/help/deutsch/DiskProtection

COLLABORATORS			
	TITLE : /help/deutsch/DiskProtection		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		March 6, 2025	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

1 /help/deutsch/DiskProtection 1

1.1 /help/deutsch/DiskProtection.guide . . . 1
1.2 DiskProtection.guide/Rechtliches . . . 2
1.3 DiskProtection.guide/Copyrights . . . 2
1.4 DiskProtection.guide/Haftungsausschluss . . . 3
1.5 DiskProtection.guide/Lizenz . . . 3
1.6 DiskProtection.guide/Ueberblick . . . 4
1.7 DiskProtection.guide/Installation . . . 5
1.8 DiskProtection.guide/Konzept . . . 5
1.9 DiskProtection.guide/Ansatz . . . 6
1.10 DiskProtection.guide/Units . . . 6
1.11 DiskProtection.guide/DOS-Devices . . . 7
1.12 DiskProtection.guide/Verschlüsselung . . . 8
1.13 DiskProtection.guide/Passwörter . . . 8
1.14 DiskProtection.guide/Passwort . . . 9
1.15 DiskProtection.guide/Systempasswort . . . 9
1.16 DiskProtection.guide/Reset . . . 10
1.17 DiskProtection.guide/Passwort resetfest machen . . . 10
1.18 DiskProtection.guide/In Datei verstecken . . . 10
1.19 DiskProtection.guide/Zugangsschutz . . . 11
1.20 DiskProtection.guide/DiskProtection . . . 12
1.21 DiskProtection.guide/Preferences-Konzept . . . 13
1.22 DiskProtection.guide/Programmstart . . . 13
1.23 DiskProtection.guide/Speichern der Einstellungen . . . 13
1.24 DiskProtection.guide/Hauptfenster . . . 14
1.25 DiskProtection.guide/Units und Passwoerter . . . 15
1.26 DiskProtection.guide/Neu . . . 15
1.27 DiskProtection.guide/Editieren . . . 15
1.28 DiskProtection.guide/Entfernen . . . 16
1.29 DiskProtection.guide/System-Verschluesselung . . . 16

1.30 DiskProtection.guide/Einstellungen Zugangsschutz . . . 16
1.31 DiskProtection.guide/Blanker-Hotkey . . . 17
1.32 DiskProtection.guide/Aktivieren nach # Sek. . . . 17
1.33 DiskProtection.guide/Beim Programmstart . . . 17
1.34 DiskProtection.guide/Screenmode u. -font . . . 17
1.35 DiskProtection.guide/Dimmer + Blanker-Zeitsp. . . . 18
1.36 DiskProtection.guide/Standard-Gadgets . . . 18
1.37 DiskProtection.guide/Menus . . . 18
1.38 DiskProtection.guide/Projekt . . . 19
1.39 DiskProtection.guide/Vorgaben . . . 19
1.40 DiskProtection.guide/Optionen . . . 19
1.41 DiskProtection.guide/DPUnit Editieren . . . 20
1.42 DiskProtection.guide/DPUnit . . . 20
1.43 DiskProtection.guide/Datenschutz . . . 20
1.44 DiskProtection.guide/Algorithmus . . . 21
1.45 DiskProtection.guide/Passwort Wahl . . . 21
1.46 DiskProtection.guide/Erweiterte Einstellungen . . . 21
1.47 DiskProtection.guide/Device . . . 22
1.48 DiskProtection.guide/Unit . . . 22
1.49 DiskProtection.guide/FFS-Patch Aktiviert . . . 22
1.50 DiskProtection.guide/Anmeldedateien . . . 22
1.51 DiskProtection.guide/DOS-Device . . . 23
1.52 DiskProtection.guide/Mountlist-Eintrag Neu . . . 23
1.53 DiskProtection.guide/Mountlist-Eintrag Kopieren . . . 23
1.54 DiskProtection.guide/Mountlist-Eintrag Editieren . . . 23
1.55 DiskProtection.guide/Mountlist-Eintrag Löschen . . . 24
1.56 DiskProtection.guide/Mounten . . . 24
1.57 DiskProtection.guide/Beim Booten Mounten . . . 24
1.58 DiskProtection.guide/Passwort Editieren . . . 24
1.59 DiskProtection.guide/Passwortname . . . 25
1.60 DiskProtection.guide/Wartezeit . . . 25
1.61 DiskProtection.guide/Passwort Eingabe . . . 25
1.62 DiskProtection.guide/Resetfest . . . 26
1.63 DiskProtection.guide/Verstecken . . . 26
1.64 DiskProtection.guide/Dateiname . . . 26
1.65 DiskProtection.guide/Units des Passworts . . . 26
1.66 DiskProtection.guide/Requester . . . 27
1.67 DiskProtection.guide/Automatische Unit-Aenderung . . . 27
1.68 DiskProtection.guide/DOS-Device auswaehlen . . . 28

1.69 DiskProtection.guide/Algorithmus und Modus auswaehlen 28
1.70 DiskProtection.guide/diskprot.device 29
1.71 DiskProtection.guide/Passworteingabe 29
1.72 DiskProtection.guide/Unit-Konvertierung 29
1.73 DiskProtection.guide/Konvertierungs-Fehler 30
1.74 DiskProtection.guide/DPInit 31
1.75 DiskProtection.guide/Grundlagen 31
1.76 DiskProtection.guide/Hash-Wert 32
1.77 DiskProtection.guide/Block-Verschluesselung 33
1.78 DiskProtection.guide/DES 33
1.79 DiskProtection.guide/IDEA und FEAL 35
1.80 DiskProtection.guide/SCRM 35
1.81 DiskProtection.guide/Frage & Antwort 36
1.82 DiskProtection.guide/History 37
1.83 DiskProtection.guide/Zukunft 37
1.84 DiskProtection.guide/Adresse 38
1.85 DiskProtection.guide/Credits 38
1.86 DiskProtection.guide/Standardwerte 39
1.87 DiskProtection.guide/Glossar 40
1.88 DiskProtection.guide/Index 40

Chapter 1

/help/deutsch/DiskProtection

1.1 /help/deutsch/DiskProtection.guide

```
DiskProtection
**************

   DiskProtection  ist ein Datenschutzpacket für den Amiga, das die
Datenblöcke beim Zugriff auf Diskette transparent ver- und
entschlüsselt.

   Diese Anleitung beschreibt DiskProtection  V1.2.


Einführung
  Rechtliches       Status von DiskProtection
  Ueberblick        Kurzfassung der Features
  Installation      Wie wird DiskProtection  installiert?
  Konzept           Die Grundideen von DiskProtection
  Grundlagen        Methoden der Kryptologie

Bedienung
  DiskProtection    Das Preferences-Programm
  diskprot.device   Passworteingabe, DPUnit-Konvertierung, etc.
  DPInit            Starten des DiskProtection Systems

Verschiedenes
  Frage & Antwort   Bekannte Probleme, Tips & Tricks
  History           Bisherige Programmversionen
  Zukunft           Was kommt in der nächsten Version?
  Adresse           Wie erreiche ich den Autor?
  Credits           Vielen Dank an ...

Anhang
  Standardwerte     für Passwörter und System-Einstellungen
  Glossar           einige Begriffe
  Index             Stichwortregister
```

1.2 DiskProtection.guide/Rechtliches

```
Rechtliches
***********


  Copyrights           Warenzeichen, Produktbezeichnungen
  Haftungsausschluss   Benutzung auf eigene Gefahr
  Lizenz               DiskProtection  ist Shareware
```

1.3 DiskProtection.guide/Copyrights

```
Copyrights
==========

DiskProtection und seine Dokumentation
     (C) 1994,95 Patrick Ohly

xpkFEAL
     (C) 1992,93 Christian von Roques

FEAL-N
     patentiert durch
     Intellectual Property Department, NTT
     1-6 Uchisaiwai-cho, 1-chome, Chiyada-ku
     100 Japan

xpkIDEA
     (C) 1992 André Beck

IDEA, International Data Encryption Algorithm
     patentiert durch
     Ascom-Tech AG, Solothurn Lab
     Postfach 151
     4502 Solothurn, Schweiz

MD5 Message-Digest Algorithm
     (C) 1990, RSA Data Security, Inc.

D3DES
     (C) 1988-92 bei Richard Outerbridge

Triton, Oberflächen-Library
     (C) 1993-1995 Stefan Zeiger

Icons
     (C) Michael-Wolfgang Hohmann (mickh@iM.Net). Sie dürfen nur mit
     seiner schriftlichen Genehmigung in anderen Projekten verwendet
     werden.

   Registrierte Warenzeichen sind in dieser Anleitung nicht als solche
gekennzeichnet; fehlt ein Hinweis, heißt das also nicht, daß der Name
frei ist!
```

1.4 DiskProtection.guide/Haftungsausschluss

Haftungsausschluß
==========

Es gibt keine Garantie für Benutzer von DiskProtection, soweit es nicht durch gültiges Recht gefordert wird. Soweit nicht anders schriftlich festgelegt, stellt der Besitzer des Copyrights und jeder Dritte, der das Paket verteilt, das Programm "wie es ist" zur Verfügung, ohne irgendeine Garantie, implizit oder explizit, über, aber nicht beschränkt auf, die Eignung für einen bestimmten Zweck. Sie tragen das alleinige Risiko was die Qualität und Benutzung des Programms betrifft. Sollte sich das Programm als defekt erweisen, so tragen Sie die Kosten für alle nötigen Serviceleistungen, Reparaturen oder Nachbesserungen.

In keinem Fall, soweit nicht durch gültiges Recht gefordert oder durch schriftliche Einwilligung gewährt, wird der Besitzer des Copyrights oder irgendein Dritter Ihnen für Schäden haften, einschließlich irgendwelcher allgemeiner, spezieller, zufälliger oder sich ergebender Schäden, die aus der Benutzung des Programms oder Unvermögen seiner Benutzung (einschließlich, aber nicht beschränkt auf den Verlust von Daten, verfälschte Daten, Verluste, die Sie oder Dritte erlitten haben oder Fehler des Programms bei der Benutzung zusammen mit anderen Programmen), auch wenn der Besitzer des Copyrights oder ein Dritter über die Möglichkeit eines solchen Schadens informiert wurden.

1.5 DiskProtection.guide/Lizenz

Lizenz
======

DiskProtection wird als Shareware vertrieben. Das Paket darf frei verteilt werden, solange diese Punkte erfüllt sind:

1. Jede Weitergabe muß alle Dateien in diesem Achriv ohne Änderung umfassen.

2. Dieses Paket darf frei weitergegeben werden über Mailboxen, InterNet/UseNet, Software-Bibliotheken wie die von Fred Fish und Aminet CD-ROM’s und andere ähnliche elektronische Kanäle.

3. Disketten-Magazine und Dienstleister, die Zusatzgebühren für Dateiübertragung erheben, dürfen es nicht ohne Erlaubnis des Autors verteilen!

Wenn Sie das Programm regelmäßig verwenden wollen, sollten Sie mir mindestens 20,-DM oder einen entsprechenden Betrag in anderer Währung

schicken. Bitte beachten Sie, daß Schecks ausländischer Banken z.T. nur unter Schwierigkeiten eingelöst werden können. Euroschecks oder Bargeld werden bevorzugt.

Falls die Bezahlung des Shareware-Betrages zu große Schwierigkeiten machen sollte oder das Programm dazu zu selten genutzt wird, bin ich auch mit einer interessanten Postkarte oder einer anderen Aufmerksamkeit zufrieden. Für die Registrierung füllen Sie bitte die Datei Registrierung aus und schicken Sie sie mir per eMail oder Post zu.

Diese Version von DiskProtection ist in keiner Weise eingeschränkt. Der Shareware-Beitrag ist also eine Bezahlung für die Ware, die Sie bereits erhalten habe. Er berechtigt auch zur Nutzung zukünftiger Versionen. Registrierte Benutzer können auf Wunsch auch die neueste Version per eMail zugeschickt bekommen. Per Post ist dies jedoch nur gegen zusätzliche Bezahlung des nötigen Portos möglich.

Neue, verbesserte Versionen wird es aber nur geben, wenn ich genügend motiviert werde und sich dieses Konzept bewährt (Zuckerbrot ...). Ansonsten könnte es sein, daß die nächsten Versionen nur für registrierte Benutzer voll funktionsfähig sein werden (... und Peitsche).

1.6 DiskProtection.guide/Ueberblick

Überblick
****

DiskProtection verschlüsselt Daten völlig transparent für den Benutzer beim Schreiben auf Diskette. Es werden die einzelnen Diskblöcke verschlüsselt, daher wird auch das Inhaltsverzeichnis geschützt. DiskProtection unterstützt alle Exec-Geräte, also Festplattenpartitionen, Disketten, etc., nicht jedoch die RAM-Disk. Sie können weiterhin jedes beliebige Filesystem einsetzen.

Verschlüsselt wird mit IDEA, FEAL oder DES. Falls die XPK-Schnittstelle zu den Sub-Libraries verbessert werden sollte, könnten diese und andere Algorithmen auch über XPK angesprochen werden. Es werden beliebig viele Passwörter verwendet.

Passwörter werden beim ersten Zugriff auf ein Gerät abgefragt. Sie lassen sich jedoch auch nach der ersten Eingabe resetfest im Speicher ablegen, damit sie nach einem Reset nicht neu abgefragt werden müssen. So kann DiskProtection auch für Mailboxen ohne ständige Aufsicht verwendet werden. Alternativ können die Passwörter auch auf Festplatte in beliebigen Dateien versteckt werden. Der Rechner kann vor unbefugter Benutzung geschützt werden.

Es gibt ein Preferences-Programm mit grafischer Benutzeroberfläche. Die Verschlüsselung einer Partition kann jederzeit umgestellt werden. Die Partition wird vom Programm automatisch neu verschlüsselt, unverschlüsselte Daten können also übernommen werden.

DiskProtection läuft auf jedem Amiga mit mindestens OS 2.0. Es hat

eine grafische Benutzeroberfläche, die mit Triton V1.3 gestaltet wird. Die Locale-Library wird unterstützt, Kataloge und Übersetzungen der kompletten Anleitung gibt es in Englisch und Deutsch. Die Anleitungen liegen im AmigaGuide-, ASCII- und DVI-Format vor und können jederzeit als kontextsensitive Online-Hilfe aufgerufen werden.

1.7 DiskProtection.guide/Installation

Installation von DiskProtection
****

DiskProtection wird mit dem Commodore-Installer installiert. Sie haben die Auswahl zwischen zwei Installationsmöglichkeiten: Alles in einem eigenem Verzeichnis mit den entsprechenden Assigns in der user-startup oder jeden Programmteil in das Verzeichnis, wo sie normalerweise gesucht werden würden.

Zum Testen des Programms genügt es, durch die Batch-Datei MakeAssigns die nötigen Assigns zu setzen. Achtung: Wenn Sie dann DiskProtection starten, werden auf jeden Fall die Dateien ENV[ARC]:diskprot.prefs angelegt.

DiskProtection ist mit PGP und MD5-Prüfsummen vor Manipulation geschützt. Bei der Installation werden die in der Datei DiskProtection.readme abgelegten Prüfsummen automatisch mit den dazugehörenden Dateien verglichen. Die Prüfsummen selbst sind durch eine PGP-Signatur geschützt, die jedoch manual geprüft werden muß. Dazu starten Sie PGP mit dieser Datei als Argument. Mein PGP-Public-Key steht am Anfang dieser Datei. Anhand der Unterschriften können Sie entscheiden, ob Sie ihn für gültig halten.

Hinweis für WB 2.04 Benutzer: Die Asl-Library dieser WB-Versionen bietet noch keinen Screenmode-Requester. DiskProtection verwendet dafür statt dessen die ReqTools-Library, falls installiert. Sie können auch ohne diese Library weiterhin alle anderen Features von DiskProtection verwenden, nur die Auswahl eines Screenmodes ist nicht möglich.

Da die ReqTools-Library weit verbreitet ist und nicht zwingend von DiskProtection benötigt wird, ist sie nicht in diesem Archiv enthalten. Sie finden Sie auf dem AmiNet als /util/libs/ReqTools#?.lha, falls Sie sie noch nicht haben sollten.

1.8 DiskProtection.guide/Konzept

Konzept von DiskProtection
****

In diesem Kapitel wird das Konzept von DiskProtection beschrieben.

Ansatz	Device contra Handler
Units	Basis des diskprot.devices
DOS-Devices	Auswahl des Filesystems, etc.
Verschlüsselung	Welche Algorithmen stehen zu Verfügung?
Passwörter	Arten, Verwendungen und Eingabe
Reset	Passwörter nach einem Reset
Zugangsschutz	Wie schütze ich meinen Computer vor Benutzung?

1.9 DiskProtection.guide/Ansatz

Ansatz von DiskProtection
==========

Es gibt genug Programme, die auf vielerlei Arten eine bestimmte Datei verschlüsseln. Das hat meist den Nachteil, das man die Datei erst wieder manuell entschlüsseln muß, bevor man sie mit anderen Programmen verwenden kann, oder man kann nur Programme verwenden, die auch selbst die verschlüsselte Datei lesen können.

Eine wesentlich komfortablere und vielseitigere Möglichkeit, seine Daten zu schützen, ist ein Filesystem, das die Daten beim Schreiben und Lesen transparent für das Anwendungsprogramm ver- und entschlüsselt oder den Zugriff darauf kontrolliert, indem es das normale Filesystem ersetzt. Dafür gibt es z. B. das Programmpacket XFH, bei dem man die XPK-Libraries "IDEA" oder "FEAL" verwenden kann, um den Inhalt der Dateien zu schützen. Der größte Nachteil ist jedoch, daß man weiterhin auf der Festplatte die Filenamen und die Verzeichnisstruktur erkennen kann. So kann ein Unbefugter immer noch erkennen, was man auf der Platte liegen hat, auch wenn er den Inhalt der Dateien nicht lesen kann. Außerdem könnte er anhand des Namens Anhaltspunkte über den Inhalt einer Datei bekommen, was das Knacken der Verschlüsselung erleichtert.

DiskProtection geht daher einen anderen Weg. Sein Kernstück besteht aus einem Exec-Device, das jeden einzelnen Block verschlüsselt, bevor er auf Diskette oder Festplatte geschrieben wird. So können sie weiter jedes beliebige Filesystem verwenden. Ohne dieses Device und das korrekte Passwort, mit dem die Blöcke verschlüsselt wurden, erhält man nur eine "Unreadable Disk", auf der weder Dateinamen, Inhaltsverzeichnis noch Dateiinhalt zu lesen sind.

Dieses Konzept hat dafür einen anderen Nachteil: Einstellungen können jeweils nur für eine Unit und damit immer nur für eine ganze Partition oder Diskette gemacht werden. Die Unterscheidung verschiedener Verzeichnisse oder Dateien ist nicht möglich.

1.10 DiskProtection.guide/Units

```
Units des diskprot.devices
==========================
```

Das diskprot.device beruht wie jedes andere Exec-Gerät auch auf sogenannten Units. In diesem Fall ist jede DPUnit eine Einheit, für die völlig unabhängig von den anderen bestimmte Einstellungen getroffen werden können.

Da das diskprot.device nicht selbst auf die Hardware zugreift, sondern auch wieder andere Exec-Devices verwendet, ist die wichtigste Einstellung, auf welches Device und welche Unit dieses Devices zugegriffen wird. Das ist z. B. für DF0: das "trackdisk.device", Unit 0. Außerdem muß angegeben werden, welche Blöcke zu dieser Unit gehören, um auch Festplattenpartitionen verschlüsseln zu können. Wechselmedien werden besonders unterstützt. Bei diesen können Sie bei einer Umstellungen der Verschlüsselungsart beliebig viele Medien konvertieren.

Zur Verschlüsselungsart gehört der zu verwendende Algorithmus, sein Modus und das Passwort.

1.11 DiskProtection.guide/DOS-Devices

```
Anmeldedateien zum Mounten
==========================
```

Um überhaupt Daten auf eine Unit schreiben zu können, muß man erst mit dem MOUNT-Befehl ein DOS-Device mounten, das auf diese Unit zugreift. Dazu braucht MOUNT Einträge in einer Mountlist oder--in Workbench 2.1 eingeführt--einzelne Dateien in den Verzeichnissen DEVS:DOSDrivers, bzw. SYS:Storage/DOSDrivers. Die Geräte in DEVS:DOSDrivers werden ab 2.1 beim Booten automatisch durch die Startup-Sequence angemeldet, während Sie unter 2.0 selbst den MOUNT-Befehl für jede Unit eintragen müssen.

Falls das Verzeichnis DEVS:DOSDrivers existiert, dann legt DiskProtection dort Anmeldedateien an. Andernfalls werden Mountlist-Einträge in der Datei DEVS:DP-Mountlist verwaltet. Dann müssen Sie beim MOUNT-Befehl noch das Argument FROM DEVS:DP-Mountlist angeben! DiskProtection kann DOS-Drivers zwischen DEVS:DOSDrivers und SYS:Storage/DOSDrivers hin- und herschieben. Bei der Verwendung der Mountlist müssen Sie die DOS-Devices selbst mounten.

DiskProtection braucht auch selbst einen Teil der Informationen aus der Anmeldedatei, bzw. Mountlist: Das Device verwendet die Einträge SectorSize = BlockSize, SectorsPerTrack = BlocksPerTrack, BufMemType und Flags, falls sie vorhanden sind.

Wenn eine Unit konvertiert werden soll, werden die Anmeldedateien der Unit nach LowCyl, HighCyl, Surfaces und SectorsPerTrack = BlocksPerTrack durchsucht. Ohne diese Informationen kann nicht konvertiert werden.

Warnung: Wenn Sie per Hand eine Anmeldedatei erstellen sollten Sie STACKSIZE auf mindestens 4000 setzen!

1.12 DiskProtection.guide/Verschlüsselung

Verschlüsselung
==========

DiskProtection kann nur Verschlüsselungs-Algorithmen verwenden, die an der Länge eines Datenblocks nichts ändern. Die Datensicherheit liegt nur darin, daß das Passwort geheim gehalten wird, da die Algorithmen selbst bekannt sind.

Es gibt eine Schnittstelle zu den Sub-Libraries des XPK-Packets. Leider ermöglicht das bisherige XPK-Konzept keine Sub-Libraries, die einen Datenblock verschlüsseln, ohne Zusatzinformationen anzuhängen. Daher wurden mit Erlaubnis der Autoren xpkFEAL und xpkIDEA in das diskprot.device eingebaut. Falls das Konzept von XPK einmal überarbeitet werden sollte, dann könnten auch für diese Verschlüsselungsalgorithmen die Sub-Libraries verwendet werden.

Mehr Informationen zu den Hintergründen von Datenverschlüsselung und diesen Algorithmen finden Sie in Grundlagen.

1.13 DiskProtection.guide/Passwörter

Passwörter
==========

DiskProtection kennt mehrere Arten von Passwörter, die unterschiedlich verwendet werden. Allen gemeinsam ist jedoch, daß kein Passworttext irgendwo abgespeichert wird. Von einem Passwort wird nur ein sogenannter Hash-Wert gespeichert (mehr zu Hash-Werten in Hash-Wert). Dieser Wert wird nur verwendet, um zu überprüfen, ob ein eingegebenes Passwort richtig ist. Zur Datenver/entschlüsselung wird der Hash-Wert nicht verwendet, dazu braucht man weiterhin unbedingt das richtige Passwort.

Es gibt keine "Hintertür", um ein verlorenes Passwort anhand der Programm-Einstellungen herauszufinden!

Bei Passwörtern sind alle Zeichen erlaubt und Groß-/Kleinschreibung wird unterschieden. Ein Passwort darf fast beliebig lang sein und muß auch nicht aus einem einzigen Wort bestehen. Am sichersten wären eine zufällige Reihenfolge wirrer Zeichen, oder ein langer Satz. Auf keinen Fall sollten Sie ein einzelnes Wort nehmen, das irgendeinen Bezug zu Ihrem Namen oder Person hat, oder in einem Wörterbuch steht. Dies und Variationen davon würde ein Programm zum Ausprobieren von Passwörtern zuerst testen. Ein guter

Kompromiß ist, sich einen langen Satz zu merken, aber nur die Anfangsbuchstaben und Satzzeichen zu verwenden. Das Ergebnis ist meist recht zufällig, aber einfach zu merken.

Passwort	Schlüssel zu Datenverschlüsselung bei Units
Systempasswort	Schützt vor unbefugter Verwendung des Programms

1.14 DiskProtection.guide/Passwort

Passwort

Das Problem bei zu vielen Units und je einem Passwort pro Unit wäre, daß Sie bei einem Reset sehr lange mit der Eingabe der Passwörter beschäftigt sein könnten. Auf der anderen Seite kann es aber wünschenswert sein, eine besonders geheime Unit mit einem eigenen Passwort zu verschlüsseln. Beides ist bei DiskProtection möglich. Sie können dazu beliebig viele Passwörter erstellen. Für jedes Passwort stellen Sie die Units ein, für die es verwendet wird.

Ein Passwort wird dann abgefragt, wenn das erste Mal auf eine seiner Units zugegriffen wird. Sie haben dann eine einstellbare Zeitspanne Zeit, ein Passwort einzugeben. Geben Sie ein Passwort ein, dann wird der Hash-Wert des eingegebenen Passworts mit dem gespeicherten Hash-Wert verglichen. Falls die Werte nicht übereinstimmen, wird das Passwort zurückgewiesen. Es stehen beliebig viele Versuche zur Verfügung, und die Eingabe kann jederzeit abgebrochen werden.

Ist die Zeitspanne verstrichen, z. B. weil Sie nicht am Rechner sitzen, oder wurde die Eingabe abgebrochen, dann wird das Filesystem, das auf das diskprot.device zugegriffen hat, nicht länger blockiert, sondern kann das Device nicht öffnen.

Ohne dieses Verhalten würde das Anwenderprogramm, das auf das Filesystem zugegriffen hat, ebenfalls blockiert werden, was u.U. nicht wünschenswert wäre. Man kann die Zeitspanne aber auch auf Null setzten, dann werden alle Zugriffe auf eine Unit solange angehalten, bis ein Passwort eingegeben wurde.

1.15 DiskProtection.guide/Systempasswort

Systempasswort

Es gibt ein besonderes Passwort, das nicht gelöscht werden kann, aber auch einstellbar ist: das Systempasswort. Selbstverständlich können Sie hier auch dieselben Einstellungen treffen, wie bei allen anderen Passwörtern auch. Dieses Passwort wird u. a. verwendet, um die Programmeinstellungen zu laden oder zu speichern und vor unbefugter

Benutzung des Preferences-Programms zu schützen. Voreingestellte ist eine leerer Passworttext, bei der Abfrage genügt also ein Return.

1.16 DiskProtection.guide/Reset

Passwörter nach einem Reset
==========

Die Eingabe der Passwörter ist ein Problem, wenn der Rechner ohne Aufsicht läuft und auch nach einem Reset seine Arbeit fortsetzten soll, wie etwa bei einer Mailbox. Ein Sysop kann zwar den Rechner einschalten und die Passwörter eingeben, aber nach einem Reset, etwa wegen eines Rechnerabsturzes, würde der Computer nur soweit hochfahren, wie keine Passwörter nötig wären. Auch dafür bietet DiskProtection Lösungen:

Passwort resetfest machen
In Datei verstecken

1.17 DiskProtection.guide/Passwort resetfest machen

Passwort resetfest machen

Nachdem ein Passwort nach einem Kaltstart eingegeben wurden, kann DiskProtection es auf Wunsch resetfest im Speicher ablegen und nach dem nächsten Reset aus dem Speicher auslesen.

Nachteile wären, daß hier eine Angriffsstelle für eine Attacke auf DiskProtection gegeben wäre. Zwar werden die Passwörter verschlüsselt im Speicher abgelegt, aber dazu wird immer dasselbe Passwort und ein einfacher Algorithmus verwendet. Durch eine Analyse des Programmcodes könnten die Passwörter gefunden werden. Außerdem könnten durch einen schweren Rechnerabsturz die resetfesten Passwörter entfernt werden.

Trotzdem ist diese Methode noch recht sicher, denn um die Passwörter zu knacken, müßte jemand die Möglichkeit haben, mit dem Rechner zu arbeiten, nachdem die Passwörter eingegeben und bevor der Rechner ausgeschaltet wird.

1.18 DiskProtection.guide/In Datei verstecken

Versteckte Passwörter

Der Nachteil der vorherigen Methode ist, daß nicht sicher ist, ob die Passwörter einen Reset überleben. Ist der zuverlässige Betrieb des Rechners wichtiger als die Sicherheit vor Ausspähung der Daten, dann könnem Sie auch eine andere Methode wählen:

Ein Passwort wird aus einer frei einstellbaren Datei an irgendeiner Stelle ausgelesen. Diese Datei könnte man in irgendeinem Verzeichnis verstecken, oder auf eine Diskette schreiben, die man bei Bedarf schnell verschwinden lassen kann. Ist die Datei nicht vorhanden, wird das Passwort ganz normal abgefragt. Man kann diese Methode auch zusätzlich zu dem resetfesten Ablegen der Passwörter verwenden. Dann wird nur auf die Datei zugegriffen, wenn die Passwörter nicht im RAM stehen.

Das Passwort kann auch über mehrere Zeilen gehen, die Zeilenenden werden stillschweigend übergangen. Sollte beim nächsten Leseversuch an der gespeicherten Stelle nicht mehr das gesuchte Passwort stehen, so wird es ohne Fehlermeldung wie sonst auch vom Benutzer erfragt.

Diese Methode ist aber unsicher:
Der gravierendste Mangel ist wohl das System an sich, da der Rechner gleich nach dem Einschalten auch den Zugriff auf die verschlüsselten Daten ermöglicht, es sei denn, man löscht oder entfernt rechtzeitig die Datei, in der das Passwort steht. Schon ohne Programmierkenntnisse kann jeder z. B. mit SnoopDos feststellen, welche Datei geladen wird. Zwar wird die ganze Datei in den Speicher geladen, aber auch das Passwort selbst könnte man durch Analyse des Programmcodes finden.

1.19 DiskProtection.guide/Zugangsschutz

Zugangsschutz
==========

Das bisher geschilderte System hat noch eine Schwachstelle: Sobald der Rechner gestartet und die Passwörter eingegeben wurde, kann sich jeder vor den Rechner setzten und auch Dateien auf geheimen Partitionen lesen. Nachdem die Passwörter eingegeben wurden, müßte man den Rechner also für Benutzereingaben sperren können, damit man in einer Kaffee-Pause den Rechner auch mal unbeaufsichtigt lassen kann.

Das realisiert DiskProtection , indem auf Tastendruck ein Bildschirm geöffnet wird und aus der Eingabe die Eingaben herausfiltert, mit denen der Bildschirm nach hinten gebraucht werden könnte. Außerdem wird der DiskProtection -Bildschirm in kurzen Zeitabständen vom Programm automatisch nach vorne gebracht. Dieser Bildschirm wird erst entfernt, wenn in dem String-Gadget dieses Bildschirms das System-Passwort eingetragen wurde. Dazu richtet DiskProtection einen Input-Handler und ein Commodity ein, das in Exchange unter DPSecurity aufgeführt ist. Über Exchange können Sie daher den Zugangsschutz auch aktivieren, bzw. deaktivieren und den Bildschirm öffnen.

Sie können DiskProtection auch so konfigurieren, daß dieser Bildschirm automatisch beim Start geöffnet wird. Da es immer wieder vorkommt, daß man mal kurz den Rechner verläßt und dann doch länger

als erwartet aufgehalten wird, kann dieser Bildschirm auch wie bei einem Screenblanker nach einer einstellbaren Zeitspanne ohne Benutzeraktivität automatisch aktiviert werden.

Anders als die Eingabe des System-Passworts, die für den Zugriff auf die Voreinstellungen und damit indirekt auf die verschlüsselten Units nötig ist, wird dadurch nicht der Boot-Vorgang des Rechners blockiert! Daher ist diese Einstellung sehr zu empfehlen, wenn Sie das System-Passwort in einer Datei verstecken wollen (In Datei verstecken), da bei dieser Kombination der Recher von alleine bootet, aber erst dann wirklich genutzt werden kann, wenn es noch einmal manuell eingegeben wurde.

Falls der Bildschirm etwa wegen Speichermangels nicht geöffnet werden kann, könnte man auch das Device selbst sperren und immer wieder versuchen, den Bildschirm zu öffnen. So könnte man sich hundertprozentig darauf verlassen, daß durch die "Screenblanker"- und "Beim Start Öffnen"-Optionen der Zugriff auf verschlüsselte Partitionen immer verhindert wird. Dadurch könnte aber auch eine Patt-Situation entstehen: Der Speicher wird knapp und der Bildschirm kann nicht geöffnet werden. Also würde das Device gesperrt werden und Anwenderprogramme könnten ihre Daten nicht abspeichern. Daher kann man auch keine Programme beenden um Speicher frei zu machen => der Rechner ist ausweglos blockiert.

Falls also der Bildschirm des Zugangsschutzes nicht geöffnet werden kann, so wird der Schutz einfach nicht aktiviert! Wenn sie den Zugangsschutz per Hand aktivieren wollten, können Sie entsprechend reagieren. Bei der Screenblankermethode bleibt ein zusätzliches Risiko, aber da er sich eh erst verspätet einschaltet, sollte man eigentlich auch nicht zu sehr auf ihn vertrauen, sondern eher per Hand einschalten. Beim Booten schließlich kann man aufgrund der eigenen Erfahrung sehr gut einschätzen, ob der Bildschirm geöffnet werden kann.

Ein solcher Zugangsschutz wird auch schon durch andere Programme realisiert. Der Nachteil ist dabei--wie auch bei DiskProtection --aber immer, daß diese Programme auf dem Amiga viel zu leicht umgangen werden können, indem etwa von einer Diskette gebootet oder die Startup-Sequence nicht ausgeführt wird. Sicher ist bei DiskProtection aber auf jeden Fall, daß niemand diesen Zugangsschutz umgehen und trotzdem Zugriff auf verschlüsselte Units bekommen kann. Der Zugangsschutz und die Verschlüsselung werden beide im diskprot.device realisiert, daher kann man nicht das eine umgehen, aber das andere trotzdem nutzen.

1.20 DiskProtection.guide/DiskProtection

DiskProtection, Preferences
****

Mit dem Preferences-Programm DiskProtection treffen Sie alle Voreinstellungen für das DiskProtection -Packet. Es heißt wie das gesamte Programmpacket, läßt sich aber im Text durch die

unterschiedliche Schreibweise unterscheiden.

Preferences-Konzept	Wichtig! Grundlegende Informationen
Hauptfenster	Die grafische Benutzeroberfläche
DPUnit Editieren	Das Fenster zum Editieren einer Unit
Passwort Editieren	Das Fenster zum Editieren eines Passworts
Requester	Dialogfenster des Prefs-Programms

1.21 DiskProtection.guide/Preferences-Konzept

```
Preferences-Konzept
===================
```

DiskProtection wird fast wie jedes andere Preferences-Programm verwendet. Es gibt allerdings ein paar Unterschiede, die hier geschildert werden:

Programmstart	Eingabe des Systempassworts notwendig
Speichern der Einstellungen	in DiskProtection.prefs/Unit/DOSDrivers

1.22 DiskProtection.guide/Programmstart

```
Programmstart: Argumente, Programmschutz
----------------------------------------
```

Sie müssen jedes Mal das Systempasswort eingeben, bevor Sie das Programm verwenden können. So wird vor unbefugter Benutzung geschützt. Daher läßt sich DiskProtection nur interaktiv mit grafischer Benutzeroberfläche betreiben. Die von anderen Preferences-Programmen bekannten Argumente gibt es nicht. DiskProtection unterstützt nur ein einziges Argument:

```
PubScreen/K
```

Es kann sowohl in der Shell als auch als ToolType angegeben werden und bewirkt, daß die Fenster von DiskProtection auf dem angegebenen PublicScreen geöffnet werden.

1.23 DiskProtection.guide/Speichern der Einstellungen

```
Speichern der Einstellungen
---------------------------
```

Falls die DiskProtection -Einstellungen nicht vorhanden oder manipuliert worden sind, werden Sie beim Laden in einem Requester darauf hingewiesen und haben dann die Wahl, abzubrechen oder die Standardeinstellungen zu verwenden. Wenn Sie DiskProtection durch einen Aufruf von DiskProtection initialisieren, werden Sie zweimal gefragt, einmal durch das Device und einmal duch das Prefs-Programm selbst. Das Standardpasswort ist ein leerer String.

Wichtig ist außerdem, daß Sie beachten, daß die Einstellungen an insgesamt drei Stellen festgehalten werden:

* ENV[ARC]:DiskProtection.pref

  Dort stehen die für DiskProtection spezifischen Einstellungen: Units, Passwörter und globale Einstellungen. Diese Dateien werden mit Prüfsummen und durch Verschlüsseln mit dem Systempasswort und dem Systemalgorithmus gegen Manipulation und Ausspähung geschützt. Die einzelnen Passworttexte werden nicht abgespeichert!

* Units

  Jede Unit von DiskProtection ist gemäß der eingestellten Optionen verschlüsselt. Ändern Sie in ENV[ARC]:DiskProtection.pref diese Einstellungen, z. B. das Passwort, dann muß die komplette Unit neu verschlüsselt werden, um weiterhin auf die Dateien zugreifen zu können. Eine Formatierung der Unit nach der Aktivierung der neuen Einstellungen hat dieselbe Wirkung, allerdings gehen dabei alle Daten verloren.

* DEVS:DosDrivers und SYS:Storage/DosDrivers oder DEVS:DP-Mountlist

  Hier stehen--wie auch von AmigaDOS bekannt--die Anmeldedateien bzw. -einträge, die der MOUNT-Befehl braucht, um die Geräte anzumelden, die auf den DPUnits beruhen.

Man kann weiterhin alle Einstellungen innerhalb dieses einen Preferences-Programms ändern. DiskProtection sorgt dafür, daß alle drei Stellen immer überein stimmen, auch wenn während des Änderns der Einstellungen mal der Rechner abstürzt oder die Änderungen doch nicht abgespeichert werden.

Die Änderungen an Anmeldedateien werden immer sofort abgespeichert. Auch Einstellungen einer Unit, die die Verschlüsselung betreffen, werden automatisch abgespeichert, wenn Sie die entsprechenden Units konvertiert haben.

1.24 DiskProtection.guide/Hauptfenster

Hauptfenster von DiskProtection
==========

Das Hauptfenster ist in fünf Bereiche unterteilt: Units, Passwörter, System-Verschlüsselung (unter/in dem

Passwort-Bereich), Zugangsschutz und die Standard-Gadgets für
Preferences.

Units und Passwoerter	Einrichten, Editieren und Löschen
System-Verschluesselung	System-Passwort und -Algorithmus
Einstellungen Zugangsschutz	Aufruf des Bildschirms
Standard-Gadgets	Speichern, Benutzen, Abbrechen
Menus	Standard-Preferences Menus

1.25 DiskProtection.guide/Units und Passwoerter

Units und Passwörter

Diese beiden Bereiche lassen sich gleich bedienen. Sowohl die Units als auch die Passwörter werden mit ihrer Bezeichnung in den entsprechenden Listviews dargestellt und lassen sich dort anwählen. Noch zu konvertierende Units werden durch einen vorangestellten Stern (*) markiert. Mit den darunter liegenden Gadgets ändern Sie diese Listen.

Unit oder Passwort ...

Neu	neu erzeugen
Editieren	Einstellungen ändern
Entfernen	löschen

1.26 DiskProtection.guide/Neu

Neu
...

Mit dem Gadget Neu wird eine neue Unit, bzw. ein neues Passwort erzeugt. Bei Units können Sie dazu aus einem Requester ein bereits bestehendes DOS-Device wie etwa DF0: auswählen, deren Werte dann für die entsprechende Unit übernommen werden (s.a. DOS-Device auswaehlen) Auf Wunsch wird auch eine Unit mit Standardwerten eingerichtet, in der Sie noch manuell Eintragungen machen müssen. Bei einem neuen Passwort werden Standard-Werte voreingestellt, z.B. "" als Passworttext.

1.27 DiskProtection.guide/Editieren

Editieren
....

Mit Editieren wird für eine bestehende Unit das Fenster DPUnit Editieren , für Passwörter das Fenster Passwort Editieren geöffnet, in denen der angewählte Eintrag aus dem Listview im Hauptfenster editiert wird.

1.28 DiskProtection.guide/Entfernen

Entfernen
....

Löschen von Units und Passwörtern läßt sich nicht rückgängig machen. Bevor Daten verloren gehen, erhalten Sie aber immer noch vorher die Möglichkeit, abzubrechen.

Wenn die Unit verschlüsselt ist, wird zuerst gefragt, ob die angewählte Unit entschlüsselt werden soll. Sie können jetzt noch abbrechen, andernfalls wird die Unit nach erfolgreicher Entschlüsselung sofort gelöscht.

Entfernt Sie ein Passwort, dann werden ihm zugeordnete Units dem Systempasswort zugeordnet und bei Bedarf auf Nachfrage geändert. Enthält ein Passwort keine Units oder lassen sich diese ohne Konvertierung verschieben, dann wird ohne Warnung gelöscht!

1.29 DiskProtection.guide/System-Verschluesselung

System-Passwort und -Algorithmus

Das Check-Button-Gadget System-Passwort bezieht sich auf das im Listview darüber angewählte Passwort und legt fest, welches Passwort als System-Passwort verwendet wird. Deselektieren Sie es, so wird das erste Passwort zum System-Passwort.

Darunter wählen Sie über den Requester Algorithmus und Modus auswaehlen den für System-Daten zu verwendenden Algorithmus aus.

1.30 DiskProtection.guide/Einstellungen Zugangsschutz

Einstellungen Zugangsschutz

Sie unterteilen sich in einen Bereich für die Einstellung des zu verwendenden Bildschirms und die Art, wie und wann der Zugangsschutz aktiviert wird:

Blanker-Hotkey	Hotkey für Zugangsschutz
Aktivieren nach # Sek.	Zeitspanne ohne Benutzer-Aktivität
Beim Programmstart	Gleich bei Programmstart öffnen?
Screenmode u. -font	Bildschirmeinstellungen
Dimmer + Blanker-Zeitsp.	DiskProtection-Screenblanker

1.31 DiskProtection.guide/Blanker-Hotkey

```
Zugangsschutz-Hotkey
....................
```

Bei Hotkey können Sie auf die von Commodities bekannte Art eine Tastenkombination einstellen, mit der der Zugangsschutz aktiviert wird.

1.32 DiskProtection.guide/Aktivieren nach # Sek.

```
Aktivieren nach # Sek.
......................
```

Soll der Zugangssschutz außerdem nach einer bestimmten Zeitspanne ohne Benutzer-Aktivität automatisch aktiviert werden, dann müssen Sie bei Aktivieren nach # Sek. diese Zeit in Sekunden eintragen. Eine Null schaltet diese Funktion aus.

1.33 DiskProtection.guide/Beim Programmstart

```
Beim Programmstart aktivieren
.............................
```

Schließlich können Sie den Bildschirm auch gleich beim Programmstart aktivieren lassen, indem Sie die Option beim Programmstart einschalten.

1.34 DiskProtection.guide/Screenmode u. -font

```
Bildschirmeinstellungen
.......................
```

Mit ASL-Requestern können Sie für den Zugangsschutz-Bildschirm den Screenmode und -font festlegen.

WB 2.04: Statt der Asl- muß hier die ReqTools-Library für den

Screenmode-Requester verwendet werden. Falls diese nicht installiert ist, ist der Button nicht anwählbar.

1.35 DiskProtection.guide/Dimmer + Blanker-Zeitsp.

DiskProtection-Screenblanker
.....

Da der Zugangsschutz-Bildschirm immer im Vordergrund bleibt, kann kein Screenblanker seine Funktion erfüllen, weil auch sein Bildschirm nach hinten gelegt wird. Daher hat DiskProtection einen eingebauten Screenblanker, der nach einer einstellbaren Zeitspanne (Blanker-Zeitspanne) die Helligkeit des vordersten Screens auf einen beliebigen Prozentsatz (Dimmer) reduziert. Eine Null schaltet diese Funktion aus.

Dieser Blanker funktioniert nicht mit Custom-Screeens! Auch das Ändern der Farben der Workbench oder eines Public-Screens ist eigentlich illegal und kann zu falschen Farben führen.

1.36 DiskProtection.guide/Standard-Gadgets

Standard-Gadgets

Die Funktion dieser Gadgets dürfte von den anderen Preferences-Programmen bekannt sein:

* Speichern--Änderungen dauerhaft in ENVARC:DiskProtection.prefs abspeichern

* Benutzen--Änderungen aktivieren, aber nicht dauerhaft festhalten (d. h. in ENV:DiskProtection.prefs abspeichern)

* Abbrechen--Beenden ohne zu ändern

Man muß jedoch beachten, was in Preferences-Konzept gesagt wurde: Auch wenn Sie abbrechen oder Änderungen mit Benutzen nur temporär aktivieren, kann es dennoch sein, daß einige der Änderungen dauerhaft gespeichert wurden, weil sie Anmeldedateien oder die Verschlüsselung von Units betreffen.

1.37 DiskProtection.guide/Menus

Menus

DiskProtection hat alle Standard-Menus eines Preferences-Programms:

Projekt	betrifft das Programm
Vorgaben	Zurückstellen auf Bestehendes
Optionen	Piktogramme erzeugen?

1.38 DiskProtection.guide/Projekt

Projekt
....

In dem Menu Projekt finden Sie zwei Menupunkte. Mit über ... erhalten Sie Informationen über ihre Version von DiskProtection. Das beinhaltet die Versionsnummer und Kompilierungsdatum des Preferences-Programms und des Devices. Beenden verläßt das Programm, ohne abzuspeichern.

1.39 DiskProtection.guide/Vorgaben

Vorgaben
....

Mit allen drei Menupunkten des Menus Vorgaben setzen Sie die Einstellungen auf bestimmte Vorgaben zurück. Auch hier gelten die in Preferences-Konzept geschilderten Einschränkungen. Konvertierte Units und Anmeldedateien werden nicht zurückgesetzt.

* auf Vorgaben zurücksetzen:
  Stellt nur die Optionen für Zugangsschutz und System-Algorithmus auf die programminternen Vorgaben zurück.

* auf zuletzt gespeichertes:
  Stellt die dauerhaft gesicherten Einstellungen wieder her.

* auf vorherigen Stand:
  Stellt Einstellungen beim Programmstart wieder her.

1.40 DiskProtection.guide/Optionen

Optionen: Piktogramme erzeugen?
....

Das Menu Optionen enthält nur einen Menupunkt. Mit Piktogramme erzeugen? legen Sie fest, ob für die Anmeldedateien Piktogramme erzeugt werden sollen. DiskProtection verwendet dazu das Piktogramm def_project.info aus ENV:Sys, sofern vorhanden.

1.41 DiskProtection.guide/DPUnit Editieren

```
DPUnit Editieren
================
```

Mit diesem Fenster ändern Sie die Einstellungen für die Unit, die Sie im Hauptfenster ausgewählt haben. Das Fenster gliedert sich in folgende Bereiche:

DPUnit	Welche Unit wird bearbeitet?
Datenschutz	Optionen für den Datenschutz
Erweiterte Einstellungen	Device
Anmeldedateien	Liste der DOS-Devices dieser Unit

1.42 DiskProtection.guide/DPUnit

```
Anzeige der DPUnit
------------------
```

In diesem Feld links oben bekommen Sie zum einen die interne Unit-Nummer angezeigt. Das ist die Nummer, die ein Filesystem beim Öffnen des diskprot.devices angeben muß, um diese Unit anzusprechen. Die Nummer kann nicht geändert werden und wird vom Programm so vergeben, daß es keine Überschneidung mit bereits bestehenden oder auch gelöschten Units gibt. Außerdem wird angezeigt, ob die Unit noch konvertiert werden muß, weil Sie die Einstellungen zwar geändert, die Unit aber noch nicht angepaßt haben.

Praktischer ist der Name der Unit, den Sie selbst festlegen könne. Er wird verwendet, um die Unit zu identifizieren, wie etwa im Listview des Hauptfensters. Sie sollten hier also einen aussagekräftigen Namen verwenden. Schließlich legen Sie noch fest, ob das Gerät Wechselmedien verwendet.

1.43 DiskProtection.guide/Datenschutz

```
Datenschutz-Einstellungen
-------------------------
```

In dieser Gruppe wurden die für die Verschlüsselung ausschlaggebenden Optionen zusammengefaßt. Diese Einstellungen können

jederzeit ohne Datenverlust geändert werden. Wenn Sie Algorithmus oder Passwort ändern, dann müssen Sie allerdings bei einer Übernahme der Änderungen mit OK auch die Unit neu verschlüsseln (siehe auch Automatische Unit-Aenderung).

Algorithmus	Datenverschlüsselung: Keiner, XPK
Passwort Wahl	Übernahme des Passworts für die Unit

1.44 DiskProtection.guide/Algorithmus

Verschlüsselungs-Algorithmus
.....

Bei Algorithmus können Sie über den Requester Algorithmus und Modus auswaehlen den zu verwendenden Algorithmus für diese Unit einstellen.

1.45 DiskProtection.guide/Passwort Wahl

Zugehörigkeit zu einem Passwort
.....

Bei Passwort wird das Passwort der Unit eingestellt. Vorgegeben ist das Systempasswort. Wurde das neue Passwort noch nicht eingegeben, dann muß es jetzt eingegeben werden, bevor die Unit dem Passwort hinzugefügt werden kann, weil sonst nicht klar ist, wie die Unit verschlüsselt werden muß.

1.46 DiskProtection.guide/Erweiterte Einstellungen

Erweiterte Einstellungen

Diese Einstellungen sollte man nur ändern, wenn man eine Unit per Hand einrichtet. Normalerweise werden alle Werte bereits bei der Erzeugung der Unit über die Auswahl eines bestehenden Gerätes auf die richtigen Werte gesetzt. Nur wenn man bei der Erzeugung kein Gerät angewählt hat, sind diese Optionen von Anfang an anwählbar, denn dann müssen Sie hier etwas eingeben. Ansonsten muß man zuerst immer Änderung möglich anklicken, bevor man etwas aus dem folgenden ändern kann:

Device	Das zugrunde liegende Exec-Device
Unit	Die Unit davon
FFS-Patch Aktiviert	Ermöglicht dem FFS das Lesen verschieden großer Medien

1.47 DiskProtection.guide/Device

```
Device
......
```

In Device steht das Exec-Device, auf dem diese DPUnit beruht. Das Device muß kompatibel zum trackdisk.device sein.

1.48 DiskProtection.guide/Unit

```
Unit-Nummer
...........
```

Unit ist die Nummer der Unit des eingestellten Devices, auf das zugegriffen werden soll.

1.49 DiskProtection.guide/FFS-Patch Aktiviert

```
FFS-Patch für Diskettenwechsel
..............................
```

FFS-Patch Aktiviert kann mit den Filesystemen OFS/FFS/INTL/CACHE in den Versionen von 2.04 bis 3.1 verwendet werden. Er darf nicht mit anderen Filesystemen und Exec-Devices, die das Kommando TD_GETGEOMETRY nicht unterstützen, verwendet werden.

Dieser Patch ermöglicht dem Filesystem verschieden große Medien zu erkennen, etwa bei einem Diskettenwechsel. Er wird benötigt, um HD- und DD-Disketten in einer DPUnit zu verwenden.

1.50 DiskProtection.guide/Anmeldedateien

```
Anmeldedateien
--------------
```

Zur Bearbeitung der Anmeldedateien gibt es folgende Funktionen:

DOS-Device	Listview und String-Gadget
Mountlist-Eintrag Neu	neues DOS-Device
Mountlist-Eintrag Kopieren	Inhalt übernehmen
Mountlist-Eintrag Editieren	Inhalt ändern

```
  Mountlist-Eintrag Löschen     DOS-Device löschen
  Mounten                       jetzt anmelden
  Beim Booten Mounten           automatisch beim Booten anmelden
```

1.51 DiskProtection.guide/DOS-Device

```
DOS-Device: Listview und String-Gadget
.....................................

   Jeder Eintrag in dem Listview entspricht einer Datei in
DEVS:DOSDrivers, bzw. SYS:Storage/DOSDrivers oder einem Eintrag in
DEVS:DP-Mountlist und damit einem DOS-Device. In den DiskProtection
-Preferences wird vermerkt, welche DOS-Devices erzeugt wurden. Mit dem
String-Gadget DOS-Device wird der Namen geändert.
```

1.52 DiskProtection.guide/Mountlist-Eintrag Neu

```
Neu bei Anmeldedateien
......................

   Neu erzeugt auch hier einen neuen Eintrag mit Standard-Vorgaben.
Sie müssen auf jeden Fall noch per Hand einige Werte eintragen!
```

1.53 DiskProtection.guide/Mountlist-Eintrag Kopieren

```
Kopieren von Anmeldedateien
...........................

   Mit Kopieren wird der aktive Eintrag kopiert.
```

1.54 DiskProtection.guide/Mountlist-Eintrag Editieren

```
Editieren von Anmeldedateien
............................

   Anmeldedateien sind normale ASCII-Dateien. Daher ruft Editieren den
in der Enviroment-Variablen EDITOR eingestellten Editor auf.
```

1.55 DiskProtection.guide/Mountlist-Eintrag Löschen

```
Löschen von Anmeldedateien
..........................
```

Der Button Löschen löscht die zugehörige(n) Datei(en)/Mountlisteintrag und den Eintrag im Listview.

1.56 DiskProtection.guide/Mounten

```
Gerät anmelden
..............
```

Mounten meldet das Gerät sofort an. Dazu werden die Einstellungen verwendet, die Sie bereits früher aktiviert haben oder mit denen das Gerät erzeugt wurde, also nicht die Einstellungen, die bisher nur innerhalb des Preferences-Programms geändert wurden.

1.57 DiskProtection.guide/Beim Booten Mounten

```
Gerät automatisch anmelden?
...........................
```

Bei Beim Booten Mounten wird über DiskProtection eingestellt, ob das Gerät beim Booten automatisch angemeldet werden soll. Dazu wird die Anmeldedatei zwischen DEVS:DOSDrivers und SYS:Storage/DOSDrivers hin- und hergeschoben. Das Gadget ist nicht anwählbar, wenn Sie statt DOSDrivers die DP-Mountlist verwenden.

1.58 DiskProtection.guide/Passwort Editieren

```
Passwort Editieren
==================
```

In diesem Fenster treffen Sie Einstellungen für das Passwort, das Sie im Hauptfenster angewählt haben. Die Einstellungen hier betreffen auch die Verschlüsselung von Units, etwa wenn Sie ein Passwort festlegen oder eine Unit diesem Passwort zuordnen.

Daher kann es sein, daß Sie bei der Übernahme der Änderungen durch OK gefragt werden, ob Sie Units neu verschlüsseln wollen (Automatische Unit-Aenderung).
Dazu wird intern eine Kopie des Passworts erzeugt, in das die Units verlegt werden. Brechen Sie zwischendurch ab, dann sind die noch nicht konvertierten Units in dem zweiten Passwort weiterhin ohne Probleme ansprechbar.

Für jedes Passwort lassen sich folgende Einstellungen treffen:

Passwortname	Identifiziert das Passwort
Wartezeit	Zeitspanne für die Passworteingabe
Passwort Eingabe	Passwort ändern
Resetfest	Passwort resetfest machen?
Verstecken	Passwort in Datei verstecken?
Dateiname	In dieser Datei verstecken
Units des Passworts	Mitglieder des Passworts

1.59 DiskProtection.guide/Passwortname

Identifiziert das Passwort

Der bei Passwortname eingegebene String wird verwendet, um das Passwort im Listview oder bei der Passworteingabe zu identifizieren.

1.60 DiskProtection.guide/Wartezeit

Wartezeit für Passworteingabe

Das Programm bricht die Abfrage dieses Passworts nach Wartezeit Sekunden ohne Benutzereingabe automatisch ab. Abschaltbar durch 0.

1.61 DiskProtection.guide/Passwort Eingabe

Passwort eingeben

Bei Passwort können Sie über einen Requester das aktuelle Passwort festlegen. Zur eigenen Sicherheit müssen Sie das Passwort zweimal eingegeben, bevor Sie es mit OK übernehmen können. So werden Tippfehler vermieden. Dieses Passwort wird nicht abgespeichert, sondern nur sein Hash-Wert!

Wollen Sie ein Passwort ändern, dann werden Sie auch nach dem alten Passwort gefragt, wenn Sie es nicht schon früher eingegeben haben, zum einen, um einen zusätzlichen Schutz zu schaffen, zum anderen, um eventuell damit verschlüsselte Units neu verschlüsseln zu können. Außerdem muß das Passwort bekannt sein, wenn sie es in einer Datei versteckt wollen.

1.62 DiskProtection.guide/Resetfest

```
Resetfestes Passwort
--------------------
```

Resetfest bestimmt, ob ein Passwort nach der Eingabe resetfest gemacht werden soll (Passwort resetfest machen).

1.63 DiskProtection.guide/Verstecken

```
Passwort in Datei verstecken
----------------------------
```

Verstecken schaltet das In Datei verstecken des Passworts ein. Ist das Passwort dem Programm noch nicht bekannt, müssen Sie es zuerst eingeben. Ist noch kein Dateiname festgelegt, dann wird auch gleich das ensprechende String-Gadget aktiviert. Alternativ dazu rufen Sie mit dem Gadget daneben einen Datei-Requester auf.

1.64 DiskProtection.guide/Dateiname

```
Dateiname
---------
```

In der Datei Dateiname wird das Passwort bei eingeschaltetem In Datei verstecken gesucht. Wird das Passwort in der Datei nicht gefunden, dann werden Sie darauf hingewiesen und dieses Feature automatisch ausgeschaltet.

1.65 DiskProtection.guide/Units des Passworts

```
Units des Passworts
-------------------
```

Ganz unten wählen Sie die Mitglieder des Passworts aus, wenn Sie nicht gerade das Systempasswort editieren. Dazu haben Sie die beiden Listviews Units mit Systempasswort und Mitglieder dieses Passworts, in denen die Units dargestellt werden, die Mitglied des Systempassworts und des aktuellen Passworts sind.

Mit <- und -> können Sie die angewählten Units zwischen den Passwörtern hin- und herschieben. Diese Veränderung kann auch dazu führen, daß eine Unit neu verschlüsselt werden muß.

1.66 DiskProtection.guide/Requester

```
Dialogfenster des Prefs-Programms
=================================


  Automatische Unit-Aenderung        Unit sofort konvertieren?
  DOS-Device auswaehlen              Requester beim Einrichten einer DPUnit
  Algorithmus und Modus auswaehlen   Requester zu Wahl der Verschlüsselungart
```

1.67 DiskProtection.guide/Automatische Unit-Aenderung

```
Unit-Verschlüsselung automatisch verändern
------------------------------------------
```

Machen Sie Änderungen an Einstellungen, die direkt oder indirekt die Verschlüsselung einer Unit betreffen, dann werden Sie sofort gefragt, ob und wann Sie die betroffene Unit ändern lassen wollen. Konvertierung ist notwendig, damit weiterhin auf die bestehenden Dateien zugegriffen werden kann. Formatieren Sie das Mediums nachdem die neuen Einstellungen aktiviert wurden, so läßt sich das Medium auch verwenden, Sie verlieren aber alle Daten.

In einem Requester werden folgende Optionen geboten, von denen je nach Situation nicht immer alle zur Verfügung stehen:

* Sofort

  Die Unit wird von ihrem jetzigen Zustand in den neuen Zustand gebracht. War die Umwandlung erfolgreich, dann werden die Einstellungen, die die Verschlüsselung betreffen, in der Datei ENVARC:DiskProtection.pref dauerhaft festgehalten.

* Q-Formatieren

  Die neuen Einstellungen werden auf jeden Fall aktiviert und dauerhaft gespeichert. Außerdem versucht DiskProtection, das erste gültige DOS-Device der Unit mit der Option QUICK zu formatieren. Falls nötig, wird es zuerst gemounted.

* Später

  Sie können die Unit auch erst später umwandeln lassen. So können Sie etwa eine Unit erst einem Passwort zuordnen und dann dieses Passwort ändern. Beim ersten Mal brauchen Sie noch nichts umzuwandeln, es genügt, wenn Sie beim zweiten Mal die Daten neu verschlüsseln.

* Nie

  Die Änderungen werden vermerkt, aber noch nicht dauerhaft abgespeichert, und können daher noch abgebrochen werden. Anders als bei Später werden Sie später nicht mehr gefragt, ob die Unit

noch neu verschlüsselt werden soll.

* Zurück

Kehrt ohne irgendwelche Änderungen durchzuführen in das Fenster zurück, das Sie gerade verlassen wollten.

* Abbrechen

Die Unit wird weder umgewandelt, noch werden die Verschlüsselungs-Einstellungen geändert.

Wenn Sie Änderungen an Units noch nicht durchgeführt haben und die Einstellungen benutzen oder speichern wollen, werden Sie ebenfalls vor die oben genannte Wahl gestellt. Allerdings können Sie jetzt die Änderungen nicht mehr für später zurückstellen. Außerdem werden bei Abbrechen die Einstellungen zwar gespeichert, aber ohne die Veränderungen an den Verschlüsselungseinstellungen.

1.68 DiskProtection.guide/DOS-Device auswaehlen

DOS-Device auswaehlen

Dieser Requester erscheint, wenn Sie eine neue Unit einrichten. Er bietet Ihnen in dem Listview-Gadget alle im System im Moment gemounteten DOS-Devices zur Auswahl an, für die DiskProtection eine Unit einrichten kann.

Mit OK wird eine Unit mit den Werten des ausgewählten DOS-Devices eingerichtet. Bei Standardwerte wird die Auswahl nicht berücksichtigt, sondern die neue Unit mit vorgegebenen Werten initialisiert. Sie müssen in diesem Fall noch per Hand Werte eintragen! Abbrechen schließlich verläßt den Requester, ohne eine neue Unit einzurichten.

1.69 DiskProtection.guide/Algorithmus und Modus auswaehlen

Algorithmus-Requester

Mit dem Listview-Gadget können Sie aus den verfügbaren Datenverschlüsselungs-Algorithmem einen auswählen. Darunter bekommen Sie die wichtigsten Daten zu dem angewählten Verschlüsselungs-Algorithmus angezeigt.

Für einen Algorithmus, der verschiedene Betriebsmodi unterstützt, können Sie diese mit dem Slider darunter einstellen. Ansonsten ist das Gadget nicht anwählbar.

1.70 DiskProtection.guide/diskprot.device

```
Fenster/Requester des Devices
*****************************
```

Passworteingabe	Abfrage/Neueingabe eines Passworts
Unit-Konvertierung	DPUnit neu verschlüsseln
Konvertierungs-Fehler	Reaktionsmöglichkeiten bei Fehlern

1.71 DiskProtection.guide/Passworteingabe

```
Passworteingabe
===============
```

Bei der Passworteingabe gibt es zwei Eingabearten:

Bei der einen müssen Sie ein bestimmtes Passwort eingeben. Das Programm kennt den Hash-Wert (s.a. Hash-Wert) dieses Passworts und weißt Sie so gleich bei einer fehlerhaften Eingabe darauf hin.

Bei der anderen können Sie ein neues Passwort wählen. Damit Ihnen keine Tippfehler unterlaufen, müssen Sie zur Sicherheit zweimal hintereinander dasselbe Passwort eingeben, bevor das Programm das neue Passwort akzeptiert.

Je nach Kontext enthält das Fenster folgende Gadgets:

* Textfeld

  Hier erhalten Sie Hinweise des Programms, so z.B. die Zeit, die Ihnen noch bleibt, um das Passwort einzugeben.

* Passwort

  Hier wird das Passwort eingegeben. Bei einem neuen Passwort wird das String-Gadget nach der ersten Eingabe gelöscht, und Sie müssen erst die Eingabe wiederholen.

* OK

  Übernimmt das eingegebene Passwort.

* Abbrechen

  Beendet die Eingabe ohne ein gültiges Passwort zurückzuliefern.

1.72 DiskProtection.guide/Unit-Konvertierung

Änderung der Unit-Verschlüsselung
==========

Dieses Fenster wird verwendet, wenn eine Unit tatsächlich neu verschlüsselt werden soll. Der aufrufende Programmteil bekommt mitgeteilt, ob die Änderungen durchgeführt wurden oder nicht.

Im oberen Teil bekommen Sie Informationen darüber, welche Änderungen gemacht werden sollen. Darunter finden Sie eine Statusanzeige mit einem Füllbalken, der für die bereits bearbeiteten Zylinder steht, und eine Textanzeige.

Mit den Optionen können Sie vor dem Start der Umwandlung festlegen, ob beim Schreiben noch ein Verify gemacht werdens soll oder nicht. Haben Sie Ihre Wahl getroffen und u.U. die entsprechende Diskette eingelegt, wird mit Start die Umwandlung begonnen. Soll doch nicht umgewandelt werden, aber die Einstellungsänderung trotzdem in den Preferences abgespeichert werden, dann können Sie Zurück anwählen. Warnung: Dadurch sind die Daten auf dieser Unit nicht mehr direkt lesbar, da die Verschlüsselung nicht mit den Einstellungen übereinstimmt! Mit Abbrechen verlassen Sie den Requester, ohne irgendwelche Änderungen zu machen.

Nachdem Sie die Umwandlung gestartet haben, wird zuerst die Größe des eingelegten Mediums gelesen. Daher können Sie z.B. sowohl HD- als auch DD-Disketten abwechselnd konvertieren. Danach werden alle Tracks der Reihe nach gelesen und neu verschlüsselt zurückgeschrieben. Wenn ein Fehler auftritt oder Sie jetzt noch Abbrechen wählen, wird ein Fehler-Requester (Konvertierungs-Fehler) geöffnet.

Nachdem die Konvertierung beendet wurde, können Sie bei Wechselmedien noch weitere Medien konvertieren. Sollte beim mehrfachen Konvertieren von Wechselmedien bei einigen Medien Fehler auftreten, bei anderen aber nicht, so sollten Sie sich beim Verlassen des Fensters genau überlegen, ob die Preferences geändert werden sollen oder nicht: Bei Zurück sind die noch nicht konvertierten Medien nicht direkt lesbar, bei Abbrechen die konvertierten.

1.73 DiskProtection.guide/Konvertierungs-Fehler

Konvertierungs-Fehler
==========

Sollte beim Konvertieren einer Unit ein Fehler aufgetreten oder abgebrochen worden sein, so kommt dieser Requester mit einer Erklärung des Problems und folgenden Reaktionsmöglichkeiten:

* Konvertierung rückgängig

  Alle bereits geänderten Tracks werden wieder in den Urzustand gebracht und die Preferences werden nicht geändert. Die "Konvertierungsrichtung" kann auch mehrmals geändert werden.

```
*     Wiederholen

  Nochmal versuchen, die letzte Operation auszuführen.

*     Ignorieren

  Weiter machen, ohne den aktuellen Track zu konvertieren. Dadurch
  gehen die Daten dieses Tracks verloren! Nicht anwählbar bei einem
  Abbruch durch den Benutzer...

*     Zurück

  Beendet die Konvertierung sofort, als wäre sie erfolgreich
  abgeschlossen worden. Warnung: Dadurch gehen alle Tracks verloren,
  die noch nicht konvertiert wurden. Daher erfolgt noch eine
  Sicherheitsabfrage.  Bei Wechselmedien entspricht dies Abbrechen
  und ist daher nicht anwählbar.

*     Abbrechen

  Beendet die Konvertierung sofort, als wäre sie nicht
  durchgeführt worden.  Warnung: Dadurch gehen alle Tracks verloren,
  die bereits konvertiert wurden. Daher erfolgt noch eine
  Sicherheitsabfrage.  Bei Wechselmedien wird nur die Konvertierung
  des aktuellen Mediums abgebrochen.
```

1.74 DiskProtection.guide/DPInit

```
DPInit
******

   Das DiskProtection  System, z.B. der Zugangsschutz, wird aktiviert,
wenn das Preferences-Programm gestartet oder eine DPUnit gemountet
wird. Beim Mounten muß außerdem noch das zugehörige Filesystem
gestartet werden, d.h. entweder trägt man per Hand in die Mountdatei
MOUNT = 1 oder greift auf das Gerät nach dem Mounten zu (z.B. durch CD
DP_xx).

   Beides ist nicht immer nötig, wenn nur der Zugangsschutz verwendet
werden soll. Deshalb gibt es auch noch das Programm DPInit, das nichts
weiter macht, als das diskprot.device zu öffnen. Nur beim ersten
Aufruf wird das Systempasswort abgefragt. Danach steht dann der
Zugangsschutz zur Verfügung.  DPUnit müssen aber weiterhin normal
gemounted werden. DPInit kann von der Workbench oder in der Shell
aufgerufen werden und liefert die normalen Fehlercodes zurueck.
```

1.75 DiskProtection.guide/Grundlagen

```
Grundlagen der Kryptologie
**************************
```

Hash-Wert	Erzeugung, Verwendung
Block-Verschluesselung	Verwendung, Attacken
DES	Geschichte, Sicherheit
IDEA und FEAL	zur Implementierung
SCRM	Scramble - schnell und unsicher

1.76 DiskProtection.guide/Hash-Wert

Hash-Wert
=========

Ein Hash-Wert (to hash: engl. zerhacken) ist ein Zahlenwert fester Länge, der durch eine Hash-Funktion aus einer Zeichenkette mit variabler Länge berechnet wird.

Erfüllt eine Hash-Funktion auch die folgenden Forderungen, so nennt man sie One-Way-Hash-Funktion:

1. Es ist leicht, zu einer bekannten Zeichenkette den Hash-Wert zu berechnen.

2. Es ist schwer, zu einem bekannten Hash-Wert eine Zeichenkette zu finden, die diesen Wert ergibt.

3. Es ist schwer, zu einer bekannten Zeichenkette eine zweite zu finden, die denselben Hash-Wert hat.

One-Way-Hash-Funktionen können verwendet werden, um digitale Signaturen zu Nachrichten zu erzeugen. In DiskProtection wird die One-Way-Hash-Funktion MD5 in der Implementierung durch RSA Data Security Inc. nur verwendet, um bei der Passworteingabe die Korrektheit der Eingabe überprüfen zu können. Die Hash-Werte aller Passwörter werden in der Prefs-Datei abgespeichert, wobei alle bis auf der des System-Passworts mit der System-Verschlüsselung geschützt sind.

Selbst wenn durch Analyse des Prefs-Dateiformats dieser Hash-Wert gefunden werden sollte, so ist es wegen Eigenschaft 2 unwahrscheinlich, daß dann auch das dazu passenden Passwort gefunden wird. Auch wenn ein Passwort denselben Hash-Wert haben und daher bei der Eingabe akzeptiert werden sollte, so muß das noch nicht das richtige Passwort sein, mit dem auch die Units erfolgreich entschlüsselt werden können.

MD5 selbst wird auch in PGP verwendet. Es erzeugt mit 128 Bit einen ausreichend langen Hash-Wert, um Attacken durch Ausprobieren schwer zu machen. Es scheint für die Zwecke von DiskProtection ausreichend sicher zu sein.

1.77 DiskProtection.guide/Block-Verschluesselung

```
Block-Verschlüsselung
=====================
```

Die meisten Verschlüsselungsalgorithmen und insbesondere alle, die im Moment für DiskProtection zur Verfügung stehen, verschlüsseln immer einen einzelnen Datenblock am Stück, meist 64 Bits. Es gibt jedoch verschiedenste Arten, wie man diese Algorithmen einsetzen kann.

Die einfachste Art wäre, jeweils einen Block nach dem anderen getrennt zu verschlüsseln (ECB--Electronic Code Book). Jeder Block ergibt immer denselben Ciphertext. Darin liegt die größte Schwäche, weil ein einziges Paar Quelltext/Ciphertext reichen würde, um für einen bestimmten Key schon die Verschlüsselung einzelner Byte-Folgen zu erkennen. Außerdem könnten einzelne Blöcke in einer anderen Nachrichten ersetzt werden, was ohne Checksummen nicht bemerkt werden würde.

Durch Verkettung der Blöcke mit ihrem Vorgänger werden diese Probleme umgangen. Im CBC1-Modus (Cipher Block Chaining) wird jeder zu verschlüsselnde Block vor der Verschlüsselung mit dem Ciphertext des Vorgängers XOR genommen. Dadurch hängt die Verschlüsselung eines Blocks von der Verschlüsselung aller Vorgänger ab, obwohl sich der Aufwand dabei nur unwesentlich erhöht.

Es bleibt das Problem, daß Diskettenblöcke bis zu der Stelle, wo sie sich das erste Mal unterscheiden, gleich verschlüsselt werden. Das ist an sich keine Schwachstelle, liefert aber für eine Attacke mehr Informationen, als eigentlich nötig ist. In DiskProtection gibt es einen einfachen Mechanismus, der das verhindert: Das erste Langwort jedes Diskettenblock wird mit dem Wert XOR genommen, mit dem er angesprochen wird, und dann erst verschlüsselt. Da so der Anfang jedes zu verschlüsselnden Datenblocks unterschiedlich ist, ergeben auch Diskettenblöcke mit gleichem Inhalt komplett andere Ciphertexte.

Neben diesen beiden Modi und einer Vielzahl an Varianten gibt es noch zwei wichtige Modi, die jeweils pro Blockverschlüsselung eine bestimmte Anzahl Bits am Stück verschlüsseln (meist kleiner als die Blockgröße, etwa ein Byte) und auch mit Verkettung arbeiten: OFB und CFB. Beide haben Vorteile bei der Verschlüsselung eines Stroms von Daten, etwa einer Verbindung zwischen zwei Computern. Für die Verschlüsselung eines Diskettenblocks bieten sie aber keine Vorteile.

Auch wenn Sie die Wahl haben, sollten Sie für DiskProtection nach Möglichkeit immer CBC verwenden. Beachten Sie bitte auch die in xpkIDEA.doc beschriebenen Besonderheiten eines Passworts für IDEA: Bei einem ‘normalen’ Passwort ist IDEA.76 sicherer als IDEA.100!

1.78 DiskProtection.guide/DES

```
Der DES-Algorithmus
===================
```

DiskProtection hat den "Data Encryption Standard" DES im CBC1-Modus eingebaut. Mit Genehmigung des Autors wurde der Quelltext "D3DES" von Richard Outerbridge verwendet. DES entspricht bis auf leichte Modifikationen dem von IBM entwickeltem Algorithmus "Lucifer" und wurde 1977 von dem NBS (National Bureau of Standards) als nationaler Standard für nicht klassifizierte Kommunikation der US-Regierung verabschiedet.

DES verschlüsselt 64 Bit Blöcke und verwendet dazu einen 56 Bit Key. Verschlüsselung und Entschlüsselung verwenden denselben Algorithmus, aber behandeln den Key verschieden. Dieser Algorithmus führt vereinfacht gesagt 16 Runden derselben Operationen aus: Ersetzung und Vertauschung von Bits in Abhängigkeit vom Key.

DES läßt sich sehr gut mit Hardware implementieren. Software-Implementierungen sind dagegen langsamer als die anderer Algorithmen.

Geschichte
---

* 15. Mai 1973: öffentliche Aufforderung durch das NBS, einen Standardalgorithmus für Datenverschlüsselung zu entwickeln--keine geeigneten Einsendungen

* 27. August 1974: zweite Aufforderung
  IBM bietet den Anfang der 70er Jahre entwickelten Algorithmus "Luzifer" zu unentgeltlichen Nutzung an. Die NSA (National Security Agency) überprüft den Vorschlag und verringert die Key-Länge von 128 auf 56 Bits.

* 1975: Veröffentlichung des Vorschlags und Bitte um Stellungname

* 1976: Zwei öffentliche Workshops mit lebhaften Diskussionen über die Funktionsweise des Algorithmus' und die Frage nach einer "Trapdoor"

* 15. Januar 1977: Veröffentlichung als 'Data Encryption Standard" (DES) und darauf folgend Übernahme durch andere Standardisierungs-Organisationen; breite Nutzung durch Industrie und Banken

* 1987: trotz starker Bedenken der NSA Bestätigung von DES als Standard

* 1992: erneute Bestätigung des Standards, da keine Alternative in Sicht

Sicherheit

Es wurde viel darüber diskutiert, ob die NSA bei ihrer Überprüfung des Algorithmus' neben der Verkürzung der Key-Länge auch noch eine "Trapdoor" eingebaut haben könnte, um selbst DES-verschlüsselte Daten entschlüsseln zu können. Diese Behauptung wurde in Stellungnahmen von zwei Entwicklern IBMs und durch eine Untersuchung des US Senats verneint, obwohl nicht alle Zweifel

beseitigt wurden, weil das Ergebnis der Untersuchung klassifiziert und nicht veröffentlicht wurde.

Ein anderes Thema war die Key-Länge von 56 Bits. Es gibt verschiedene Berechnungen, zu welchen Kosten eine Maschine gebaut werden könnte, die durch Ausprobieren aller möglichen Keys eine Nachricht innerhalb einer bestimmten Zeit entschlüsselt. Diese Überlegungen kamen alle zu dem Schluß, das nur sehr große, staatliche Organisationen wie etwa die NSA dazu in der Lage wären, daß aber auf Grund der fortschreitenden technischen Entwicklung eine solche Maschine immer billiger und damit wahrscheinlicher werde.

DES hat sich auch als sehr resistent gegen verschiedene Attacken erwiesen, obwohl es schon Verfahren gibt, die weniger aufwendig als Ausprobieren sind. Mit vertretbarem Aufwand wurde DES bisher nur bei einer kleineren Rundenanzahl als 16 geknackt. Bei 16 Runden braucht die laut Bruce Schneier in 1993 effektivste bekannte Attacke, lineare Cryptoanalyse, noch 2^43 bekannte Plain-Texte.

1.79 DiskProtection.guide/IDEA und FEAL

Verwendung von IDEA und FEAL
============================

In der aktuellen Version des diskprot.devices sind mit Erlaubnis der Autoren leicht abgewandelte Versionen von xpkFEAL und xpkIDEA eingebaut, da es aufgrund des XPK-Konzepts im Moment nicht möglich ist, die Sub-Libraries direkt zu verwenden. Da die Algorithmen ansonsten vollständig den XPK-Sub-Libraries entsprechen, sei hier nur auf die entsprechenden Doc-Dateien verwiesen: IDEA.doc und FEAL.doc.

1.80 DiskProtection.guide/SCRM

Der Scramble-Algorithmus
========================

Scramble ist ein sehr schneller Verschlüsselungsalgorithmus, weil er extrem einfach ist - und daher auch völlig unsicher. Er kann den Inhalt Ihrer Platten nicht wirklich verschlüsseln, sondern nur verschleiern. Scramble kann und wird sicher gebrochen werden, wenn es jemand versucht. Er ist jedoch sicher genug, um es unmöglich zu machen, gleich auf den ersten Blick die Daten lesen zu können.

Scramble beruht darauf, daß jedes Langwort mit einem Wert xor genommen wird, der aus dem Passwort der DPUnit berechnet wurde. Dieser Wert ist jedoch nicht derselbe wie der in den Prefs gespeicherte Hash-Wert. Weitere Details verrate ich nicht, weil die (fragliche) Sicherheit des Algorithmus' zum Teil darauf beruht, daß der Algorithmus selbst geheim bleibt.

1.81 DiskProtection.guide/Frage & Antwort

```
Bekannte Probleme, Tips & Tricks
********************************

Doppelte Abfrage des System-Passworts
=====================================
```

Geben Sie beim Start von DiskProtection oder Ansprechen einer Unit das abgefragte Systempasswort nicht ein, sondern wählen Abbrechen, so werden Sie unter Umständen noch ein zweites Mal danach gefragt. Dies läßt sich nicht innerhalb von DiskProtection abstellen. Das Passwort wird nämlich beim Versuch, das diskprot.device zu öffnen, abgefragt. Das Öffnen schlägt fehl, wenn Sie das Passwort nicht eingeben. Das Betriebsystem versucht jetzt von sich aus ein zweites Mal, das Device zu öffnen, bevor es schließlich erst nach dem zweiten Fehlschlag zum Anwenderprogramm zurückkehrt.

```
DOS-Fehlermeldungen bei unverschlüsselter DPUnit
================================================
```

Wenn Sie in einer gemounteten DPUnit keine Verschlüsselung gewählt haben, können Sie über dieses DOS-Device auch unverschlüsselte Disketten ansprechen. Falls außerdem noch das DOS-Device gemountet haben, das normalerweise auf das jeweilige Exec-Device zugreift, etwa DF0:, dann bekommt Amiga-DOS zweimal dasselbe Volume in verschiedene Geräten gemeldet.

Damit kommt DOS nicht zurecht. Das äußert sich in z.B. in der Aufforderung, ein Volume einzulegen, das bereits eingelegt ist. Bei anderen CLI-Befehlen kann man dann immer noch auf das Volume zugreifen, mit anderen nicht mehr, etc. Derselbe Fehler tritt übrigens auf, wenn Sie eine Diskettenkopie anfertigen, bei der das Datum nicht geändert wird, und dann Original und Kopie in zwei verschiedene Laufwerke einlegen.

Das Problem läßt sich umgehen, indem man immer nur über ein DOS-Device auf das Volume zugreift, also entweder nur ueber die DPUnit oder ganz ohne die DPUnit anzusprechen.

```
Formatierung einer DPUnit
=========================
```

Ein Medium muß nicht unbedingt konvertiert werden, um in einer DPUnit verwendet werden zu können. Es genügt auch, das oder die Medien in der DPUnit zu formatieren. Die Option QUICK kann dabei verwendet werden.

Formatiert man so etwa eine Diskette, so wird jedoch DFx: nicht mitgeteilt, daß der Inhalt der Diskette sich geändert hat. Daher wird eine vorher normal formatierte Diskette weiterhin als vorhanden angezeigt, aber spätestens nach einem Diskettenwechsel oder durch Befehl DiskChange DFx: wird die Änderung erkannt.

```
Entfernen der ursprünglichen Partition
======================================
```

Wenn Sie eine Partition verschlüsselt habe, wird sie immer noch gemounted, obwohl sie nur noch als 'bad disk' erkannt wird. Mit HDToolBox kann diese Partition entfernen: HDToolBox starten, die unnütze Partition auswählen und Advanced Options und Change... anklicken. Automount this partition ausschalten, (zweimal) Ok, Save Changes to Drive und beenden.

Triton-Prefs für DiskProtection
==========

Ein kleiner Tip: DiskProtection sieht etwas besser aus, wenn Sie als Hintergrund für alle Fenster bei Bilder im Triton-Preferences-Programm etwas anderes als das normale Grau auswählen, z.B. Hell/Hintergrund.

1.82 DiskProtection.guide/History

History
****

Bitte in der englischen Anleitung oder der Datei History nachlesen. Auf Dauer ist es einfach sehr aufwendig, zwei Dokumente mit gleichem Inhalt zu führen...

1.83 DiskProtection.guide/Zukunft

Zukunft
****

Mir schweben noch einige Verbesserungen vor, die ihren Weg in eine zukünftige Version von DiskProtection finden könnten. Allerdings habe sich bis jetzt (16.11.95) erst 3 Personen registriert, und ich habe noch andere interessante und lohnende Projekte, daher werde ich mir gut überlegen, ob ich größere Features wirklich noch einbauen werde...

* Eine Möglichkeit, bei einem Absturz während der Konvertierung diese DPUnit zu retten.

* Einen schnellen, aber daher auch unsicheren Algorithmus einbauen.

* Hotkey(s), um die resetfesten Passwörter und/oder das komplette DiskProtection-Paket zu entfernen.

* Geschwindigkeitsoptimierung

* Mehr Sprachen unterstützen. Hier bin ich auf Hilfe angewiesen: Meine Sprachkenntnisse sind auf Englisch und Deutsch beschränkt. Jede Hilfe ist herzlich willkommen, auf Anfrage verschicke ich dann mehr Informationen darüber, wie ein Katalog für {No Value

```
     For "DiskProt"} erstellt werden kann.

   * Bei fehlendem Passwort das Device-Öffnen nicht fehlschlagen
     lassen, sondern solange "Keine Diskette eingelegt" melden, bis das
     Passwort eingegeben wurde. Braucht das jemand?

   Falls Sie irgendwelche Anregungen äußern wollen, Fehler gefunden
haben oder Ihnen das Programm ganz einfach gefallen hat, so würde ich
mich freuen, davon zu hören. Vor allem natürlich im letzten Fall,
besonders wenn zusammen mit der Nachricht auch die Shareware-Gebühr
eintrifft...

   Meine Adresse steht in Adresse.
```

1.84 DiskProtection.guide/Adresse

```
Adresse des Autors
******************

     Patrick Ohly
     Weechstr. 1, WG E0/1
     76131 Karlsruhe

     Tel.: 0721/615662
     eMail: patrick.ohly@stud.uni-karlsruhe.de
     IRC: Irish

     Bankverbindung:
     Sparkasse Karlsruhe, BLZ 660 501 01
     Konto--Nr. 100 621 31

   Bitte nach Möglichkeit eMail benutzen--so bekommen Sie am ehesten
eine Antwort ;-)
```

1.85 DiskProtection.guide/Credits

```
Credits
*******

   Mein Dank geht an (Reihenfolge ohne tiefere Bedeutung ;-):

Stefan Zeiger
     für die triton.library im allgemeinen und insbesondere die
     Berücksichtigung meiner Wünsche und Anregungen

Richard Outerbridge
     für seinen DES-Quellcode

Angela Schmidt
     für ihren hübschen GadTools Registriernummer-Requester
```

```
Christian 'Nescum' von Roques
     für xpkFEAL, Informationen zur xpkmaster.library

André 'ABPSoft' Beck
     für xpkIDEA und Ideen zur Verschlüsselung von Disketten

Bernhard 'ZZA' Möllemann, Mark Rose
     für's Beta-Testen, Anregungen und Kritik

Daniel Schrod
     für seine Bemühungen, mich vom großen Nutzen von DiskProtection
     für die Menschheit zu überzeugen ;-), häufiges Nachhaken und
     schließlich Beta-Testen

Thomas Schröder
     für das bereitwillige Verleihen seiner Terry-Pratchett-Bücher 8-)

Michael 'Mick' Hohmann
     für seine NetWB-Icons (mein eigener Versuch konnte seinem
     DiskProtection-Icon nicht das Wasser reichen...)

Klaus Deppisch
     für seinen FFS-Patch

all die, die ich bisher vergessen habe sollte
     für dies und das

   Alle Angaben ohne Gewähr. Der Rechtsweg ist ausgeschlossen.
```

1.86 DiskProtection.guide/Standardwerte

```
Standardwerte
*************

   * Zugangsschutz

        - Hotkey: "CTRL ALT b"

        - Zeitspanne: 300s

        - beim Programmstart: Nein

        - Bildschirm: PAL/NTSC:LowRes, 320x200, 4 Farben

        - Zeichensatz: topaz 8

        - Dimmer: 100%

   * System-Verschlüsselung: IDEA, Mode 100

   * Passwort-Text: "" (leerer String)
```

1.87 DiskProtection.guide/Glossar

```
Glossar
*******

DES
     Data Encryption Standard: Datenverschlüsselungsalgorithmus,
     Standardalgorithmus der US-Regierung für nicht klassifizierte
     Informationen

DOS-Device
     Gerätetreiber für IO-Geräte auf DOS-Seite. Verwaltet Daten in
     Dateien und Verzeichnisse und schreibt sie u.U. über ein
     Exec-Device als Blöcke auf einen Datenträger. Beispiele: DF0:,
     HD0:, RAM: (letzteres verwendet kein Exec-Device). Werden beim
     Booten oder nachträglich durch MOUNT eingerichtet.

(DP)Units
     Bezeichnet eine Einheit des diskprot.devices. Steht auch für den
     Datenträger, der damit über DiskProtection  angesprochen wird,
     oder das DOS-Device, mit dem das geschieht. Wenn aus dem
     Zusammenhang klar, wird das DP aus Gründen der Lesbarkeit
     weggelassen.

Exec-Device
     Gerätetreiber auf Exec-Ebene. Verwaltet Daten i.d.R. blockweise.
     Beispiele: trackdisk.device, ramdrive.device

FEAL
     Fast Encryption Algorithm: ein Datenverschlüsselungsalgorithmus

HASH-Wert
     Großer Zahlenwert, der aus einer Zeichenkette gebildet wird, aber
     keine Rückschlüsse auf diese erlaubt und für unterschiedliche
     Zeichenketten mit hoher Wahrscheinlichkeit auch unterschiedlich
     ist.

Medium
     Der eigentliche Datenträger in einem Gerät. Beispiele: Diskette,
     Wechselplatte

IDEA
     International Data Encryption Algorithm: ein
     Datenverschlüsselungsalgorithmus

Volume
     Ein einzelner Datenträger so wie er von DOS gesehen wird. Wird
     durch seinen Namen angesprochen, unabhängig davon, ob er im
     Moment in einem Gerät eingelegt ist. Beispiele: Eine bestimmte,
     formatierte Diskette, Workbench: im Gegensatz zu HD0:.
```

1.88 DiskProtection.guide/Index

Index
*****

Adresse des Autors Adresse
Aenderung der DPUnit-Verschluesselung-Requester Unit-Konvertierung
Aktivierung des Zugangschutzes Zugangsschutz
Algorithmen, Anforderung an Verschlüsselung
Algorithmus-Requester Algorithmus und Modus auswaehlen
Anmeldedateien DOS-Devices
Anmeldedateien Editieren Anmeldedateien
Ansatz von DiskProtection Ansatz
Anzeige der DPUnit DPUnit
Argumente von DiskProtection (Prefs) Programmstart
Autor von DiskProtection Adresse
Bankverbindung Adresse
Bekannte Fehler und Maengel Frage & Antwort
Block-Verschluesselung Block-Verschluesselung
Blockmodi bei Verschluesselung Block-Verschluesselung
Blockorientierte Verschluesselung Ansatz
CBC Block-Verschluesselung
CFB Block-Verschluesselung
Copyrights Copyrights
Credits Credits
Danksagung Credits
Data Encryption Standard DES
Datei fuer Passwort verstecken Dateiname
Datenschutz-Einstellungen Datenschutz
Default-Werte Standardwerte
DES DES
Device contra Handler Ansatz
Disclaimer Haftungsausschluss
DiskProtection (Prefs), Hauptfenster von Hauptfenster
DiskProtection (Prefs), Menus von Menus
DiskProtection (Prefs), Starten von Programmstart
DiskProtection, Ansatz von Ansatz
DiskProtection, Autor von Adresse
DiskProtection, bisherige Versionen von History
DiskProtection, Konzept von Konzept
DiskProtection, Kopieren von Lizenz
DiskProtection, Prefs-Programm DiskProtection
DiskProtection, Testen von Installation
DiskProtection, Triton-Prefs fuer Frage & Antwort
DiskProtection, Units von Units
Doppelte Abfrage des System-Passworts Frage & Antwort
DOS-Device auswaehlen-Requester DOS-Device auswaehlen
DOS-Drivers DOS-Devices
DOS-Fehler bei unverschluesselter DPUnit Frage & Antwort
DP-Mountlist DOS-Devices
DPInit DPInit
DPUnit Units
DPUnit Editieren-Fenster DPUnit Editieren
DPUnit Editieren: Anmeldedateien Anmeldedateien
DPUnit Editieren: Anzeige der DPUnit DPUnit
DPUnit Editieren: Datenschutz Datenschutz
DPUnit Editieren: Erweiterte Einstellungen Erweiterte Einstellungen
DPUnit, Formatierung einer Frage & Antwort

DPUnit-Verschluesselung aendern?-Requester Automatische Unit-Aenderung
DPUnits eines Passworts (Prefs) Units des Passworts
ECB Block-Verschluesselung
Einfuehrung Ueberblick
Einstellungen einer DPUnit Units
Einstellungen eines Passworts Passwort
Einstellungen, Speichern der Speichern der Einstellungen
eMail-Adresse Adresse
Erweiterte Einstellungen einer DPUnit Erweiterte Einstellungen
Erzeugung eines Hash-Wertes Hash-Wert
FEAL IDEA und FEAL
Fehler, bekannte Maengel und Frage & Antwort
Fenster: 'DPUnit Editieren' DPUnit Editieren
Fenster: 'Passwort Editieren' Passwort Editieren
Formatierung einer DPUnit Frage & Antwort
Glossar Glossar
Grundlagen der Kryptologie Grundlagen
Haftungsausschluss Haftungsausschluss
Hash-Funktion Hash-Wert
Hash-Wert, Erzeugung eines Hash-Wert
Hash-Werte von Passwoertern Passwörter
Hauptfenster von DiskProtection Hauptfenster
Hauptfenster, Listviews im Units und Passwoerter
Hauptfenster, Sytem-Verschluesselung System-Verschluesselung
Hauptfenster, Zugangsschutz im Einstellungen Zugangsschutz
History History
IDEA IDEA und FEAL
Installation Installation
Konvertierungs-Fehler-Requester Konvertierungs-Fehler
Konzept von DiskProtection Konzept
Kopieren von DiskProtection Lizenz
Kryptologie, Grundlagen der Grundlagen
Listviews im Hauptfenster Units und Passwoerter
Lizenz Lizenz
Luzifer DES
Maengel, bekannte Fehler und Frage & Antwort
MakeAssigns Installation
Menu: Piktogramme erzeugen? Optionen
Menu: Projekt Projekt
Menu: Vorgaben Vorgaben
Menus von DiskProtection (Prefs) Menus
Mounten einer DPUnit DOS-Devices
OFB Block-Verschluesselung
One-Way-Hash-Funktion Hash-Wert
Online-Verschluesselung Ansatz
Passwoerter Passwörter
Passwoerter nach einem Reset Reset
Passwoerter, erlaubte Zeichen in Passwörter
Passwoerter, Hash-Werte von Passwörter
Passwoerter, in Datei versteckte In Datei verstecken
Passwoerter, resetfeste Passwort resetfest machen
Passwort Editieren-Fenster Passwort Editieren
Passwort verstecken (Prefs) Verstecken
Passwort, Abfrage eines Passwort
Passwort, DPUnits eines Passwort
Passwort, Einstellung der DPUnits eines Units des Passworts
Passwort, Einstellungen bei Passwort

Passwortabfrage Passwort
Passworteingabe-Requester Passworteingabe
Piktogramme erzeugen? Optionen
Preferences, Speichern der Speichern der Einstellungen
Preferences-Konzept Preferences-Konzept
Prefs-Programm von DiskProtection DiskProtection
Programm-Versionen History
Programmschutz Programmstart
Projekt-Menu Projekt
Requester: Aenderung der DPUnit-Verschluesselung Unit-Konvertierung
Requester: Algorithmus Algorithmus und Modus auswaehlen
Requester: DOS-Device auswaehlen DOS-Device auswaehlen
Requester: DPUnit-Verschluesselung aendern? Automatische Unit-Aenderung
Requester: Konvertierungs-Fehler Konvertierungs-Fehler
Requester: Passworteingabe Passworteingabe
Reset, Passwoerter bei einem Reset
Resetfeste Passwoerter Passwort resetfest machen
Scramble SCRM
SCRM SCRM
Shareware Lizenz
Speichern der Einstellungen Speichern der Einstellungen
StackSize in Anmeldedateien DOS-Devices
Standardwerte Standardwerte
Starten von DiskProtection (Prefs) Programmstart
System-Passwort, doppelte Abfrage des Frage & Antwort
System-Passwort, Vorgaben Standardwerte
System-Verschluesselung (Prefs) System-Verschluesselung
Systempasswort Systempasswort
Testen von DiskProtection Installation
Tips & Tricks Frage & Antwort
Trademarks Copyrights
Triton-Prefs fuer DiskProtection Frage & Antwort
Ueberblick Ueberblick
Uebersicht Ueberblick
Units von DiskProtection Units
Unverschluesselte DPUnit, DOS-Fehler bei Frage & Antwort
Verbreitung Lizenz
Verschluesselung von Diskettenbloecken Ansatz
Verschluesselung, Blockmodi Block-Verschluesselung
Verschluesselungs-Algorithmen Verschlüsselung
Verschluesselungsart Units
Versionen des Programms History
Versteckte Passwoerter In Datei verstecken
Voraussetzungen Ueberblick
Vorgaben setzen Vorgaben
Vorgaben-Menu Vorgaben
Vorgabewerte Standardwerte
Warenzeichen Copyrights
XPK-Sub-Libraries Verschlüsselung
xpkFEAL IDEA und FEAL
xpkIDEA IDEA und FEAL
Zeichen in Passwoertern Passwörter
Zeitlimit bei Passwortabfrage Passwort
Zugangsschutz Zugangsschutz
Zugangsschutz (Prefs) Einstellungen Zugangsschutz
Zukunft Zukunft