Enigma für Windows Hilfe Inhalt

■ Klicken Sie auf das unterstrichene Thema, das Sie einsehen möchten. Sie können auch die TABULATORTASTE benutzen, um das Thema zu markieren und dann die EINGABETASTE drücken. Um die Verwendung von Hilfe zu erlernen, drücken Sie die Taste F1.

Der Index enthält eine Liste aller Hilfe Themen zu Enigma. Um allgemeine Informationen zur Benutzung des Windows Hilfesystem zu erhalten, betätigen Sie die Taste F1 oder den Menüpunkt "Hilfe benutzen".

Was ist Enigma für Windows ?

Enigma für Windows ist ein leistungsfähiges Programm zum Chiffrieren und Dechiffrieren von Dateien beliebiger Art. Es beinhaltet neben den Chiffrierfunktionen auch die Funktion eines elektronischen Aktenvernichters. Der Name "Enigma" stammt von der gleichnamigen legendären Verschlüsselungsmaschine des 2. Weltkrieges.

Jeder hat wenigstens eine Datei, deren Inhalt er geheimhalten möchte, sei es ein Liebesbrief oder etwas so wichtiges wie eine Patentschrift. Viele Angestellte arbeiten täglich mit Daten, die nicht für die Allgemeinheit bestimmt sind, z.B. individuelle oder Firmendaten, Gehalts- oder Personallisten, usw., die sich gewöhnlich erst dann "in Sicherheit" befinden, wenn sie hinter einem traditionellen Schloß eingeschlossen sind.

Im Zeitalter des massiven Computereinsatzes in Arztpraxen, Banken, Büros und Behörden, der Vernetzung mehrerer Rechner und des elektronischen Datenaustausches sind Hilfsmittel notwendig, um die Daten alternativ vom herkömmlichen Wege geeignet zu schützen.

Obwohl es eine gute Idee ist, Disketten mit sensiblen Inhalt wegzuschließen, wird dieser Vorgang durch das Verschlüsseln seiner Daten mit einem privatem Passwort eine Stufe sicherer. Sie sollten Dateien immer dann chiffrieren, wenn sie streng vertrauliche Informationen enthalten, die unter keinen Umständen ohne Ihre Zustimmung gelesen werden dürfen. Chiffrierte Dateien können weder von anderen Benutzern gelesen noch dechiffriert werden. Die einzige Möglichkeit, die Daten wieder lesbar und benutzbar zu machen, ist die Dechiffrierung mit dem bei der Chiffrierung eingegeben Passwort.

Die Sicherheit verschlüsselter Daten gegenüber potentiellen Schnüfflern oder Eindringlingen hängt maßgeblich von der verwendeten Chiffriermethode ab. Neben dem RSA-Verschlüsselungssystemen hat sich vor allem der sogenannte Data Encryption Standard (DES), ein in den USA für öffentliche Behörden zum Standard erklärtes und hier implementiertes Verfahren, in der Praxis bewährt.

Es kann davon ausgegangen werden, daß mit DES chiffrierte Daten innerhalb eines sinnvollen Zeitraums auch mittels eines Superrechners nicht dechiffriert werden können.

Viele große Unternehmen benutzen Aktenvernichter, um sich ihrer sensiblen Daten auf Papier zu entledigen. Die in Enigma implementierte Funktion Wipe (zu deutsch: vernichten) ist das elektronische Gegenstück dazu. Viele Computerbenutzer wissen nicht, daß mit dem MSDOS Befehl **DEL** gelöschte Dateien ohne größeren Aufwand in den meisten Fällen wiederhergestellt werden können, sogar nach längerer Zeit, wenn man bereits gar nicht mehr an diese denkt. Benutzen Sie die Wipe Funktion, so können Sie sicher sein, daß von Ihren so gelöschten Dateien keine Spuren mehr auf Ihrer Festplatte zu finden sind.

Chiffrierung

Die klassische Aufgabe der Kryptographie ist es, eine Nachricht oder Aufzeichnung für den Unbefugten unverständlich zu machen mit dem Ziel der Geheimhaltung dieser Daten. Die Transformation der "echten" Daten, des sogenannten Klartext in den Geheimtext bezeichnet man als Chiffrierung.

RSA Algorithmus

Verschlüsselungssytem mit öffentlichen Schlüssel, benannt nach seinen Entwicklern Ronald Rivest, Adi Shamir und Leonard Adleman, die ihren Algorithmus 1978 am MIT vorstellten. Hierbei werden jedem Benutzer zwei Schlüssel (Passwörter) zugeordnet, ein privates und ein öffentliches. Letzteres wird meistens in einer Liste veröffentlicht, die jedem Nutzer zugänglich ist. Chiffriert wird mit dem privaten Passwort und dem öffentlichen Passwort des Empfängers. Der Empfänger dechiffriert die Nachricht durch die Eingabe seines privaten Passworts. Der hierbei verwendete Algorithmus beruht auf der Faktorisierung großer Zahlen (meist Primzahlen), ausgehend von der weithin akzeptierten (aber nicht bewiesenen) Hoffnung, daß diese Faktorisierung mit den heutigen Mitteln nicht umkehrbar ist.

Änderungen zur Version 1.1

Die aktuelle Version 2.0 zeichnet sich im Vergleich zur Version 1.1 durch zahlreiche Erweiterungen aus, die im folgenden kurz genannt seien:

- Komfortables Installationsprogramm.
- Kontextsensitive Hilfe durch Betätigung der F1-TASTE
- Chiffrierung, Dechiffrierung und Vernichtung von mehreren Dateien und ganzer Verzeichnisstrukturen in einem Schritt
- Dialog gesteuerte Wahl des Ausgabeverzeichnisses
- Abbruchmöglichkeit des Chiffrierungsvorgangs
- 15% Steigerung der Performance bei Chiffrierung
- Entfernung der Möglichkeit die Dateien vor der Chiffrierung zu komprimieren. Ein Programm mit dieser Funktionalität ist getrennt erhältlich.
- Inkompatibel zu mit Enigma 1.x erstellten Dateien (Um das gleichzeitige Bearbeiten mehrerer Dateien zu ermöglichen, mußte die produzierte Dateistruktur grundsätzlich überarbeitet werden. Herausgekommen ist eine moderne Archivstruktur, an die sich zukünftige Versionen halten werden.

Enigma Installation

Enigma für Windows wird mit einem komfortablen Installations Programm vertrieben, daß die folgenden Aufgaben erfüllt:

- Kopieren der Enigma Programmdateien in ein Verzeichnis Ihrer Wahl. (default: C:\Enigma20). Enigma für Windows belegt ungefähr 700 Kilobyte Ihrer Festplatte.

- Modifikation des Windows Initialisierungsfile WIN.INI durch das Hinzufügen der Zeile "en2=C:\ENIGMA20\ENIGMA20.EXE ^.EN2".

- Erzeugung der Programm - Manager Gruppe "Enigma 2.0"

- Erzeugung der Datei "ENIGMA20.INI" in Ihrem Windows Verzeichnis

Zur Installation gehen Sie nach folgender Reihenfolge vor:

- Starten Sie MS-Windows !

- Starten Sie den Programm Manager !

- Aus dem Menüpunkt "Datei" wählen Sie "Ausführen..." !

- Geben Sie jetzt entweder "A:\INSTALL" oder "B:\INSTALL" ein, je nach dem in welchem Laufwerk sich Ihre Installationsdiskette befindet !

- Es erscheint eine Dialogbox, die das empfohlene Verzeichnis für Enigma anzeigt: Wählen Sie hier das Verzeichnis, in das Sie das Programm installieren wollen. Existiert das angegebene Verzeichnis noch nicht, wird es automatisch angelegt. Betätigen Sie den Schalter "OK" um die Installation zu starten !

- Das Installationsprogramm beginnt nun mit dem Kopieren der Dateien in das angegebene Verzeichnis. Danach wird die Programm-Manager Gruppe angelegt, und die Installation ist beendet.

Die Versionen 1.1 und 2.0 sind untereinander nicht kompatibel. Für die Dechiffrierung ist immer die Version notwendig, mit der chiffriert wurde.

System Anforderungen

Für die Benutzung von Enigma Version 2.0 gelten folgende Minimalanforderungen:

Software:
- Microsoft Windows Version 3.1 oder Windows NT
- IBM OS/2 Version 2.1

Hinweis: Bei der Benutzung von On-Line Komprimierern wie Stacker oder DoubleSpace kann keine Garantie übernommen werden, daß mit WIPE gelöschte Daten nicht wiederherstellbar sind.

Hardware:
- VGA - Karte
- Enigma erfordert keine weiteren Hardwarevoraussetzungen, außer die, die für die Lauffähigkeit der oben genannten Software notwendig sind.

Hinweis: Obwohl Enigma mit sehr schnellen Algorithmen arbeitet, ist das Chiffrieren auf Grund der Komplexität der Algorithmen immer eine zeitintensive Angelegenheit. Es wird deshalb ein AT486 empfohlen.

Enigma starten

Sie können Enigma sowohl von Windows als auch von der DOS-Eingabeaufforderung aus starten.

So starten Sie Enigma aus dem Windows Programm-Manager

1 Wechseln Sie zum Programm-Manager-Fenster.
2 Öffnen Sie das Gruppenfenster, welches das Enigma-Symbol enthält.
3 Führen Sie einen der folgenden Schritte aus:

- Doppelklicken Sie auf das Enigma-Symbol.
- Verwenden Sie die Cursortasten, um das Enigma-Symbol auszuwählen, und drücken Sie dann die EINGABETASTE.

Starten von Enigma aus dem Windows-Menü Datei

1 Wählen Sie im Programm-Manager-Menü Datei den Befehl Ausführen.
2 Führen Sie einen der folgenden Schritte aus:

- Befindet sich Enigma in Ihrem Pfad, geben Sie Enigma ein.
- Befindet sich Enigma nicht in Ihrem Pfad, geben Sie den Pfad für Enigma ein, zum Beispiel: c:\enigma20\enigma20.exe

3 Wählen Sie "OK".

So starten Sie Enigma von der DOS-Eingabeaufforderung aus

1 Geben Sie nach der DOS-Eingabeaufforderung "win enigma20" ein.
2 Drücken Sie die EINGABETASTE.

Hinweis:
Erscheint eine Meldung, die angibt, daß die Datei "enigma20.exe" nicht gefunden werden konnte, so ist das Verzeichnis, das enigma enthält, nicht in Ihrem Pfad. Wechseln Sie zu dem Verzeichnis, das Ihre Datei "enigma20.exe" enthält, und versuchen Sie erneut, Enigma zu starten.

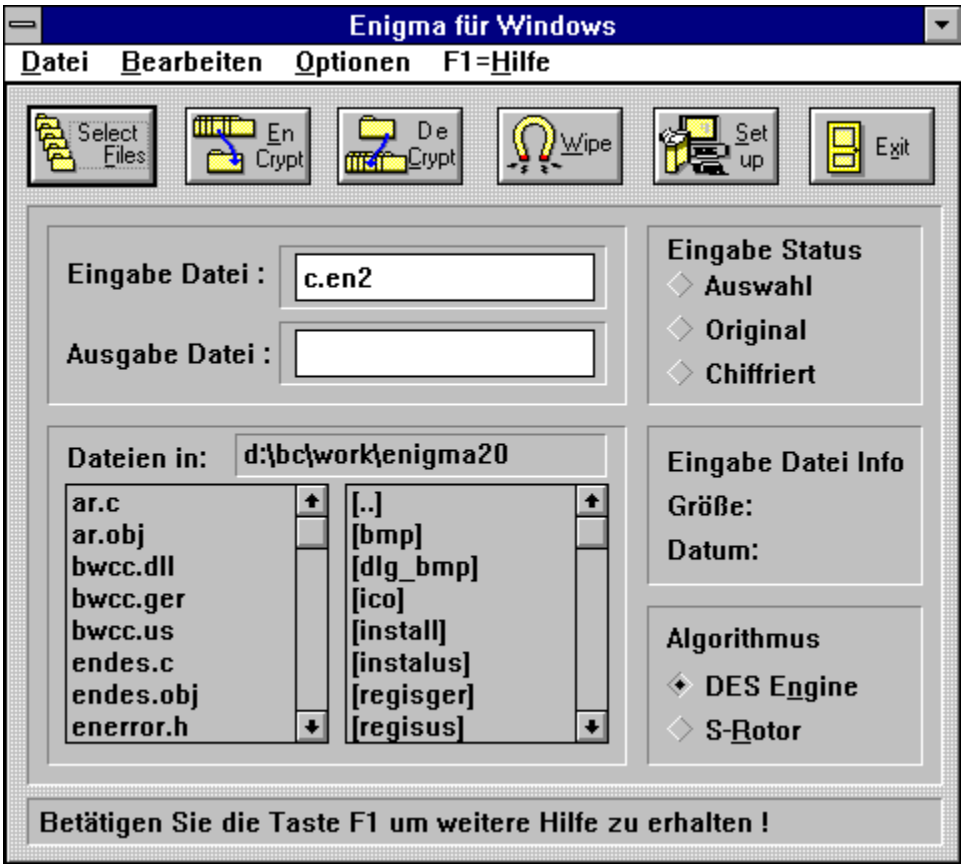
Starten von Enigma aus einem Windows-Kommandozeilen Interface

Innerhalb WinCLI, WinCLI Pro, 4Win ... durch das Wechseln in das Directory wo enigma20.exe gespeichert ist und das Eingeben von enigma20.

Bemerkung: Wenn Sie Enigma das erste Mal starten, erscheint ein kleiner Dialog, der Sie zur Registrierung des Programms auffordert. Geben Sie hier Ihre Registrierungsnummer ein. Sie finden Sie auf dem Diskettenlabel. Ohne Eingabe dieser Nummer ist der DES Algorithmus nicht verfügbar.

Die Enigma Oberfläche

■ Bewegen Sie den Mauszeiger über das Bild. Immer wenn Sie eine Hand zu sehen bekommen, können Sie durch Drücken der linken Maustaste weitere Informationen erhalten.



Befehle des Menüs Datei

Auswählen...

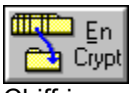
Öffnet einen Dialog, indem einzelne Dateien oder auch ganze Verzeichnisse ausgewählt werden können. **[(ALT-S),(ALT-D,A)]** Weitere Informationen erhalten Sie im Thema "Dateien auswählen"

Beenden

Enigma beenden.**[(ALT-X),(ALT-D,B),(ALT-F4)]**

Befehle des Menüs Bearbeiten

Chiffrieren...



Chiffrierung der ausgewählten Dateien. **[(ALT-E),(ALT-B,C)]** Weitere Informationen erhalten Sie im Thema "Dateien chiffrieren".

DeChiffrieren...

Dechiffrierung der ausgewählten Datei. **[(ALT-C),(ALT-B,D)]** Weitere Informationen erhalten Sie im Thema "Datei dechiffrieren".

Wipe...

Vernichtung der ausgewählten Dateien. **[(ALT-W),(ALT-B,W)]** Weitere Informationen erhalten Sie im Thema "Dateien vernichten".

- # Befehle des Menüs Optionen

Setup...

Öffnet das Setup Fenster, indem verschiedene Einstellungen von Enigma verändert werden können. **[(ALT-U),(ALT-O,S)]**

Benutzer Passwort...

Öffnet ein Fenster, indem der Benutzer das Passwort eintragen kann, daß er permanent zur Chiffrierung benutzen möchte. Weitere Informationen erhalten Sie im Thema "Benutzer Passwort".**[(ALT-O,B)]**

Registrierung...

Öffnet ein Fenster, indem das Passwort zur Registrierung von Enigma eingegeben werden kann. **[(ALT-O,R)]** Der DES Algorithmus ist ausschließlich in der registrierten Version von Enigma verfügbar.

Befehle des Menüs Hilfe

Inhalt

Öffnet das Hilfe Inhaltsverzeichnis für Enigma

Dateien auswählen

Anzeigen des Hilfethema "Dateien auswählen"

Dateien chiffrieren

Anzeigen des Hilfethema "Dateien chiffrieren"

Datei dechiffrieren

Anzeigen des Hilfethema "Datei dechiffrieren"

Dateien vernichten

Anzeigen des Hilfethema "Datei vernichten"

Registrierung

Anzeigen des Registrierung Formulars, das von hier aus gedruckt werden kann.

Hilfe benutzen

Anzeigen des Thema "Microsoft Hilfe benutzen"

Info...

Anzeigen der aktuellen Hard- und Software Umgebung, der Enigma Versionsnummer und des Copyrights.

Dateien auswählen

Dieser Dialog besteht im wesentlichen aus drei Listenfenstern und ist für die Zusammenstellung der Dateien bestimmt, die später chiffriert oder vernichtet werden sollen. Mit Hilfe verschiedener Schalter können sowohl Dateien als auch ganze Verzeichnisstrukturen ausgewählt werden. Die ausgewählten Dateien befinden sich im unteren Listenfenster. In den beiden anderen Listenfenstern markierte Dateien und Verzeichnisse können mit dem Schalter "Update" in dieses Listenfenster bewegt werden. Wenn Sie die gewünschten Dateien ausgewählt haben, betätigen Sie den "OK" Schalter. Es folgt eine kurze Beschreibung der wichtigsten Schalter in diesem Dialog.

Beim Betätigen dieses Schalters wird das Datei-Listenfenster entsprechend der links stehenden Dateimaske (regulärer Ausdruck) aktualisiert. **[(ALT-M)]**

Beim Betätigen dieses Schalters wird das Startverzeichnis für die Chiffrierung gesetzt. Bei der Verarbeitung mehrerer Dateien in unterschiedlichen Directories muß ein definierter Ausgangspunkt geschaffen werden, um die Verzeichnisstruktur bei der Dechiffrierung restaurieren zu können. Dieser Schalter ist anfänglich nicht verfügbar und das aktuelle Directory ist automatisch als Startverzeichnis gesetzt. Dieser Schalter wird verfügbar, wenn in ein Verzeichnis gewechselt wird, daß in seiner Hierarchie höher liegt (**[..]**) als das momentan eingestellte Startverzeichnis oder beim Wechsel des Laufwerks. **[(ALT-T)]**

Markierung aller im linken Listenfenster befindlichen Dateien. Die linke Listbox läßt die sogenannte "Mehrfachauswahl" zu, daß heißt, Sie können durch einfaches Herunterziehen der Maus (bei gedrückter linker Maustaste) mehrere Einträge auswählen, bei gleichzeitigem Halten der CTRL Taste auch Einträge, die nicht unmittelbar aufeinander folgen. **[(ALT-S)]**

Markierung im linken Listenfenster zurücknehmen. **[(ALT-D)]**

Beim Betätigen dieses Schalters wird das hervorgehobene Verzeichnis im rechten Listenfenster ausgewählt. Wenn Sie als nächstes den "Update" Schalter drücken, werden alle Dateien die sich unter diesem Verzeichnis und dessen Unterverzeichnissen befinden, ausgewählt (sofern sie der gesetzten Dateimaske entsprechen) und in das untere Listenfenster übertragen. **[(ALT-R)]**

Bei Betätigung dieses Schalters werden die vorher markierten Dateien in das untere Listenfenster übertragen. Jeder Markierung muß die Betätigung dieses Schalters folgen, um die Auswahl abzuschließen. **[(ALT-U)]**

Markierte Dateien im unteren Listenfenster entfernen. **[(ALT-E)]**

Alle Dateien im unteren Listenfenster entfernen. **[(ALT-A)]**

Hinweis: In der jetzigen Version von Enigma sind die Anzahl der Dateien, die in einem Schritt ausgewählt werden können, beschränkt. Dies hat seine Ursache in der begrenzten Kapazität der Standard Listboxen unter Windows. Diese Schwachstelle wird in der nächsten Version behoben sein. Wenn Sie als Ausgabedatei eine existierende Archivdatei wählen, werden alle Dateien, die dort noch nicht enthalten, sind dem Archiv hinzugefügt.

Regulärer Ausdruck

Als Dateimaske kann auch ein (begrenzter) regulärer Ausdruck eingegeben werden. Folgende Metazeichen sind implementiert:

- ***** steht für jede Zeichenkette einschließlich der leeren.
- **?** steht für jedes einzelne Zeichen.
- **[...]** steht für jedes einzelne Zeichen innerhalb der Klammern.
- **[^...]** steht für jedes einzelne Zeichen, welches NICHT innerhalb der Klammern steht.
- **-** Kann innerhalb von Klammern zur Kennzeichnung eines Zeichenbereichs benutzt werden (z.B. paßt sws[1-36] für sws1, sws2, sws3 und sws6).
- **** Kann innerhalb von Klammern zur Entwertung von Spezialzeichen benutzt werden, insbesondere für die hier verwendeten Metazeichen, z.B. "\]" und "\-" an jeder Stelle innerhalb der Klammern und "\^" direkt nach der öffnenden Klammer. Der Ausdruck \xyz entspricht dem ASCII - Zeichen dessen oktaler Wert gleich xyz ist..

- Alle anderen Zeichen stehen für sich selbst.

(Herr Duden , verzeihen Sie mir !)

Dateien chiffrieren

Sie können entweder eine einzelne Datei oder mehrere Dateien chiffrieren. Sollen mehrere Dateien chiffriert werden, so müssen diese vorher im Dialog "Dateien auswählen" markiert werden.

Eine gültige Dateiauswahl läßt sich an der Markierung des Statussymbols "Auswahl" erkennen. In diesem Fall erscheint im Textfeld "Eingabe Datei" das Wort ">> Auswahl Liste <<", bei der Chiffrierung einer Einzeldatei deren Dateiname. Tragen Sie nun den Namen (ohne Pfad) für die Augabedatei in das Textfeld "Ausgabe Datei" ein.

Nach Wahl der Ein- und Ausgabedatei(en) kennzeichnen Sie den Algorithmus, mit dem die Dateien chiffriert werden sollen. Klicken Sie dazu auf das Statussymbol "DES-Engine" oder "S-Rotor".

Jetzt betätigen Sie den Schalter "EnCrypt" oder den gleichnamigen Befehl im Menü "Bearbeiten". Haben Sie mehrere Dateien ausgewählt, erscheint ein neuer Dialog, indem Sie Ihre Auswahl nochmals bestätigen.

Benutzen Sie in diesem Dialog die 4 Schalter in der Mitte, um die Dateien zwischen den Listboxen zu bewegen. Alle Dateien in der unteren Listbox werden chiffriert. Betätigen Sie den "OK" Schalter.

Es erscheint ein neuer Dialog, indem Sie das Directory bestimmen können, in das Ihre Ausgabedatei kopiert wird. Vergleichen Sie die beiden Größenangaben. Sie müssen ein Verzeichnis auswählen, das ausreichend Platz für die chiffrierten Daten bietet. Betätigen Sie den "OK" Schalter.

Vor der Chiffrierung der ausgewählten Dateien müssen Sie in dem nun folgenden Dialog Ihr persönliches Passwort eingeben. Niemand kann auf die chiffrierten Daten zugreifen, es sei denn, er hat Kenntnis von diesem Passwort. Nähere Informationen hierzu erhalten Sie im Thema "Passwort auswählen".

Nach Eingabe des Passworts kann der Chiffriervorgang gestartet werden; es erscheint ein neues Fenster, das Sie über den Status der Chiffrierung informiert und wo Sie jederzeit die Operation abbrechen können.

Hinweis: Soll eine bereits chiffrierte Datei nochmals chiffriert werden, so muß vorher das Statussymbol "ORIGINAL" markiert werden.

Haben Sie als Ausgabedatei eine schon existierende chiffrierte Datei ausgewählt, so werden die selektierten Dateien dieser Datei hinzugefügt. Befinden sich gleichnamige Dateien in dieser Datei, so werden diese durch die aktuell ausgewählten ersetzt. Wenn Sie zur aktuellen Chiffrierung ein anderes Passwort als zur Chiffrierung der bestehenden Datei verwenden, so müssen Sie selbst dafür Sorge tragen, wie sie die einzelnen Dateien mit dem richtigen Passwort wieder dechiffrieren. Dieses Vorgehen wird ausdrücklich NICHT empfohlen !!!

Datei dechiffrieren

Markieren Sie die zu dechiffrierende Datei in der linken Listbox des Hauptdialoges. Ist die Datei chiffriert, wird das Statussymbol "Chiffriert" markiert.

Sie können selbstverständlich nur Dateien mit Enigma dechiffrieren, die vorher mit dem Programm chiffriert wurden. Der Dateiname erscheint in der Textbox "Eingabe Datei:". Danach betätigen Sie den Schalter "DeCrypt" oder den gleichnamigen Befehl im Menü "Bearbeiten".

Es erscheint ein Dialog, indem die chiffrierten Dateien innerhalb der Eingabedatei angezeigt werden. Dort können Sie die Dateien auswählen, die dechiffriert werden sollen. Betätigen Sie "OK" nach Abschluß der Auswahl.

Nun erscheint ein Dialog, indem Sie das Directory bestimmen können, in das Ihre dechiffrierten Dateien kopiert werden sollen. Vergleichen Sie die beiden Größenangaben. Sie müssen ein Verzeichnis auswählen, das ausreichend Platz für die dechiffrierten Daten bietet. Betätigen Sie den "OK" Schalter.

Als nächstes erscheint ein Dialog, indem das bei der Chiffrierung der Dateien verwendete Passwort eingegeben werden muß. Nun kann die Dechiffrierung gestartet werden; es erscheint ein neues Fenster, das Sie über den Status informiert werden und wo Sie jederzeit die Operation abbrechen können.

Wenn Sie alle Dateien einer Eingabedatei dechiffrieren, überzeugen Sie sich bitte, bevor Sie die Eingabedatei löschen, ob Ihre Daten auch richtig dechiffriert wurden. Das Programm hat keine Möglichkeit, die Richtigkeit eines Passworts festzustellen, es kann auch an Hand der erzeugten Daten dies nicht erkennen. Beachten Sie bitte auch die Warnung im Abschnitt "Dateien chiffrieren".

Dateien vernichten

Sie können entweder eine einzelne Datei oder mehrere Dateien in einem Schritt vernichten. Sollen mehrere Dateien vernichtet werden, so müssen diese vorher im Dialog "Dateien auswählen" markiert werden. Eine gültige Dateiauswahl läßt sich an der Markierung des Statussymbols "Auswahl" erkennen.

In diesem Fall erscheint im Textfeld "Eingabe Datei" das Wort ">> Auswahl Liste <<", bei der Vernichtung einer Einzeldatei deren Dateiname. Danach betätigen Sie den Schalter "Wipe" oder den gleichnamigen Befehl im Menü "Bearbeiten".

Haben Sie mehrere Dateien ausgewählt, erscheint ein neuer Dialog, indem Sie Ihre Auswahl nochmals bestätigen. Nun kann die Operation gestartet werden; es erscheint ein neues Fenster, das Sie über den Status der Vernichtung informiert und wo Sie jederzeit die Operation abbrechen können.
.

Nach Ausführung dieser Funktion sind die ausgewählten Dateien unwiederbringlich verloren. Sein Sie deshalb besonders vorsichtig bei der Auswahl der Dateien.

Benutzer Passwort

In diesem Dialog haben Sie die Möglichkeit, ein festes privates Passwort einzustellen, welches bei der Chiffrierung benutzt werden kann. Dieses Feature ist nur in der registrierten Version verfügbar, weil zum Speichern dieses Passworts die Registrierungsnummer eingegeben werden muß. Sie sollten Ihre Installationsdiskette an einem sicheren Ort aufbewahren, damit niemand an diese Nummer gelangt.

Enigma Setup

- **Dateien nur löschen anstatt vernichten (Wipe) (default: nicht markiert) [(ALT-N)]**
  Die ausgewählten Dateien werden einfach gelöscht. Eine Wiederherstellung ist u.U. möglich.

- **Leere Verzeichnisse entfernen bei Vernichten (Wipe) (default: markiert) [(ALT-L)]**
  Beim Vernichten (Wipe) ganzer Verzeichnisstrukturen werden leere Verzeichnisse gelöscht.

- **Benötigte Verzeichnisse bei Dechiffrierung anlegen (default: markiert) [(ALT-B)]**
  Verzeichnisse werden entsprechend der Archivdateien angelegt. Ist dieser Schalter nicht markiert, werden Dateien, die einen Pfadnamen enthalten ins aktuelle Ausgabeverzeichnis dechiffriert, z.B. "tmp/dir1/datei.txt" wird als Datei "datei.txt" ins Ausgabeverzeichnis dechiffriert.

- **Alle selektierten Dateien ohne weitere Abfrage chiffrieren (default: nicht markiert) [(ALT-A)]**
  Ist dieses Statussymbol markiert, werden alle ausgewählten Dateien ohne weitere Abfrage chiffriert. Ansonsten besteht die Möglichkeit, in einem zusätzlichen Dialog die Auswahl zu verändern.

- **Alle selektierten Dateien ohne weitere Abfrage vernichten (default: nicht markiert) [(ALT-E)]**
  Ist dieses Statussymbol markiert, werden alle ausgewählten Dateien ohne weitere Abfrage vernichtet. Ansonsten besteht die Möglichkeit, in einem zusätzlichen Dialog die Auswahl zu verändern.

- **Netzwerk Laufwerke für temporäre Dateien benutzen (default: nicht markiert) [(ALT-Z)]**
  Ist dieses Statussymbol markiert, so wird versucht, temporäre Dateien auf Netzwerk Laufwerken anzulegen falls der verfügbare Platz auf lokalen Laufwerken nicht ausreicht.

- **Regulärer MSDOS - Ausdruck (default: markiert) [(ALT-R)]**
  Werden die Dateien über einen regulären Ausdruck ausgewählt, so führt die Markierung dieses Kontrollelements dazu, daß bei Angabe von "*.*" auch Dateien ohne Extension wie z.B. "MAKEFILE" , etc. markiert werden. Ist dieser Schalter nicht gesetzt, müßte man wie in UNIX üblich als regulären Ausdruck "*" angeben um solche Dateien zu markieren.

- **Erhöhtes Multitasking (default: markiert) [(ALT-M)]**
  Ist dieses Statussymbol markiert, so wird Windows die Möglichkeit gegeben, 10 mal so oft die interne Messagequeue abzuarbeiten als wie das umgekehrt der Fall wäre.

- **Datei Extension [en2] (default: markiert) [(ALT-D)]**
  Wird bei der Eingabe der Ausgabedatei keine Extension angegeben, so wird die in der Textbox stehende Erweiterung automatisch angehängt. Eine einheitliche Extension ist bei der Wiederauffindung von chiffrierten Dateien recht nützlich.

- **Fragen vor dem Vernichten (default: markiert) [(ALT-V)]**
  Vor dem Löschen (Wipe) einer einzelnen Datei aus dem Hauptmenü wird der Benutzer zur Bestätigung aufgefordert.

- **Fragen vor dem Überschreiben einer Datei (default: markiert) [(ALT-C)]**
  Vor dem Überschreiben einer Datei wird der Benutzter zur Bestätigung aufgefordert.

Änderungen der Einstellungen sind immer nur in der aktuellen Sitzung aktiv. Wenn Sie eine Option permanent ändern wollen, betätigen Sie den Schalter "Save Options" oder die Taste ALT-S.

National **B**ureau of **S**tandards

National **S**ecurity **A**gency

eineindeutige Abbildung einer endlichen Menge auf sich selbst

Einheit des Informationsgehalts einer Nachricht. 1 Bit (binary digit) kennzeichnet eine ja/nein Entscheidung.

Daten**F**ern**Ü**bertragung

Antivalenz (exklusiv ODER), y genau dann 1, wenn x1 identisch x2

Data Encryption Standard (DES)

Im Jahre 1972 fand in den USA eine Ausschreibung statt, in der das Nationale Büro für Standardisierung (NBS) um ein Angebot für ein Programm zum Chiffrieren beliebiger Daten (unclassified computer data) bat. Aufgrund der extrem geringen Reaktion auf diese Ausschreibung wurde im Jahre 1974 die Nationale Sicherheitsbehörde (NSA) zur Mithilfe aufgefordert, die einige Erfahrung in der Entwicklung von einfachen Codierern und Chiffrieralgorithmen hatte. Nach langwierigen Diskussionen erhob das NBS im Jahre 1977 einen von IBM entwickelten Algorithmus zum Standard (DES).

Dieser baut auf dem Prinzip der während des 1. Weltkriegs von dem deutschen Elektroingenieur Arthur Scherbius entwickelten und im 2. Weltkrieg von Deutschland eingesetzten elektromechanischen Chiffriermaschine "Enigma" auf. Wie die Enigma benutzt DES eine Folge von Permutationen, die für sich genommen recht einfach, in Kombination aber höchst kompliziert sind. Bei der Enigma wurden die Permutationen durch mechanische Räder erzeugt, während DES Programmfunktionen oder in einigen Fällen Mikrochips verwendet.

Da der Chiffrierprozeß von einem Computer durchgeführt wird, sind die zu chiffrierenden Symbole nicht Buchstaben (wie bei der Enigma), sondern Bits, also binäre Ziffern. Der DES behandelt jeweils eine Folge von 64 Bits auf einmal. Die zu verschlüsselnde Datei muß also zunächst in eine Sequenz von 64 Bit Folgen zerlegt werden. Die Verschlüsselung einer Datei nach dem DES Verfahren kann man sich als Fluß vorstellen, der sich in höchst komplizierter Weise immer wieder teilt und erneut vereinigt.

DES zerstückelt den 64 Bit Block in einem mehrstufigen Algorithmus und verknüpft ihn mit dem 64 Bit (8 Zeichen) langen Passwort des Benutzers.

Da viele Protokolle der DFÜ nur 7 Bit pro Zeichen übertragen und das 8. Bit als Paritätsbit benutzen, wird das oberste Bit (msb) jedes Passwortzeichens nicht mit diesem Block verknüpft.

Zunächst werden die 64 Bits einer festen internen Eingangspermutation unterworfen und anschließend in zwei 32 Bit Blöcke, in die sogenannte rechte und linke Hälfte geteilt. Der Zerstückelungsprozeß umfaßt 16 Iterationen, die den Zweck haben, die Blöcke bis zur Unkenntlichkeit zu verstümmeln. Die daraus entstandenen chiffrierten 32 Bit Blöcke werden danach durch eine zur ersten Permutationstabelle inversen Tabelle wieder zu einem 64 Bit Block permutiert, dem chiffrierten Block, der dann in die Ausgabedatei geschrieben wird.

In jeder Iteration wird die linke Hälfte über XOR mit der 32 Bit Ausgabe der Funktion ξ verknüpft. Mit Ausnahme der 16. Iteration werden danach beide Hälften vertauscht. Der Funktion ξ wird die rechte Hälfte und die 48 Bit Ausgabe der Funktion ϑ als Argument übergeben. Die rechte Hälfte bezeichnen wir als R. ξ permutiert die 32 Bit von R zu 48 Bit. Die dabei verwendete Permutation ergibt sich aus der XOR Verknüpfung mit der 48 Bit Ausgabe von ϑ. Das 48 Bit Resultat wird jetzt in acht 6 Bit Werte aufgeteilt. Mit Hilfe der Funktion ϕ wird aus jedem 6 Bit Wert ein 4 Bit Wert substituiert. Die acht 4 Bit Werte werden nun zu einem 32 Bit Wert zusammengesetzt., der danach mit einer weiteren Permutationstabelle verknüpft wird. Der aus dieser Permutation entstandene 32 Bit Wert ist die Ausgabe der Funktion ξ. ϕ besteht aus 8 verschiedenen Teilfunktionen $\phi_1,\phi_2,\ldots,\phi_8$, die auf die 6 Bit Werte angewandt werden. Jede Teilfunktion besitzt eine Permutationstabelle. In dieser Tabelle, einer 16x4 Matrix, ist jedem der 64 Matrixelemente ein Wert im Bereich von 0..15 zugeordnet, ein 4 Bit Wert der jeweils einen 6 Bit Wert substituiert. Die Matrix Koordinaten eines 6 Bit Wert ergeben sich auf folgende Weise: Aus Bit 1 und 6 ergibt sich die Spalte 0..3, aus den Bits 2-5 errechnet sich die Zeile 0..15. ϕ gibt den 4 Bit Wert des so adressierten Matrixelements zurück. Der Sinn von ϕ ist, Klartext und Passwort so miteinander zu vermischen, daß schon nach wenigen Iterationsschritten jedes Passwortzeichen von jedem anderen sowie von jedem Klartext-Bit abhängt. Dadurch wird die Häufigkeitsverteilung der Zeichen im Klartext völlig verwischt und jede Häufigkeitsanalyse vereitelt. Die Funktion ϑ gibt einen 48 Bit Wert zurück, der mit Hilfe des Passworts gebildet wird. Argumente von ϑ sind die Nummer der aktuellen Iteration und das Passwort. Für die Permutation des Passworts stehen wiederum zwei interne Tabellen bereit. Bei der ersten Iteration wird

das Passwort mit der ersten permutiert und danach in zwei Hälften geteilt. Jede dieser Hälften wird in Abhängigkeit von der Iterationsnummer ein- (1,2,9,16) bzw. zweimal (3-8,10-15) nach links geshiftet. Eine interne Tabelle steuert den Shiftprozeß. Jede nachfolgende Iteration benutzt den geshifteten Wert der vorhergehenden Iteration als Eingabe, macht ihren eignen Shiftvorgang und permutiert danach den Wert mit der zweiten Permutationstabelle.

Für das Dechiffrieren wird der beschriebene Algorithmus angewandt, wobei die Ausgaben der Funktion ϑ jetzt aber in umgekehrter Reihenfolge zum Einsatz kommen.

Sicherheit des DES

>> *The best that can be expected is that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is finally reached, the information this obtained has lost all its value.* << William F. Friedman

Es läßt sich zeigen, daß bereits nach wenigen Iterationen jedes Bit der chiffrierten Daten von jedem Bit des Klartextes und jedem Bit des Passworts abhängt. Minimale Änderungen des Klartextes oder des Passworts bewirken, daß sich mehr als die Hälfte der Bitpositionen ändern - den sogenannten Lawineneffekt.

Da Häufigkeitsanalysen bei DES nicht zum Erfolg führen, bleibt potentiellen Hackern nur der Weg, durch Probieren das Passwort herauszufinden. Bei einer Passwortlänge von 8 Zeichen, also 64 Bits abzüglich der 8 nicht genutzten höherwertigsten Bits eines jeden Zeichens (Paritätsbit), muß er also 72 Billiarden (2 exp 56) Passwörter durchprobieren.

Mit einem Spezialchip, der in der Lage ist 1.000.000 Passwörter pro Sekunde zu testen, bräuchte er dafür maximal 2284 Jahre. 10000 solcher Chips in einem Parallelcomputer vereinigt, würde diese Aufgabe nach gut 80 Tagen bewältigt haben. Die Überprüfung der Plausibilität des dechiffrierten Textes ist bei dieser Rechnung nicht mit einbezogen. Einzige Schwachstelle von DES sind die Benutzer selbst, die Ihre Passwörter austauschen.

msb - most significant bit

S-ROTOR

S-ROTOR verwendet einen XOR-Substitutionsalgorithmus, was bedeutet, daß jedes gelesene Zeichen mit einem Passwortzeichen über XOR verknüpft in die Ausgabedatei geschrieben wird. Im Gegensatz zu trivialen Algorithmen, werden hier die einzelnen Passwortzeichen nicht der Reihe nach verknüpft, sondern über eine "Zufälligkeitsfunktion" ermittelt, die vom Passwort und der Größe der Datei abhängig ist.

Durch Vorbelegung des Ausgabepuffers mit "Zufallszahlen" wird die "Unordnung" weiter erhöht. Da das Passwort selbst nicht in der Ausgabedatei gespeichert wird, dürfte es selbst bei Kenntnis des Quelltextes von S-ROTOR relativ kompliziert werden, eine verschlüsselte Datei ohne Kenntnis des Passworts zu entschlüsseln.

Man sollte sich deshalb das verwendete Passwort gut einprägen. Wird eine Datei versehentlich mehrfach verschlüsselt, so kann sie in umgekehrter Reihenfolge wieder entschlüsselt werden. Eine doppelte Verschlüsselung mit dem gleichen Passwort ergibt **nicht** die originale Datei.

Passwort Eingabe

Vor der (De)Chiffrierung der ausgewählten Dateien muß an dieser Stelle Ihr persönliches Passwort eingegeben werden. Niemand kann auf die chiffrierten Daten zugreifen, es sei denn er hat Kenntnis von diesem Passwort.

Das Passwort sollte mindestens 5 Zeichen lang sein und kann alle mit der Tastatur eingebbaren Zeichen enthalten, wobei zwischen "großen" und "kleinen" Zeichen, wie z.B.- "A" und "a", unterschieden wird. Das Passwort wird zum Schutz vor unerwünschten Beobachtern beim Eingeben nicht dargestellt. Es muß deshalb zur Sicherheit doppelt eingegeben werden (Felder "Passwort:" und "Bestätigung:").

Die Betätigung des "Make Key" Schalters erlaubt die automatische Generierung eines zufälligen 8 Zeichen langen Passworts. Es wird im Feld Automatisch: dargestellt. Sie sollten sich dieses Passwort unbedingt aufschreiben, bevor sie "OK" betätigen. Wenn Sie den Schalter "Default" anklicken wird Ihr voreingestelltes Benutzerpasswort zur Chiffrierung verwendet.

Lizenz Vereinbarungen

Shareware Version:

Sie erhalten hiermit die Lizenz, die Shareware Version von Enigma für eine Zeit von 60 Tagen zu benutzen. Diese Version dürfen Sie beliebig oft kopieren und weitergeben sowie über elektronische Medien verbreiten. Die Möglichkeit, Daten nach dem sogenannten Data Encryption Standard (DES) zu chiffrieren, wird ausschließlich in der registrierten Version angeboten.

Wenn Sie die Software über die vereinbarte Zeit benutzen wollen, müssen Sie sich bei uns als Lizenznehmer registrieren lassen.

Ihnen ist es ohne unsere ausdrückliche, vorherige schriftliche Zustimmung nicht gestattet, diese Version gegen Gebühr zu vertreiben, Änderungen auf der Diskette, am Diskettenumfang oder an den Programmen vorzunehmen, mit folgenden 2 partiellen Ausnahmen: Eingetragenen Shareware Händlern wird hiermit erlaubt, diese Version ohne unsere Zustimmung gegen eine Gebühr von höchstens 10 DM zu vertreiben. Der Vertrieb auf CDROM bedarf ebenfalls nicht unserer schriftlichen Zustimmung.

Registrierte Version:

Die Benutzung der registrierten Version von Enigma 2.0 folgenden Bedingungen:

- Enigma 2.0 ist urheberrechtlich geschützt.

- Das Programm sowie die dazugehörigen Dateien dürfen weder in Teilen noch im Ganzen kopiert, verändert oder decompiliert werden.

- Der rechtmäßige Erwerb der Programmdiskette erlaubt ausschließlich die Erstellung von Sicherheitskopien für den persönlichen Gebrauch. Entsprechend der Unmöglichkeit, ein Buch zu einem gegebenen Zeitpunkt an verschiedenen Orten zu lesen, darf das Programm nicht gleichzeitig von verschiedenen Personen an verschiedenen Orten und auf verschiedenen Geräten benutzt werden.

Garantie

Diese Software wurde ausgiebig in verschiedenen Systemumgebungen getestet. Trotzdem kann für die fehler- und unterbrechungsfreie Lauffähigkeit dieser Software auf Ihrem Computer keinerlei Garantie übernommen werden. Für die Erreichung eines bestimmten Verwendungszwecks wird ebenfalls keine Garantie übernommen. Der Benutzer trägt das volle Risiko für Schäden die sich aus der Benutzung dieser Software ergeben.

Zusatz Garantie für registrierte Version:

Wir garantieren, daß alles gelieferte Material in einem einwandfreien Zustand ist und ersetzen defekte Lieferungen, falls innerhalb von 10 Tagen nach Erhalt der Lieferung berechtigte Gewährleistungsansprüche geltend gemacht werden.

Die Haftung für unmittelbare Schäden, mittelbare Schäden, Folgeschäden und Drittschäden ist, soweit gesetzlich zulässig ausgeschlossen. Die Haftung bei grober Fahrlässigkeit bleibt hiervon unberührt, in jedem Fall ist jedoch die Haftung beschränkt auf den Kaufpreis.

Standardisierung

Der in diesem Programm verwendete DES-Algorithmus orientiert sich (soweit in einer Software - Implementation möglich) an folgenden Standards:

- FIPS PUB 46-1 - Data Encryption Standard (1988)
  Contains the specification for the Data Encryption Standard (DES) algorithm, which can be implemented hardware to protect sensitive unclassified information.

- FIPS PUB 74 - Guidlines for Implementing and Using the NBS DES (1981)
  Companion to FIPS PUB 46-1. Contains guidance for the use of cryptographic techniques.

- FIPS PUB 81 - DES Modes of Operation (1980)
  Companion to FIPS-PUB 46-1. Contains descriptions of the four modes of operation for the DES: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB).

- ANSI X3.92 - Data Encryption Algorithm (DEA)
- ANSI X3.106 - DEA Modes of Operation

Im Jahre 1986 veröffentlichte ISO den Standard "DEA-1", wo die Benutzung des DES zur Chiffrierung empfohlen wird.

- FIPS - Federal Information Processing Standards
- ANSI X3 - American National Standards Institute (Information Processing)
- ISO - International Standards Organization

Der verwendete Wipe Algorithmus hält sich an den Standard, der in "National Computer Security Center standard, CSC-STD-005-85, Department of Defense Magnetic Remanence Security Guideline, 15 Nov 85, Section 5.3.1. " beschrieben wird.

Registrierung

▪ Enigma für Windows Version 2.0

[Bitte drucken Sie diese Seite aus und schicken oder faxen sie ausgefüllt an unten stehende Adresse]

Vorname: Nachname:

_____

Firma:

_____

Adresse:

_____

Stadt:

_____

Postleitzahl: Telefon:

_____

Telefax: eMail:

_____

Computer Typ:

_____

Von wem haben Sie Enigma erhalten:

_____

_____

Kommentar ?

_____

_____

_____

Anzahl Registrierungen von Enigma:	_____	X	99 DM	_____
Updates auf Enigma 2.0:	_____	X	49 DM	_____
Porto/Verpackung/Versand				
Vorkasse (nur innerhalb Deutschlands)			05 DM	_____
Nachnahme (innerhalb Deutschlands)			09 DM	_____
Nachnahme (europäisches Ausland)			20 DM	_____

Gesamt Betrag DM _____

Ich habe die Lizenz- und Garantie Bedingungen für die Benutzung von Enigma gelesen und erkläre mich damit einverstanden.

Unterschrift: _____

Stefan Wolf Software
GartenStr. 22
D-61449 Steinbach/Ts.
Telefon/FAX: 06171 980483

Betätigen Sie diesen Button um Enigma zu beenden

Textfeld für Namen der Eingabedatei wird. Wird automatisch besetzt von DateiListBox.

Textfeld für Namen der Ausgabedatei.

Textfeld zur Anzeige des aktuellen Verzeichnis.

Listenfenster zur Anzeige der Dateien im aktuellen Verzeichnis

Listenfenster zur Anzeige der Verzeichnisse im aktuellen Verzeichnis und der Laufwerke

Textfenster, indem in Abhängigkeit der Mausposition ein kleiner Hilfstext angezeigt wird

Dieses Statuselement ist markiert, wenn eine gültige Dateiauswahl vorliegt, die mit dem entsprechenden Dialog erzeugt wurde.

Dieses Statuselement ist markiert, wenn die Datei im Textfeld "Eingabe Datei" mit Enigma chiffriert wurde.

Dieses Statuselement ist markiert, wenn die Datei im Textfeld "Eingabe Datei" mit Enigma noch nicht chiffriert wurde. Soll eine bereits chiffrierte Datei nochmals chiffriert werden, muß dieser Schalter vorher mit der Maus angeklickt werden.

Textfeld zur Anzeige der Größe der ausgewählten Eingabedatei.

Textfeld zur Anzeige des Erstellungsdatums der ausgewählten Eingabedatei.

Statuselement zur Auswahl des DES Chiffrier - Algorithmus. Handelt es sich bei der Eingabedatei um eine bereits mit DES chiffrierte Datei wird dieses Element automatisch gesetzt.

Statuselement zur Auswahl des S-ROTOR Chiffrier - Algorithmus. Handelt es sich bei der Eingabedatei um eine bereits mit S-ROTOR chiffrierte Datei wird dieses Element automatisch gesetzt.

Shareware Version

Sie haben mit Enigma für Windows ein Shareware - Programm vor sich. Was ist das eigentlich - SHAREWARE ? Viele Computeranwender meinen, daß es sich dabei um Public-Domain oder kostenlose Programme handelt, was so allerdings nicht zutrifft: Shareware ist ein Vertriebsweg für kommerziell vermarktete Software - das ist alles. Der Vorteil für Sie als Anwender dabei ist: Sie haben die Möglichkeit, das Programm gründlich kennenzulernen, bevor Sie sich für einen Kauf bzw. Registrierung entscheiden. Beim Erwerb kommerzieller Software bezahlen Sie und hoffen, daß alles so funktioniert wie angegeben. Bei Shareware haben Sie die ultimative Geld-Zurück Garantie - Wenn Ihnen das Programm nicht zusagt, bezahlen Sie auch nicht dafür. Hinzu kommt der Verkauf direkt vom Softwarehersteller, was unnötige Kosten spart.

- ## Anwender Registrierung

Sie haben mit Enigma ein Programm vor sich, das als Shareware vertrieben wird. Sie registrieren das Programm durch Eingabe Ihrer Registrierungsnummer im ersten Dialog. Sie finden Sie auf Ihrem Diskettenlabel. Sie können die Shareware Version **60 Tage** benutzen und sich von ihrer Leistungsfähigkeit überzeugen. Nach dieser Zeit sind Sie verpflichtet, sich für 99,00 DM bei uns als Lizenznehmer für die neueste Vollversion registrieren zu lassen oder das Programm von Ihrem Rechner zu entfernen.

Haben Sie sich für die Registrierung entschieden, so drucken Sie das Registrierungs-Formular aus, am besten gleich aus der Hilfe. Schicken Sie uns dieses ausgefüllt zu. Sie erhalten dann umgehend die neueste Vollversion.