davor warnen, ein Verfahren unter Ausschluß der Öffentlichkeit zu entwickeln.

Die Methoden der Endrunde lieferten sich hinsichtlich der Leistungen ein Kopf an Kopf Rennen. Letztlich fiel folgende Entscheidung:

Rijndael:	86 Stimmen
Serpent:	59 Stimmen
Twofish:	31 Stimmen
RC6:	23 Stimmen
MARS:	13 Stimmen

Die Entscheidung zu Gunsten von Rijndael kam letztlich dadurch zu Stande, dass er die Anforderungen (siehe AES), die unterschiedlich gewichtet wurden, am besten erfüllte. Gleichzeitig bedeutet dies jedoch, dass die anderen Verfahren durchaus in bestimmten Einsatzgebieten bessere Eigenschaften aufweisen, als der Gewinner. Sicher, nach heutigem Verständnis, sind alle der oben aufgeführten Methoden.

Informationen über die Verfahren erhalten Sie unter den angegebenen Internetadressen:

- [MARS](#) - IBM
- [RC6](#) - RSA Laboratories
- [RIJNDAEL](#) - Joan Daemen, Vincent Rijmen
- [Serpent](#) - Ross Anderson, Eli Biham, Lars Knudsen
- [Twofish](#) - Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
- [Blowfish](#) - Bruce Schneier

Alle der aufgeführten Verfahren sind als Referenzimplementierung in der Programmiersprache C, teilweise auch in Java frei verfügbar. Zudem gibt es für jedes Verfahren s.g. Testvektoren, mit denen man sicherstellen kann, dass die Implementation

der Verfahren korrekt ist.

5.4 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 Einzelwörtern 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 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 und AES herauszuholen.

Zeichen der Tastatur als Passwort:

Wir haben 26 Groß- und 26 Kleinbuchstaben, 10 Ziffern und 42 Sonderzeichen zur Verfügung. Sie müssen sich nur noch ca. 38 Zeichen aus diesem Vorrat merken um ein sicheres Passwort zu haben. 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 Einzelwörter 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 mit AES 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 bei seiner Suche auf diese Zeichen beschränken kann. Mit der speziellen Möglichkeit bei ArchiCrypt, können Sie den gesamten Bereich der ASCII-Tabelle nutzen.

5.5 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 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)

5.6 Sinnvoller Einsatz von Schlüsseldisketten

Was ist eine Schlüsseldiskette?

Eine Schlüsseldiskette ist ein Wechselmedium. Im Normalfall handelt es sich um eine eine 3.5" Diskette. Eigentlich ist der Schlüssel bzw. die Schlüsseldatei nur 256 Byte groß und belegt auf der Diskette nur 1 Kilobyte. Die Datei kann auf jedem beliebigen Medium gespeichert werden. Sie sollten der Datei allerdings tatsächlich eine eigene Diskette gönnen.

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.

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.

5.7 AES

Das NIST (National Institute of Standards and Technology) rief 1997 weltweit dazu auf, ein neues symmetrisches Verschlüsselungsverfahren zu entwickeln.

Am 02.10.2000 erklärte der amerikanische Staatssekretär Norman Mineta den Algorithmus der beiden belgischen Kryptographen Joan Daemen von der Firma Proton-Welt International und Vincent Rijmen Mitglied von der Katholischen Universität Leuven zum neuen Standard der Nation.

Der Rijndael Algorithmus ist damit der Gewinner eines dreijährigen Wettbewerbes, an denen sich einige der führenden Kryptographen der Welt beteiligten.

Der Wettbewerb selbst wurde mit großer Begeisterung aufgenommen. Auf der 2. AES-Konferenz am 22./23. März 1999 in Rom wurden die zur Diskussion stehenden Algorithmen sowie die dazu durchgeführten Analysen vorgestellt und diskutiert. Die Konferenz hatte ca. 180 Teilnehmer aus 23 Ländern und es wurden 21 White-Papers vorgestellt. In der ersten Runde gab es hierzu 15 Vorschläge, aus welchen in mehreren Schritten der endgültige AES Algorithmus ausgewählt werden sollte. Informationen hierzu finden Sie unter <http://www.nist.gov/aes>.

In der zweiten Runde gab es noch die Kandidaten: **MARS**, RC6, **Rijndael**, Serpent und **Twofish**. (siehe auch Eingesetzte Verfahren)

Der Gewinner sollte folgenden Anforderungen genüge leisten:

Aufruf des NIST vom 12.09.1997

Symmetrische Blockchiffre

- Unterstützt mindestens die Schlüssellängen 128, 192 und 256 bits und eine Blocklänge von 128 bits
- Besser als derzeitige Verfahren: Sicherer und effizienter (hinsichtlich Laufzeit, Platzbedarf auf Chip) als Triple-DES
- Einsetzbar in verschiedenen Anwendungsumgebungen
- Verwendbar für Stream Cipher, Message Authentication Code (MAC) Generator, Pseudozufallszahlen-Generator, Hashfunktion etc.
- Implementierbar in Hard- und Software
- Weltweit lizenzfrei verfügbar
- Sicherheit soll für 20-30 Jahre gewährleistet sein
- Der Algorithmus soll öffentlich definiert und evaluiert sein.

War es bisher ein Privileg von Regierungen und Militärs, sensible Daten mit kryptographischen Mitteln zu schützen, verwendet heute fast jeder solche Mittel, ohne es zu merken. Beim Surfen im Internet, bei der Nutzung von Pay-TV, beim Gebrauch der EC-Karte, beim Telefonieren usw.

Das neue AES-Verfahren wird sich auf unseren gesamten Lebensbereich ausdehnen. Alle

Unternehmen und Dienstleister werden das Verfahren einsetzen.

5.8 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 noch als relativ sicher einstuft. Aber wie lange noch?

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 nutzt daher Ihre Mausbewegungen zur Erzeugung eines **Zufallszahlenpools**.

5.9 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 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 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 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.

5.10 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. Man erhält 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 Passwörter 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.

5.11 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.

5.12 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 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.

Index

- " -

"Angewandte Kryptographie" von Bruce Schneier 46

- A -

Administratorrechte 5
 Aktion abbrechen 37
 Aktualisieren 6
 Algorithmus 45
 Anpassen der Größe 11
 Anpassen des Dialoges 10
 Ansicht 6
 Anzeigen 34
 Anzeigen/Starten 34
 ArchiCrypt Online 6
 Archiv 20
 Archiv entpacken [ohne Pfad] 34
 Archiv entpacken [Pfad] 34
 Archive entpacken [Pfad] 33
 Art der KeyDisk festlegen 28
 Arten von Schlüsseldisketten 28
 asymmetrische Verfahren 43
 auf der Empfängerseite keinerlei zusätzliche Programme zur Entschlüsselung 12
 Aufruf des Selfdecryptors 6
 Aufruf Methodenauswahl Dialog 41
 ausdrucken 35

- B -

Basisoperationen 14
 Beenden der Anwendung 6
 Beispiele für den Einsatz des Satellite 18
 Bewertung Ihres Passwortes 24
 Blockchiffre 47
 Brute Force 46
 Brute-Force 48

- D -

Datei 6

Datei(en) entpacken [ohne Pfad] 34
 Datei(en) entpacken [Pfad] 34
 Datei(en) löschen 34
 Dateimanager 5, 9
 Dateimanageransicht 5
 Der Selfdecryptor ist High Tech. 12
 Der Selfdecryptor ist personalisierbar. 12
 Dialog zum Einlesen einer Schlüsseldiskette/KeyDisk 31
 Die Fortschrittsanzeige bei "normaler" Ver-/Entschlüsselung 37
 Durchführung komplexer Arbeitsabläufe 15

- E -

Eigenschaft festlegen 26
 Eingabe des Passwortes 24
 Eingabe eines Passwortes zur Entschlüsselung 24
 Eingabe eines Passwortes zur Verschlüsselung 24
 Einstellen der Verschlüsselungsmethode 32
 Einstellungen 6
 Einweg-Eigenschaft 48
 Einweg-Hashfunktionen 48
 Emailadresse auch einen Betreff und einen kurzen Text beifügen 10
 Entropie 49
 Entropie einer Datei 49
 Entropiewert 49
 Entschlüsseln 6
 Entschlüsseln von Dateien 14
 Erstellen selbstentschlüsselnder Dateien 14
 Erstellen von Listeneinträgen 20
 Erster Start 39
 Extremwerte 49

- F -

Festlegen des Zoomfaktors 11
 Filesharing 21
 Fixieren 34
 formatierte Texte 11
 Fortschrittsanzeige beim Erstellen von Selfdecryptor Dateien 37
 FTP-Server 21
 Web-Server 21
 Für wen eignet sich eine Schlüsseldiskette? 46

- G -

Grafik in ein Graustufenbild umwandeln 11
 Gütegrad 26

- H -

Hashfunktion 48
 Hauptmenü 6
 Hex Code 24
 Hilfe 6
 HKEY_CLASSES_ROOT\rem 5
 Hybrid-Codierung 43

- I -

Informationsgehalt 49
 Informieren 35
 Inhalte von ZIP-Archiven angezeigt 6
 Installation 39
 Installieren 34

- K -

KeyDisk 6, 20, 28, 39
 Keylogger 24
 Kontextmenü für Archive 33
 Kontrast 11
 Farb- und Helligkeitswerte festlegen 11

- L -

Laden einer Grafik 11
 Länge des Schlüssels 48
 Letzte Aktion rückgängig machen 11
 Listenpasswort 18
 Log Bereich 35
 LogBuch 6
 Logdatei 18
 Logdatei ansehen 21
 Logdatei erstellen 19
 Logo 11

- M -

MARS 44, 47

Methode 45
 mit den Wizards viele Spezialfunktionen nutzen
 15
 Mit welchem Schlüssel sollen die Dateien bearbeitet
 werden 15, 16, 17
 Mitschrift/Protokoll um eigene Anmerkungen
 erweitern 35
 Mooreschen Gesetz 48

- N -

Name 20
 Namen für die Datei angeben 14
 National Institute of Standards and Technology 47
 neue Schlüsseldiskette 6
 Neuigkeiten oder Produktupdates 6
 NIST 47

- O -

offene Eingabe des Passwortes 24

- P -

Passphrase (Merksatz) 23
 Passwort 6, 20
 Passwort festlegen 28
 Passwörter erstellen 26
 Personalisierer 5
 Protokollieren 35

- R -

Radiergummi 23
 RC6 44
 Rechte eines lokalen Administrators 39
 Rijndael 44, 47

- S -

Satellite 5, 18
 Schlüssel 6
 Schlüsseldatei speichern 28
 Schlüsseldiskette 6
 Schlüsseldiskette(KeyDisk) 23
 Schlüsseleingabe 23
 Schlüssels 14
 Schnellbefehle 5, 9

Schnittstelle zu ArchiCrypt Safe 24, 45
 Schreiben nach 20
 Schriftgröße der Kurzhilfe vergrößern 36
 Schriftgröße der Kurzhilfe verkleinern 36
 Schutz der Anwendung 23
 selbstentschlüsselnde Datei erstellen 14
 Serpent 44
 Silent Modus 23
 Sitzungsschlüssel 23
 Soll die Datei versendet werden 17
 Soll die Datei zusätzlich in ein Archiv gepackt werden 17
 Sollen die Dateien in eine Datei geschrieben werden 15
 Sollen die Originaldateien gelöscht werden 15, 16, 17
 speichern 35
 Speichern der Grafik 11
 Statusleiste 36
 symmetrische Verfahren 43

- T -

Tastaturkürzel Dateimanager 41
 Tastaturkürzel Ver-/Entschlüsselung 41
 Texteditor 11
 Tools 6
 Trojaner 24
 Trojanern 24
 Twofish 44, 47

- U -

Überschrift 10
 Überwachen von 20
 Überwachungsliste 18

- V -

verdeckte Eingabe 24, 26
 verdeckte Eingabe des Passwortes 24
 Verknüpfte Internetadresse 10
 Verschiedene Grafikfilter und Effekte 11
 Verschlüsseln 6
 Verschlüsseln von Dateien 14
 Verschlüsselung aller Dateien in einem Verzeichnis 39

Verschlüsselung aller Dateien in einem Verzeichnis mit KeyDisk 39
 Verschlüsselung einer Einzeldatei 39
 Verschlüsselung einer Einzeldatei mit einer KeyDisk 39
 Verschlüsselungsmethode 6, 32
 Verschlüsselungsverfahren 43
 Versenden vertraulicher Dokumente 21
 Verteilen vertraulicher Dokumente 21
 virtuelle Tastatur 26
 Vorgehen beim Erstellen einer Selfdecryptor Datei 12
 Vorschau des Dialoges 10

- W -

Was ist eine Schlüsseldiskette? 46
 Was tun 20
 Wechseln zu 6
 Welche Dateien möchten Sie entschlüsseln 16
 Welche Dateien möchten Sie verschlüsseln 15
 Wie soll die selbstentschlüsselnde Datei benannt werden 17
 Wie sollen Dateien benannt werden 15
 Wie sollte man mit der Schlüsseldiskette umgehen? 46
 Wizards 5, 9
 Wo möchten Sie die entschlüsselten Dateien speichern 16
 Wo möchten Sie die verschlüsselten Dateien speichern 15
 Wo soll Sie abgelegt werden 17
 Wörter 45
 die Sie auf keinen Fall als Passwort benutzen sollten 45

- X -

XOR 50

- Z -

Zahlen als Passwort 45
 Zeitliche Gültigkeit festlegen 28
 Zeitverhalten des Satellite beeinflussen 19
 Zip-Archive 6
 ZIP-Funktionen 33
 Zufallsdaten 48
 Zufallsdaten sammeln 28

Zufallssequenz 48
Zufallszahlenpool 48
zurücksetzen 35