Enigma Hilfe Inhalt

Was ist Enigma ?

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.

Viele Angestellte arbeiten täglich mit Daten, die nicht für die Allgemeinheit bestimmt sind, z.B. individuelle oder Firmendaten, Gehalts- oder Personallisten, Patentschriften usw., die sich gewöhnlich erst dann "in Sicherheit" befinden, wenn sie hinter einem traditionellen Schloß eingeschlossen sind.

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

Ein Verfahren, das den oben genannten Bereichen gerecht wird, ist das Chiffrieren oder Verschlüsseln seiner Daten mit einem geheimen Passwort.

Die Sicherheit derart verschlüsselter Daten gegenüber potentiellen Eindringlingen (Hackern) 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 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.

Die Funktion eines elektronischen Aktenvernichters wurde in das Programm aufgenommen, weil viele Computerbenutzer nicht wissen , daß mit dem MSDOS Befehl **DEL** gelöschte Dateien ohne größeren Aufwand in den meisten Fällen wiederhergestellt werden können. Die Funktion WIPE löscht die ausgewählte Datei physisch und macht so eine Wiederherstellung unmöglich.

Verschlüsselungssytem mit öffentlichen Schlüssel, benannt nach den Entwicklern Ronald Rivest, Adi Shamir und Leonard Adleman

Enigma für Windows 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, das 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:\enigma\enigma.exe

3 Wählen Sie "OK".

So starten Sie Enigma von der DOS-Eingabeaufforderung aus

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

Hinweis:
Erscheint eine Meldung, die angibt, daß die Datei enigma nicht gefunden werden konnte, so ist das Verzeichnis, das enigma enthält, nicht in Ihrem Pfad. Wechseln Sie zu dem Verzeichnis, das Ihre enigma.exe-Datei 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 enigma.exe gespeichert ist und das Eingeben von enigma.

Datei Menü

Chiffrieren...

Chiffrieren der im Hauptfenster ausgewählten Datei.Es wird ein Fenster geöffnet, indem das geheime Passwort eingegeben werden muß.

DeChiffrieren...

Dechiffrieren der im Hauptfenster ausgewählten Datei. Es wird ein Fenster geöffnet, indem das geheime Passwort eingegeben werden muß.

Wipe...

Vernichten der im Hauptfenster ausgewählten Datei. In Abhängigkeit von den aktuellen Enigma Einstellungen wird der Benutzer zur Bestätigung aufgefordert.
VORSICHT :
Nach Ausführung dieser Funktion ist die Datei unwiederbringlich verloren.

Beenden

Enigma für Windows beenden.

Optionen Menü

Setup...

Öffnet das Setup Fenster, indem verschiedene Einstellungen von Enigma verändert werden können.

Registrierung..

Öffnet ein Fenster, indem das Passwort zur Registrierung von Enigma eingegeben werden kann .
Der DES Algorithmus ist ausschließlich in der registrierten Version von Enigma für Windows verfügbar.

Hilfe Menü

Inhalt
Öffnet das Hilfe Inhaltsverzeichnis für Enigma für Windows

Chiffrieren...
Anzeigen des Hilfethema Datei chiffrieren

Dechiffrieren..
Anzeigen des Hilfethema Datei dechiffrieren

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.

Haupt-Fenster

Jeder einzelne Menüpunkt von Enigma kann innerhalb des Hautfensters komfortabel durch das Anklicken eines Knopfes (Buttons) aufgerufen werden.

Chiffrieren der ausgewählten Datei. Siehe auch Thema Datei chiffrieren.

Dechiffrieren der ausgewählten Datei. Siehe auch Thema Dateidechiffrieren.

Wechseln der Enigma Einstellungen. Siehe auch Thema Enigma-Setup.

Vernichten der ausgewählten Datei. Siehe auch Thema Datei vernichten.

Hilfethemen für Enigma für Windows anzeigen.

Enigma für Windows beenden.

Datei chiffrieren

Eine Datei läßt sich durch einfaches Anklicken des dargestellten Buttons oder durch Auswahl des Menüpunktes **Datei/Chiffrieren...** chiffrieren. Es erscheint ein Fenster, indem das zur Chiffrierung verwendete Passwort eingegeben werden muß. Zunächst muß im Textfeld **Eingabe Datei:** der Name einer existierenden Datei eingegeben werden. Dies kann man entweder manuell oder durch das Anklicken der entsprechenden Datei im Datei-Listenfenster tun. Wird nach zuletzt genannter Methode verfahren,was empfohlen wird, so werden im rechten Teil des Hauptfensters Informationen über den Status der Datei angezeigt. Das Textfeld **Ausgabe Datei:** wird automatisch mit der Eingabedatei besetzt. Soll die Originaldatei im nichtchiffrierten Zustand erhalten bleiben, so muß dort manuell ein alternativer Dateinamen eingetragen werden. Die Kontrollelemente **Chiffriert** und **Nicht Chiffriert** oben rechts zeigen an, ob die ausgewählte Datei eventuell mit Enigma schon chiffriert wurde. In diesem Fall wird der Button zum Chiffrieren der Datei automatisch grau dargestellt. Soll die Datei dennoch noch einmal chiffriert werden, muß das Kontrollelement **Nicht Chiffriert** manuell gesetzt werden.
Im Algorithmus- Fenster unten rechts, kann der Algorithmus ausgewählt werden, der zum Chiffrieren der Datei verwendet werden soll. Standardmäßig ist das Kontrollelement für den S-Rotor- Algorithmus gesetzt. DES ist nur in der registrierten Version von Enigma für Windows verwendbar.

Ist die ausgewählte Datei schon chiffriert, so wird mit diesen Kontrollelementen der benutzte Chiffrieralgorithmus angezeigt.

Datei dechiffrieren

Eine Datei läßt sich durch einfaches Anklicken des dargestellten Buttons oder durch Auswahl des Menüpunktes **Datei/DeChiffrieren...** dechiffrieren. Es erscheint ein Fenster, indem das zur Dechiffrierung verwendete Passwort eingegeben werden muß.
Zunächst muß im Textfeld **Eingabe Datei:** der Name einer existierenden Datei eingegeben werden. Dies kann man entweder manuell oder durch das Anklicken der entsprechenden Datei im Datei-Listenfenster tun. Wird nach zuletzt genannter Methode verfahren,was empfohlen wird, so werden im rechten Teil des Hauptfensters Informationen über den Status der Datei angezeigt. Das Textfeld **Ausgabe Datei:** wird automatisch mit der Eingabedatei besetzt. Soll die Originaldatei im chiffrierten Zustand erhalten bleiben, so muß dort manuell ein anderer Dateinamen eingetragen werden. Die Kontrollelemente **Chiffriert** und **Nicht Chiffriert** oben rechts zeigen an, ob die ausgewählte Datei mit Enigma chiffriert wurde. Ist dies nicht der Fall wird der Button zum Dechiffrieren der Datei automatisch grau dargestellt.
Ist die ausgewählte Datei chiffriert, so wird im Algorithmus- Fenster unten rechts der Algorithmus angezeigt, der zum Chiffrieren der Datei verwendet wurde und mit dem die Datei dechiffriert werden muß. DES ist nur in der registrierten Version von Enigma für Windows verfügbar.

Datei vernichten

Eine Datei läßt sich durch einfaches Anklicken des dargestellten Buttons oder durch Auswahl des Menüpunktes **Datei/Wipe...** vernichten. Zunächst muß dasTextfeld **Eingabe Datei:** mit dem Namen einer existierenden Datei besetzt werden, was man am einfachsten durch das Anklicken der Datei im Datei-Listenfenster tut. Standardmäßig muß die Operation zum Vernichten einer Datei bestätigt werden.

VORSICHT :
Nach Ausführung dieser Funktion ist die Datei unwiederbringlich verloren.

Enigma Setup

Durch Anklicken dieses Buttons können derzeit folgende Enigma- Einstellungen verändert werden:

Fragen vor dem Vernichten einer Datei
Ist dieses Kontrollelement markiert, wird der Benutzer vor dem Vernichten der ausgewählten Datei zur Bestätigung aufgefordert.

Fragen vor dem Überschreiben einer Datei
Ist dieses Kontrollelement markiert, wird der Benutzer vor dem Überschreiben einer Datei zur Bestätigung aufgefordert. Dieser Fall tritt auf, wenn Ein- und Ausgabedatei beim Chiffrierprozeß den gleichen Namen besitzen.

Vor dem Chiffrieren Datei komprimieren
Ist dieses Kontrollelement markiert, wird die zu chiffrierende Datei komprimiert.

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

DES (Data Encryption Standard)

Im Jahre 1972 fand in den USA eine Ausschreibung statt, in der das Nationale Büro für Standardtisierung (NBS) um ein Angebot für ein Programm zum Chiffrieren beliebiger Daten 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 im 2. Weltkrieg von zunächst von Polen und dann von Deutschland entwickelten und verwendeten 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 Microchips 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 nach einer internen Permutationstabelle neu angeordnet und 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 völig verwischt und jede Häufigkeitsanalyse vereitelt.Die Funktion ϑ nun 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 vorhergenden Iteration als Eingabe, macht ihren eignen Shiftvorgang und permutiert danach den Wert mit der zweiten Permutationstabelle.

Bei der Dechiffrierung wird der beschriebene Prozeß in umgekehrter Reihenfolge durchlaufen.

Sicherheit

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 1000000 Passwörter pro Sekunde durchzutesten vermöchte, bräuchte er dafür maximal 2284 Jahre. 10000 solcher Chips in einem Parallelcomputer vereingt, würde diese Aufgabe nach gut 80 Tagen bewältigt haben. Einzige Schwachstelle von DES ist der Austausch der Passwörter zwischen den Benutzern.

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 von der Länge des Passworts abhängig ist. Durch Vorbelegung des Ausgabebuffers 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.

Die Komplexität des verwendeten Algorithmus ist linear.

Stefan **W**olf **S**oftware

Passwort Eingabe

Beim Chiffrieren bzw. Dechiffrieren der ausgewählten Datei muß an dieser Stelle das Passwort eingegeben werden. Das Passwort wird zum Schutz vor unerwünschten Beobachtern beim Eingeben nicht dargestellt. Es muß deshalb zur Sicherheit doppelt eingegeben werden (Felder **Passwort:** und **Bestätigung:**).

Beim Chiffrierprozeß kann man ein zufälliges Passwort automatisch durch das Anklicken des dargestellten Buttons generieren. Das so generierte Passwort wird im Feld **Automatisch:** dargestellt. Sie sollten sich dieses Passwort irgendwo aufschreiben bevor Sie "OK" betätigen.

Lizenz Vereinbarungen

Die Benutzung der **Vollversion** von Enigma für Windows unterliegt folgenden Bedingungen:

1.)
Enigma für Windows ist urheberrechtlich geschützt.

2.)
Das Programm darf ohne vorherige schriftliche Zustimmung von SWS weder in Teilen noch im Ganzen kopiert, verändert oder decompiliert werden.

3.)
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

SWS **garantiert**, daß alles gelieferte Material in einem guten Zustand ist und ersetzt defekte Lieferungen, falls innerhalb von 10 Tagen nach Erhalt der Lieferung berechtigte Gewährleistungsansprüche geltend gemacht werden.

SWS übernimmt **keine Gewähr** dafür, daß die Software unterbrechungs- und fehlerfrei auf Ihrem Computer läuft. Für die Erreichung eines bestimmten Verwendungszwecks wird ebenfalls keine Gewähr übernommen. 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.

Alle Fragen hinsichtlich Registrierung, technischen Support, Rabatt- und Händlerpreise usw. sind zu richten an:

Stefan Wolf Software
Bremer Str. 17-33, Appt. 7/4
D- 6236 Eschborn/Ts.
Tel./FAX.: +49 (0)6196 483093
CompuServe: 100111,140

Registrierung

Enigma für Windows Version 1.1

[Bitte drucken Sie diese Seite aus und schicken sie ausgefüllt mit entsprechenden Verechnungsscheck an unten stehende Adresse]

Vorname: Nachname:

Firma:

Addresse:

Stadt:

Postleitzahl: Land:

Telefon:

Computer Typ:

Von wem haben Sie Enigma erhalten:

Kommentar ?

Anzahl der Registierung von Enigma :_____ X 99 DM

Ich erkläre, die Lizenz- und Garantie Bedingungen für die Benutzung von Enigma für Windows gelesen zu haben und erkläre mich damit einverstanden.

Unterschrift:

Überweisung an **Stefan Wolf Softtware**
Bremer Str. 17-33, Appt. 7/4
D- 6236 Eschborn/Ts.