



Krypter V. 3.0

Copyright 1998 - 2010 by BAXBEX Software

BAXBEX im Internet: <http://www.baxbex.com>

# Inhaltsverzeichnis

<b>Teil I</b>	<b>Einführung</b>	<b>3</b>
1	Einleitung .....	3
2	Die wichtigsten Features auf einem Blick .....	3
3	Schnelleinstieg .....	4
4	Kommandozeilen-Optionen .....	5
5	Deinstallation, Software-Aktualisierung .....	6
6	Über dieses Handbuch .....	7
7	Installation .....	8
<b>Teil II</b>	<b>Arbeiten mit Krypter</b>	<b>10</b>
1	Dateien/Verzeichnisse verschlüsseln .....	10
2	Dateien/Verzeichnisse sicher vernichten .....	10
3	Selbstentschlüsselnde (Exe-) Dateien erstellen .....	11
4	Der Verschlüsselungs-Dialog .....	13
	Register: Passwort .....	13
	Register: Ausgabe .....	13
	Register: Erweitert .....	14
5	Krypter-Optionen .....	14
	Krypter-Optionen .....	14
	Protokolle .....	15
	Optionen I .....	15
	Optionen II .....	16
	Optionen III .....	16
	EMail-Optionen .....	17
<b>Teil III</b>	<b>E-Mail - Verschlüsselung</b>	<b>18</b>
1	E-Mail - Verschlüsselung .....	18
2	Einträge im Kontextmenü .....	19
3	SMTP - Client / E-Mail - Editor .....	19
4	Plug-In für Microsoft Outlook .....	20
5	Bild-für-Bild Anleitungen .....	21
<b>Teil IV</b>	<b>Bonus-Funktionen</b>	<b>21</b>
1	Krypter Bonus Funktionen .....	21
2	Exe-Dateien durch ein Passwort schützen .....	22
3	Komplette Laufwerke verstecken .....	22
4	Lokales Kryptometer .....	22
5	Verzeichnis tarnen .....	23

---

<b>Teil V Häufig gestellte Fragen (FAQ)</b>	<b>23</b>
1 FAQ .....	23
2 Algorithmen & Co .....	26
Verschlüsselungs-Algorithmen .....	26
Verschlüsselungs-Reihenfolgen .....	27
<b>Teil VI Tipps &amp; Tricks</b>	<b>28</b>
1 Tipps & Tricks .....	28
<b>Teil VII Bestellung &amp; Support</b>	<b>29</b>
1 Krypter registrieren/bestellen .....	29
2 Kontakt zu BAxBEx Software .....	30
3 Über Fehler berichten .....	31
4 BAxBEx Software Newsletter .....	32
<b>Teil VIII Über Krypter</b>	<b>32</b>
1 Copyright .....	32
2 Lizenzvereinbarung .....	33
3 Garantie und Haftung .....	34
4 Danksagung .....	34

# 1 Einführung

## 1.1 Einleitung



### ... das Programm zum Schutz Ihrer vertraulichen Dateien ...

**Krypter** ist ein einfach zu bedienendes Programm, mit dem Sie Ihre persönlichen Dokumente, E-Mails und Ihre vertraulichen Dateien schnell, einfach und sicher verschlüsseln können. Neben den Verschlüsselungsfunktionen bietet Krypter auch weitere Windows-Sicherheits-Funktionen, sowie die Möglichkeit, beliebige Dateien in eine verschlüsselte Exe-Datei umzuwandeln, die jedermann durch Eingabe des richtigen Passwortes entschlüsseln kann - unabhängig davon, ob Krypter installiert ist oder nicht.

Auch das sichere, unwiderrufliche Vernichten von Daten (*Wiping*) ist mit Krypter möglich.

#### **Bild-für-Bild-Anleitungen:**

Umfangreiche Online-Tutorials zur Krypter Verwendung, finden Sie auf unseren Webseiten unter <http://demos.baxbex.de>

- 
- >> [Features auf einen Blick](#)
  - >> [Schnelleinstieg](#)
  - >> [Dateien/Verzeichnisse verschlüsseln](#)
  - >> [E-Mail - Verschlüsselung](#)

## 1.2 Die wichtigsten Features auf einem Blick

Die wichtigsten **Krypter** Features und Funktionen auf einen Blick:

- leistungsstarke, ungebrochene [Verschlüsselungs-Algorithmen](#) (AES, Twofish, Mars, Cast 256, Blowfish, Gost, SCOP)
- Unterstützt den EMail-Versand verschlüsselter Dateien via **MAPI** oder per [SMTP](#)
- Komfortable Windows-Integration über das **Kontextmenü**
- Add-In für Microsoft Outlook
- Verschlüsselung kompletter Verzeichnisse samt Unterverzeichnissen
- Erstellung selbstentschlüsselnder Dateien
- Sichere, unwiderrufliche Vernichtung von Daten (auf Wunsch gemäß NTSC-TG-025 Richtlinien)
- Automatische Komprimierung der Daten
- Automatische Passwortbestätigung

- Verstecken von Laufwerken
- Einzelne Exe-Dateien durch ein Passwort schützen (keine Verschlüsselung notwendig)
- Leichte und intuitiv zu bedienende Oberfläche
- Verschleierung von Dateinamen
- Verschlüsselung beliebig vieler Dateien und Ordner
- Erstellung von Containerfiles (fasst mehrer Dateien/Verzeichnisse in eine einzelne verschlüsselte Datei zusammen)
- Optional: Individuelle Krypter SFX-Dateien
- Unterstützt Kommandozeilen-Optionen

## 1.3 Schnelleinstieg

### **Bild-für-Bild-Anleitungen:**

Umfangreiche Online-Tutorials zur Krypter Verwendung, finden Sie auf unseren Webseiten unter <http://demos.baxbex.de>

### **Dateien/Verzeichnisse verschlüsseln**

1. Starten Sie den Windows-Explorer.
2. Markieren Sie die Datei, indem Sie sie einmal mit der linken Maustaste anklicken.
3. Klicken Sie die Datei mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag 'Krypter/*Verschlüsseln*'.
4. Geben Sie ein Passwort ein und bestätigen Sie dieses.
5. Klicken Sie auf die 'OK' Schaltfläche.

» [Weitere Hinweise zur Verschlüsselung](#)

### **Dateien/Verzeichnisse entschlüsseln**

1. Starten Sie den Windows-Explorer.
2. Markieren Sie die verschlüsselte Datei, indem Sie sie einmal mit der linken Maustaste anklicken.
3. Klicken Sie die Datei mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag 'Krypter/*Entschlüsseln*'.
4. Geben Sie das Passwort ein.
5. Klicken Sie auf die 'OK' Schaltfläche.

» [Weitere Hinweise zur Verschlüsselung](#)

### **Krypter durch ein Passwort schützen**

1. Starten Sie Krypter (z.B. über das Startmenü).
2. Wechseln Sie in das Register '*Optionen II*'.
3. Bestätigen Sie die Option '*Krypter durch ein Passwort schützen*' und wählen Sie ein Passwort.

### Eine selbstentschlüsselnde Exe-Datei erstellen

1. Starten Sie den Windows-Explorer.
2. Markieren Sie die zu verschlüsselnde Datei, indem Sie sie einmal mit der linken Maustaste anklicken.
3. Klicken Sie die Datei mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter/Verschlüsseln*'.
4. Geben Sie ein Passwort ein und bestätigen Sie diese durch erneute Eingabe (→ **Automatische Passwortbestätigung**).
5. Wechseln Sie ins Register '*Ausgabe*'.
6. Bestätigen Sie die Option '*Exe-Datei erstellen*'.
7. Klicken Sie auf die 'Ok' Schaltfläche.
8. Bestätigen Sie den vorgeschlagenen Name für die Exe-Datei oder wählen Sie einen beliebigen anderen Namen aus.

### Eine beliebige Exe-Dateien vor der Ausführung durch ein Passwort schützen

1. Starten Sie Krypter (z.B. über das Startmenü).
2. Wechseln Sie in das Register '*Bonus*'.
3. In der Gruppe 'Programmausführung' klicken Sie auf die Schaltfläche '*Hinzufügen*'.
4. Wählen Sie nun die zu schützende Exe-Datei aus.
5. Bestätigen Sie dann die Option '*Passwortschutz aktivieren*' und geben ein Passwort an.

### Mehrere Dateien/Verzeichnisse in einem Schritt verschlüsseln

1. Starten Sie den Windows-Explorer.
2. Markieren Sie alle Dateien und Verzeichnisse, so dass alle zu verschlüsselnden Dateien blau hinterlegt sind.
3. Klicken Sie eine der Dateien (bzw. der Verzeichnisse) mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter/Verschlüsselung*'.
4. Geben Sie ein Passwort ein und bestätigen Sie dieses.

#### **Optional:**

Möchten Sie alle Dateien in einer verschlüsselten Container-Datei zusammenfassen, wechseln Sie ins Register '*Ausgabe*' und bestätigen Sie dort die Option '*Einzelne Ausgabedatei*'.

5. Klicken Sie auf die 'OK' Schaltfläche.

## 1.4 Kommandozeilen-Optionen

Mit Kommandozeilen-Optionen können Sie **Krypter** mit speziellen Parametern starten. Dadurch können Sie einige Arbeitsvorgänge bei Bedarf automatisieren.

#### **Parameter-Schema:**

Krypter.exe {Aktions-Parameter} {Input-Parameter} {Options-Parameter}

#### **Liste der unterstützten Parameter:**

##### **Aktions-Parameter**

/encrypt	- Initialisiert eine Verschlüsselung
/decrypt	- Initialisiert eine Entschlüsselung
/wipe	- Initialisiert eine (Datei-)-Vernichtung
/createmail	- Initialisiert den Krypter-Mailer (SMTP)

### **Input-Parameter**

/file=dateiname	- Relevante Datei\Verzeichnis
/filelist=dateiname	- Datei-/Verzeichnisliste in einer Ascii-Datei
/pwd=passwort	- das zu verwendende Passwort
/cipher=(0,1,2,3,4,5,6)	- <a href="#">Verschlüsselungsverfahren</a> / Algorithmus
/ciphermode=(0,1,2,3)	- <a href="#">Ciphermodus</a> / Reihenfolge
/wmode=(0,1,2,3)	- Vernichtungsmethode
/keyfilename=dateiname	- Schlüsseldatei verwenden

### **Options-Parameter**

/compress	- Daten komprimieren
/createexe	- selbstentschlüsselnde Exe-Datei erstellen
/email	- Ausgabedatei(en) per EMail versenden
/disguise	- Originaldateinamen verschleiern
/delete	- Originaldateien löschen
/singleoutput	- Dateien in einer Containerdatei zusammenfassen
/outputfilename=filename	- Name der Ausgabe-Datei
/template=ExeFileName	- Eine SFX-Vorlage verwenden (z.B. Sprachauswahl)
/overwrite=1	- Zieldatei(en) automatisch überschreiben

### **Anmerkung:**

Vor allen Parametern muss unbedingt das Zeichen "/" angegeben werden!

Falsch wäre:

Krypter.exe **encrypt** /file=c:\Eigene Dateien\wichtig.doc /pwd=geheim

Richtig wäre z.B.:

Krypter.exe **/encrypt** /file=c:\Eigene Dateien\wichtig.doc /pwd=geheim

---

Die Software kann auch als **Engine** verwendet werden, sodass zur Ver- und Entschlüsselung via Kommandozeile keine Krypter Installation erforderlich ist. [Kontaktieren](#) Sie uns bitte, um weitere Informationen zu diesem Thema zu erhalten.

## **1.5 Deinstallation, Software-Aktualisierung**

### **Deinstallation**

Öffnen Sie die Systemsteuerung über das Startmenü -> Einstellungen -> Systemsteuerung. Klicken Sie auf '*Software*' und wählen aus der Liste der installierten

Programme 'Krypter'. Anschließend klicken Sie auf die Schaltfläche 'Hinzufügen/Entfernen'.

### Software-Aktualisierung

Bitte besuchen Sie unsere Webseite unter <http://www.baxbex.de> und schauen Sie dort auf den Seiten zu Krypter nach Update-Hinweisen.

» [BAXBEx Software Newsletter](#)

## 1.6 Über dieses Handbuch

Dieses Handbuch beschreibt den Umgang und die Bedienung von **Krypter**. Dabei werden grundlegende Windows-Kenntnisse vorausgesetzt.

Beschreibung und Grafiken in diesem Handbuch orientieren sich an dem Betriebssystem Windows XP. Eventuell kann es dadurch zu geringfügigen Abweichungen zu Ihrer Windows-Oberfläche kommen. Sie haben dadurch jedoch keinerlei Einschränkungen in Bezug auf die Leistungsfähigkeit und den Programmumfang zu befürchten.

Das Handbuch soll Ihnen helfen, die wichtigsten Programm-Funktionen schnell und einfach zu nutzen. Weitere, detaillierte Informationen finden Sie auch in der Online-Hilfe des Programms. Sie rufen diese Hilfe auf, indem Sie entweder

- **Start > Programme > Krypter > Krypter Hilfe** wählen. Sie erhalten dann das Gesamt-Inhaltsverzeichnis der Hilfe, oder
- bei den jeweiligen Dialogen auf die Schaltfläche **Hilfe** klicken. Hier erhalten Sie dann kontext bezogene Informationen angezeigt.

---

» [Features auf einen Blick](#)

» [Schnelleinstieg](#)

» [Dateien/Verzeichnisse verschlüsseln](#)

» [E-Mail - Verschlüsselung](#)

## 1.7 Installation

1. Legen Sie die Programm-CD in das CD ROM Laufwerk Ihres Computers. Danach wird das Installationsprogramm automatisch gestartet.

---

Hinweise: Sollte bei Ihnen das Installationsprogramm nicht automatisch starten, ist die AutoPlay-Funktion von Windows deaktiviert. Öffnen Sie dann über **Start > Ausführen** den Dialog **Ausführen** und geben Sie im Feld **Öffnen** den Befehl „x:\start.exe“ ein. Dabei steht x für den Laufwerksbuchstaben Ihres CD-ROM Laufwerks.

Liegt Ihnen die CD-ROM nicht vor, zum Beispiel da das Produkt online erworben und geliefert wurde, führen Sie die Installationsdaten **k2010r.exe** aus. (Sofern Sie eine Testversion verwenden, lautet der Name der Installationsdatei **kryp2010.exe**.)

---

2. Sie erhalten als erstes eine Seite mit allgemeinen Infos sowie einen Link auf die BAXBEx-Homepage angezeigt. Klicken Sie auf **Weiter**.
3. Wenn Sie mit den angezeigten Lizenz-Bedingungen einverstanden sind, markieren Sie die entsprechende Option und klicken auf **Weiter**.



4. Möchten Sie ein anderes als das angezeigte Zielverzeichnis wählen, klicken Sie auf die Schaltfläche mit dem Ordner-Symbol und bestimmen ein anderes Zielverzeichnis. Ansonsten können Sie direkt auf **Weiter** klicken.
5. Auf der nächste Seite wird der Ablageort des Programms im Windows-Startmenü angezeigt. Dabei kann die angezeigte Struktur im Feld **Programmgruppe** normalerweise ohne Bedenken übernommen werden. Betätigen Sie erneut **Weiter**.
6. Die nächste Seite zeigt die von Ihnen gewählten oder übernommenen Einstellungen in Bezug auf Zielverzeichnis und Programmgruppe an. Wenn die Einstellungen in Ordnung sind, klicken Sie auf **Weiter**.
7. Das Programm wird nun installiert. Ein Fortschrittsbalken informiert Sie dabei über den Fortgang der Installation. Nach erfolgreichem Abschluss werden Sie aufgefordert Ihre Registrierungsdaten einzutragen. Bitte tragen Sie den Namen des Lizenznehmers und den Registrierungscode in den entsprechenden Feldern ein. Beachten Sie, das der vollständige Name des Lizenznehmers unbedingt eingeben

werden muss - es genügt nicht, den eventuell vorgeschlagenen Windows-Benutzername zu übernehmen. Wenden Sie sich an die IT Abteilung Ihrer Firma, wenn Ihnen die notwendigen Registrierungsdaten nicht vorliegen. Die Software kann auch zu einem späteren Zeitpunkt, nach Abschluss der Installation, eingegeben werden.

Abschließend wird folgende Meldung angezeigt:



8. Möchten Sie nach Abschluss der Installation die Online-Hilfe betrachten, lassen Sie die Option Readme jetzt anzeigen markiert. Klicken Sie auf **Fertig stellen**. Die Installation ist damit abgeschlossen.

---

>> [Deinstallation, Software-Aktualisierung](#)

## 2 Arbeiten mit Krypter

### 2.1 Dateien/Verzeichnisse verschlüsseln

**Krypter** fügt sich nahtlos in die Windows-Oberfläche ein. Durch einen Eintrag im Windows-Kontextmenü haben Sie die Möglichkeit Dateien (und auch komplette Verzeichnisse) schnell und einfach direkt im Windows-Explorer zu verschlüsseln.



#### So verschlüsseln Sie eine Datei:

1. Starten Sie den Windows-Explorer.
2. Markieren Sie die Datei, indem Sie sie einmal mit der linken Maustaste anklicken.
3. Klicken Sie die Datei dann mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter|Verschlüsseln*'.
4. Geben Sie ein Passwort ein und bestätigen Sie es durch erneute Eingabe.
5. Klicken Sie auf die 'OK' Schaltfläche.

#### So verschlüsseln Sie ein Verzeichnis

1. Starten Sie den Windows-Explorer.
2. Markieren Sie das zu verschlüsselnde Verzeichnis, indem Sie es einmal mit der linken Maustaste anklicken.
3. Klicken Sie das Verzeichnis dann mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter|Verschlüsseln*'.
4. Geben Sie ein Passwort ein und bestätigen Sie es durch erneute Eingabe.
5. Klicken Sie auf die 'OK' Schaltfläche.

#### Bild-für-Bild-Anleitungen:

Ein umfangreiches Online-Tutorial zur Krypter Verschlüsselung, finden Sie auf unseren Webseiten unter <http://demos.baxbex.de>

- >> [Register:Passwort](#)
- >> [Register:Ausgabe](#)
- >> [Register: Erweitert](#)

### 2.2 Dateien/Verzeichnisse sicher vernichten

Mit **Krypter** können Sie Daten sicher und unwiderruflich vernichten. Sobald eine Datei vernichtet wurde (von der Option 'Nur Löschen' abgesehen), ist der originale Inhalt der Dateien für immer verloren und kann selbst mit speziellen 'Undelete-Utilities' nicht wieder hergestellt werden.

#### So vernichten Sie eine Datei:

1. Starten Sie den Windows-Explorer.
2. Markieren Sie die Datei, indem Sie sie einmal mit der linken Maustaste anklicken.
3. Klicken Sie die Datei dann mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter|Vernichten*'.
4. Wählen Sie nun die **Vernichtungsmethoden**.
5. Klicken Sie auf die 'OK' Schaltfläche.

#### **So vernichten Sie ein Verzeichnis:**

1. Starten Sie den Windows-Explorer.
2. Markieren Sie das zu verschlüsselnde Verzeichnis, indem Sie es einmal mit der linken Maustaste anklicken.
3. Klicken Sie das Verzeichnis dann mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter/Vernichten*'.
4. Wählen Sie nun die **Vernichtungsmethoden**.
5. Klicken Sie auf die 'OK' Schaltfläche.

Möchten Sie mehrere Dateien/Verzeichnisse in einem Schritt vernichten, markieren Sie diese einfach im Windows-Explorer und fahren dann fort wie oben beschrieben.

#### **Achtung: Seien Sie vorsichtig bei der unwiederruflichen Vernichtung von Daten bzw. Informationen!**

---

#### **Vernichtungsmethoden**

##### **Nur löschen**

Dateien werden nur gelöscht, jedoch nicht überschrieben. Dadurch, daß die Originalinhalte auf der Platte für eine ungewisse Zeit erhalten bleiben, wird diese Methode nicht empfohlen.

##### **Einfach**

Dateien werden einmal mit Zufallsdaten überschrieben.  
Nützlich zur schnellen Vernichtung großer Datenmengen.

##### **DoD-Methode**

Die originalen Daten werden durch dreifaches Überschreiben nach den Bestimmungen NTSC-TG-025 (Version 2, Sept. 1991) des US-amerikanischen Verteidigungsministeriums vernichtet. Dies ist die empfohlene Methode.

##### **SFS-Methode**

Hier werden Daten 35 Mal mit speziellen Mustern überschrieben, um alle Informationen auf jedem denkbar möglichen magnetischen Datenträger zu entfernen. Die SFS Vernichtung wurde von Peter C. Gutmann entwickelt. Bitte beachten Sie, daß das Vernichten von Dateien mit dieser Methode sehr viel Zeit in Anspruch nimmt, selbst auf schnellen SCSI-Laufwerken. Empfohlen für die absolute Sicherheit.

##### **Hinweis:**

Bitte beachten Sie, daß Vernichten auf Netzlaufwerken unter Umständen nicht zu den gleichen Ergebnissen führt wie auf lokalen Laufwerken.

## **2.3 Selbstentschlüsselnde (Exe-) Dateien erstellen**

Diese Funktion gibt Ihnen die Möglichkeit, Ihre sensiblen Daten anderen Personen einfach zugänglich zu machen.

**Vorteile:**

Selbstentschlüsselnde Exe-Dateien sind auf jedem Windows System lauffähig (nicht Windows 3.xx). Zur Entschlüsselung auf dem Zielrechner ist es nicht erforderlich, das Krypter installiert ist. Der Empfänger führt die Exe-Datei einfach aus, gibt das Passwort ein - und schon werden die Daten dekodiert.

**So erstellen Sie eine selbstentschlüsselnde Exe-Datei:**

1. Starten Sie den Windows-Explorer.
2. Markieren Sie die zu verschlüsselnde Datei, indem Sie sie einmal mit der linken Maustaste anklicken.
3. Klicken Sie die Datei mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter/Verschlüsseln*'.
4. Geben Sie ein Passwort ein und bestätigen Sie diese durch erneute Eingabe (→ **Automatische Passwortbestätigung**).
5. Wechseln Sie ins Register '*Ausgabe*'.
6. Bestätigen Sie die Option '*Exe-Datei erstellen*'.
7. Klicken Sie auf die 'Ok' Schaltfläche.
8. Bestätigen Sie den vorgeschlagenen Namen für die Exe-Datei oder wählen Sie einen beliebigen anderen Namen aus.

**Exe-Vorlagen:**

Auf unserer Website können Sie Exe-Vorlagen downloaden, die es Ihnen ermöglichen, selbstentschlüsselnde Exe-Dateien in anderen Sprachen zu erstellen. Derzeit bitten wir Ihnen kostenlose Vorlagen für folgende Sprachen:

- Englisch
- Spanisch
- Italienisch
- Französisch
- Portugiesisch
- Schwedisch
- Niederländisch

**Individuelle Exe-Vorlagen - Unser Service für Firmenkunden!**

*Cooperate Identity!*

Wir erstellen Ihnen gern persönliche Vorlagen für selbstentschlüsselnde Krypter Exe-Dateien.

Ganz nach Ihren Wünschen erstellen wir Ihnen eine Vorlage für selbstentschlüsselnde Krypter- Exe-Dateien. Jede Exe-Datei, die Sie dann mit Krypter erstellen, wird das Erscheinungsbild dieser Vorlage übernehmen.

Beispiele und Informationen zu individuellen Exe-Dateien finden Sie auf unserer Website unter <http://www.baxbex.de>

## 2.4 Der Verschlüsselungs-Dialog

### 2.4.1 Register: Passwort

Im Register **Passwort** wählen Sie das Passwort für die Verschlüsselung. Um Tippfehler im Passwort zu vermeiden, ist eine Passwortbestätigung erforderlich. Sofern Sie ein Passwort regelmäßig verwenden, kann die Passwortbestätigung auch automatisch vorgenommen werden. → [Automatische Passwortbestätigung](#).

Möchten Sie, dass das Passwort im Klartext angezeigt wird, deaktivieren sie bitte das Häkchen bei '*Passwort verbergen*'.

- 
- [Register: Ausgabe](#)
  - [Register: Erweitert](#)
  - [Dateien/Verzeichnisse verschlüsseln](#)

### 2.4.2 Register: Ausgabe

Im Register **Ausgabe** können Sie weitere Optionen für die Verschlüsselung wählen.

#### **Dateiname verschleiern**

Standardmäßig fügt Krypter dem Namen der zu verschlüsselnden Datei lediglich eine Erweiterung zu - der Original-Dateiname bleibt beibehalten. Möchten Sie dies nicht, z.B. da der Name der Datei Rückschlüsse auf den Inhalt zulassen würde, können Sie den Original-Dateinamen verschleiern. Nach der Entschlüsselung wird der Original-Dateiname wiederhergestellt.

#### **Original-Dateien vernichten**

Möchten Sie, dass die Original-Dateien nach der Verschlüsselung automatisch vernichtet werden, aktivieren Sie bitte das Häkchen dieser Option. Bitte beachten Sie, dass die vernichteten Dateien nicht in den Windows-Papierkorb verschoben werden, sondern unwiederruflich von der Festplatte gelöscht werden. Die Vernichtungsmethode kann im Register [Erweitert](#) gewählt werden.

#### **Exe-Datei erstellen**

Diese Option gibt Ihnen die Möglichkeit ausführbare, verschlüsselte Exe-Dateien zu erstellen, so dass die Dekodierung auch auf einem Rechner erfolgen kann, auf dem Krypter nicht installiert ist. Die erstellten Exe-Dateien sind lauffähig unter Windows 95/98/NT/2000/XP/Vista/7 und Windows Server 2003/2008. (Bitte unbedingt beachten, dass Windows 3.11 NICHT unterstützt wird).

Besonders empfohlen wird diese Option, wenn Sie vertrauliche Daten per EMail versenden möchten.

#### **Einzelne Ausgabedatei**

Auf Wunsch fasst Krypter mehrere Dateien/Verzeichnisse in einer verschlüsselten Container-Datei zusammen.

**Tipp:**

Verwenden Sie häufig identische Verschlüsselungsoptionen, können Sie diese Optionen auch als Standard-Einstellungen festlegen. Rufen Sie dazu bitte die [Krypter-Optionen](#) auf.

- 
- » [Register: Passwort](#)
  - » [Register: Erweitert](#)
  - » [Dateien\Verzeichnisse verschlüsseln](#)

### 2.4.3 Register: Erweitert

Im Register **Erweitert** bestimmen Sie welcher [Algorithmus](#) und welcher [Betriebsmodus](#) für die Verschlüsselung verwendet werden soll. Außerdem können Sie festlegen, ob die Dateien gleichzeitig auch komprimiert werden sollen (um Platz auf der Festplatte zu sparen).

Die **Vernichtungsmethoden** gelten nur, sofern im Register **Ausgabe** die Option 'Originaldatei löschen' aktiviert ist.

**Wir empfehlen den Algorithmus Twofish, den Betriebsmodus CTS und die Vernichtungsmethode DoD (3x).**

**Tipp:**

Verwenden Sie häufig identische Verschlüsselungsoptionen, können Sie diese Optionen auch als Standard-Einstellungen festlegen. Rufen Sie dazu bitte die [Krypter-Optionen](#) auf.

- 
- » [Register: Passwort](#)
  - » [Register: Ausgabe](#)
  - » [Dateien/Verzeichnisse verschlüsseln](#)

## 2.5 Krypter-Optionen

### 2.5.1 Krypter-Optionen

Zu den Krypter-Optionen gelangen Sie über das Startmenü via **Start** → **Programm** → **Krypter** → **Krypter**. Alternativ können Sie die Krypter-Optionen auch über das **Kontextmenü** aufrufen. Klicken Sie dazu eine beliebige Datei mit der rechten Maustaste an und wählen Sie im Krypter-Untermenü den Eintrag Krypter.

Im erscheinendem Fenster können Sie diverse Krypter-Optionen (→ [Optionen I](#), [Optionen II](#) ) einstellen, sowie [Protokolle](#) der bisherigen Verschlüsselungs- bzw. Entschlüsselungsvorgänge betrachten. Außerdem können Sie über dieses Fenster auch

die Krypter [Bonus-Funktionen](#) aufrufen.

---

- » [Optionen I](#)
- » [Optionen II](#)
- » [Optionen III](#)
- » [Protokolle](#)
- » [Bonus-Funktionen](#)
- » [E-Mail Optionen](#)

## 2.5.2 Protokolle

Im Register '*Protokolle*' haben Sie die Möglichkeit, Protokolle der erfolgten Ver- und Entschlüsselungsvorgänge zu betrachten. Zunächst sehen Sie eine Übersicht aller Vorgänge. Die Details einzelner '*Jobs*' rufen Sie per Doppelklick auf. Möchten Sie ein bestimmtes Protokoll löschen, klicken Sie es bitte mit der rechten Maustaste an und wählen '*Protokoll löschen*'. Es ist auch möglich, alle Protokolle gleichzeitig zu löschen, indem Sie den Menüeintrag '*Alle Protokoll löschen*' auswählen.

---

### Siehe auch:

- » [Krypter-Optionen](#)
- » [Optionen I](#)
- » [Optionen II](#)
- » [Optionen III](#)
- » [Bonus-Funktionen](#)
- » [E-Mail Optionen](#)

## 2.5.3 Optionen I

Im Register '*Optionen I*' legen Sie die Standard-Einstellungen für den Ver- und für den Entschlüsselungsdialog fest.

### Beispiel:

Sie möchten, dass bei jeder Verschlüsselung,

- a)** die Original-Dateien gelöscht werden
- b)** die Dateinamen verschleiert werden
- c)** die Passworteingabe im Klartext dargestellt wird

Gehen Sie bitte folgendermaßen vor, um diese Optionen einzustellen:

Im Register '*Kodieren*' prüfen Sie, ob ein Häkchen bei '*Passwort verbergen*' gesetzt ist. Falls ja, deaktivieren Sie es, indem Sie es einmal anklicken (**c**).

Anschließend wechseln Sie in das Register '*Ausgabe*'. Dort aktivieren Sie das Häkchen bei '*Dateiname verschleiern*' (**b**) und bei der Option '*Original-Dateien löschen*' (**a**).

---

**Siehe auch:**

- » [Krypter-Optionen](#)
- » [Optionen II](#)
- » [Optionen III](#)
- » [Protokolle](#)
- » [Bonus-Funktionen](#)
- » [E-Mail Optionen](#)

## 2.5.4 Optionen II

### **Automatische Passwortbestätigung**

Auf Wunsch kann Krypter Passworte bei der Verschlüsselung automatisch bestätigen, so dass ein Passwort zu Verschlüsselung nicht grundsätzlich zweimal angegeben werden muss.

Sobald ein Passwort erfolgreich für die Verschlüsselung verwendet haben, ist es künftig nicht mehr erforderlich dieses zu Bestätigen. Ein neues Passwort muss allerdings grundsätzlich bestätigt werden; auch wenn diese *Auto-Option* aktiviert ist. Erst wenn das Passwort einmal verwendet, greift die *Automatische Passwortbestätigung*.

### **Krypter-Dateityp**

In der Gruppe Krypter-Dateityp können Sie festlegen, welche Dateierweiterung verschlüsselte Dateien erhalten sollen. Auch das Symbol für verschlüsselte Dateien können Sie hier auswählen.

### **Kontextmenü**

Vereinzelte kann es passieren, dass Sie die Krypter-Einträge im Windows-**Kontextmenü** nicht mehr vorfinden. Klicken Sie einfach auf '*Kontextmenü reparieren*' um diesen Fehler zu beheben.

---

**Siehe auch:**

- » [Krypter-Optionen](#)
- » [Optionen I](#)
- » [Optionen III](#)
- » [Protokolle](#)
- » [Bonus-Funktionen](#)
- » [E-Mail Optionen](#)

## 2.5.5 Optionen III

### **Vor Tastatur-Protokollprogrammen schützen**

Tastatureingaben können sehr einfach ausspioniert werden. Daher sollte die Option "Vor Tastatur-Protokollprogramme schützen" unbedingt aktiviert bleiben, denn so sind Passworteingaben und die Eingabe von EMail-Texten (Krypter-Mailer / Outlook-PlugIN)

sicherer.

### Qualität des Passworts darstellen

Ist diese Option bestätigt, wird das Verschlüsselungspasswort in Echtzeit, also während der Eingabe, beurteilt. Je höher der Fortschrittsbalken, desto besser ist die Passwort-Qualität.

### Outlook-PlugIN

Das Krypter Outlook-PlugIN kann über diese Schaltflächen Installiert, Neuinstalliert oder Deinstalliert werden.

### Sprach-Einstellungen:

Wählen Sie hier, ob die Krypter Oberfläche in Englischer oder Deutscher Sprache dargestellt werden soll.

---

### Siehe auch:

- » [Krypter-Optionen](#)
- » [Optionen I](#)
- » [Optionen II](#)
- » [Protokolle](#)
- » [E-Mail Optionen](#)

## 2.5.6 EMail-Optionen

### Kontextmenü

Über diese Optionen entscheiden Sie, ob die Krypter EMail-Funktionen im **Kontextmenü** angezeigt werden sollen. Ist diese Option gesetzt, können Sie eine Datei verschlüsseln und versenden, indem Sie die Datei einfach mit der rechten Maustaste anklicken und dann den entsprechenden Krypter-Menüeintrag wählen.

Bestätigen Sie die Option "**EMails direkt per MAPI senden**", sofern verschlüsselte Dateien direkt über Ihr EMail-Programm versendet werden sollen.

Sofern Sie EMail über den internen SMTP-Client versenden möchten, bestätigen Sie die Option "**EMails an den Krypter-Mailer weiterleiten**". Der [Krypter-Mailer](#) dient dann als Editor (z.b. zum Erstellen einer verschlüsselten Textnachricht) und versendet EMail, je nach Konfiguration, per SMTP oder über Ihr EMail-Programm.

### Hinweis:

Sofern Ihr EMail-Partner Krypter nicht installiert hat, achten Sie darauf, das Krypter selbstentschlüsselnde (.exe) Dateien erstellt.

- » [E-Mail Funktionen im Windows Kontextmenü](#)

### Text-Vorlagen

Krypter versendet verschlüsselte Daten, als Dateianlage einer EMail. Falls gewünscht, wird als EMailtext, automatisch der einer Vorlage verwendet. Die Text-Vorlagen können beliebige verändert werden. Klicken Sie dazu die Schaltfläche "**Text-Vorlagen bearbeiten**".

## Krypter-Mailer

Die Schaltfläche "**Krypter-Mailer starten**" öffnet den Krypter-Mailer und wechselt direkt zum Postausgang. "Verschlüsselte EMail erstellen" öffnet den Mailer ebenfalls, startet jedoch direkt im Bereich "Neue Email".

---

### Siehe auch:

» [E-Mail - Verschlüsselung](#)

» [Krypter-Optionen](#)

» [Optionen I](#)

» [Optionen II](#)

» [Optionen III](#)

» [Protokolle](#)

## 3 E-Mail - Verschlüsselung

### 3.1 E-Mail - Verschlüsselung

**Krypter** bietet zahlreiche Möglichkeiten zur Erstellung verschlüsselter E-Mails.

Es unterstützt den Versand per **MAPI** und beinhaltet für ausgehende E-Mails auch einen **SMTP-Client**. Für Microsoft Outlook steht ein **Plug-In** zur Verfügung.

Das Interface des SMTP-Clients kann auch als Editor für verschlüsselte E-Mails dienen, die über Ihr verwendetes E-Mail-Programm (z.b. Outlook, Outlook-Express, Netscape etc.) versendet werden sollen.

#### Eine verschlüsselte E-Mail erstellen:

Zur Erstellung einer verschlüsselten E-Mail, wählen Sie im Startmenü unter "Programme / Krypter" den Eintrag "Verschlüsselte EMail erstellen" und folgen den Anweisungen.

#### Bild-für-Bild-Anleitung:

Ein umfangreiches Online-Tutorial zur Krypter E-Mail-Verschlüsselung, finden Sie auf unseren Webseiten unter <http://demos.baxbex.de>

#### Weitere Informationen:

» [E-Mail Optionen](#)

» [E-Mail Funktionen im Windows Kontextmenü](#)

» [SMTP-Client / E-Mail - Editor](#)

» [Plug-In für Microsoft Outlook](#)

» [Bild-für-Bild Anleitungen](#)

## 3.2 Einträge im Kontextmenü

Im Windows-**Kontextmenü** finden Sie beim "Krypter"-Eintrag, das Untermenü "EMail". Über dieses Untermenü können folgende der Krypter EMail-Funktionen schnell aufgerufen werden.

### **Als selbstentschlüsselnde Exe-Datei senden**

Wählen Sie diesen Eintrag, wenn Sie die markierten Dateien/Verzeichnisse als selbstentschlüsselnde Exe-Datei versenden möchten. Zur Entschlüsselung der Datei, ist Krypter selbst nicht erforderlich, da die so erstellten verschlüsselten Dateien auch vollkommen eigenständige Programme sind.

### **Als verschlüsselte Datei senden**

Die aktuell markierten Dateien/Verzeichnisse werden verschlüsselt und anschließend als Dateianlage versendet. Achtung: Zur Entschlüsselung benötigt der Empfänger die Software Krypter.

### **Verschlüsselte Nachricht erstellen**

Dieser Eintrag öffnet ein Fenster, über das Sie eine verschlüsselte EMail-Nachricht erstellen können. Diesen Eintrag sollten Sie wählen, wenn Sie eine EMail erstellen möchten, die sowohl eine verschlüsselte Textnachricht, als auch verschlüsselte Dateianlage enthalten soll.

---

Über die Krypter [Optionen](#) können Sie festlegen, ob E-Mails über Ihren Standard E-Mail - Client (z.B. Outlook, Outlook-Express, Netscape etc.) oder über den [Krypter-Mailer](#) (SMTP) versendet werden.

### **Weitere Informationen:**

- » [E-Mail Optionen](#)
- » [E-Mail - Verschlüsselung](#)
- » [SMTP-Client / E-Mail - Editor](#)
- » [Plug-In für Microsoft Outlook](#)
- » [Bild-für-Bild Anleitungen](#)

## 3.3 SMTP - Client / E-Mail - Editor

### **Wichtiger Hinweis zur Verwendung des Krypter-Mailers:**

Nach der Installation ist Krypter so vorkonfiguriert, das verschlüsselte E-Mails per **MAPI**, also über Ihre Standard-E-Mail-Programm (z.B. Outlook Express, Outlook, Netscape) versendet werden.

Möchten Sie E-Mails über den Krypter-Mailer versenden, ist es unbedingt erforderlich, das Sie die Krypter E-Mail-Optionen entsprechend ändern. Bestätigen Sie dazu, die Option "EMails an den Krypter-Mailer weiterleiten" im Tab "EMail-Optionen". Weitere Informationen zu den EMail-Optionen finden Sie [hier](#).

Der Krypter-Mailer ist in erster Linie für Systeme, auf denen **MAPI** nicht installiert oder nicht verwendet werden kann.

**Mit den Krypter-Mailer können Sie:**

- Textnachrichten erstellen, verschlüsseln und versenden
- Dateien verschlüsseln und versenden
- E-Mails verschlüsseln und versenden, die sowohl eine Textnachricht, als auch Dateianlagen enthalten

**Aufruf des Krypter-Mailers:**

Den Krypter-Mailer erreichen Sie zum Beispiel über das Startmenü via **"Start"** → **"Programme"** → **"Krypter"** → **"Verschlüsselte EMail erstellen"** aufrufen.

**Konfiguration des Krypter-Mailers:**

Eine manuelle Konfiguration ist in der Regel nicht erforderlich.

Sollte es beim E-Mailversand jedoch zu Problemen kommen, prüfen Sie, ob die E-Mail-Einstellungen des SMTP-Servers korrekt übernommen worden sind. Klicken Sie dazu auf die Schaltfläche "Einstellungen", die Sie im linken, unteren Bereich des Fensters finden. Bei "Server-Einstellungen" korrigieren Sie nun ggf. die zu Ihrem E-Mail-Account gehörigen Daten. Sind Ihnen die notwendigen Einstellungen nicht bekannt, erfragen Sie diese bitte bei Ihrem Internetdienstleister oder Ihrem Administrator. Alternativ prüfen Sie, ob Sie die entsprechenden Daten für den SMTP-Server über die Konfiguration Ihres E-Mail-Programmes in Erfahrung bringen können.

**Weitere Informationen:**

- » [E-Mail Optionen](#)
- » [E-Mail Funktionen im Windows Kontextmenü](#)
- » [E-Mail - Verschlüsselung](#)
- » [Plug-In für Microsoft Outlook](#)
- » [Bild-für-Bild Anleitungen](#)

## 3.4 Plug-In für Microsoft Outlook

**Krypter** enthält ein Plug-In für Microsoft Outlook. Bitte beachten Sie, dass dieses Plug-In nicht für Outlook-Express geeignet ist.

Um eine verschlüsselte Nachricht über das Krypter Outlook-Plug-In zu erstellen, klicken Sie auf die Krypter-Schaltfläche, die Sie in der Symbolleiste des Outlook Hauptbildschirms finden.

**Bild-für-Bild-Anleitung:**

Ein umfangreiches Online-Tutorial zum Krypter Outlook Plug-In, finden Sie auf unseren Webseiten unter:

<http://demos.baxbex.de>

**Weitere Informationen:**

- >> [E-Mail Optionen](#)
- >> [E-Mail Funktionen im Windows Kontextmenü](#)
- >> [E-Mail - Verschlüsselung](#)
- >> [SMTP-Client / E-Mail - Editor](#)
- >> [Bild-für-Bild Anleitungen](#)

### 3.5 Bild-für-Bild Anleitungen

Umfangreiche Online-Tutorials zur Krypter E-Mail-Verschlüsselung, finden Sie auf unseren Webseiten unter <http://demos.baxbex.de>

## 4 Bonus-Funktionen

### 4.1 Krypter Bonus Funktionen

Obwohl echte Datenverschlüsselung die einzig sichere Methode ist, sensible Daten vor den Augen Dritter zu verbergen, haben wir uns entschlossen, Krypter mit einigen Bonus-Funktionen auszustatten - als Alternative zur mitunter doch sehr zeitintensiven Verschlüsselung.

**Wir weisen jedoch ausdrücklich darauf hin, dass diese Funktionen keinesfalls mit der Sicherheit der Krypter- Dateiverschlüsselung gleichzusetzen und lediglich als 'Kindersicherung' zu verstehen sind.**

Zum Verstecken von Verzeichnissen empfehlen wir das Programm [Folder Shield 2001](#).

- 
- >> [Exe-Dateien durch ein Passwort schützen](#)
  - >> [Laufwerke verstecken](#)
  - >> [Verzeichnis tarnen](#)

ausserdem:

» [Lokales Kryptometer](#)

## 4.2 Exe-Dateien durch ein Passwort schützen

**Krypter** gibt Ihnen die Möglichkeit, beliebige Exe-Dateien durch ein Passwort zu schützen, so dass vor der Ausführung des jeweiligen Programms zunächst ein Passwort eingegeben werden muss.

### Eine beliebige Exe-Datei vor der Ausführung durch ein Passwort schützen

1. Starten Sie Krypter (z.B. über das Startmenü).
2. Wechseln Sie in das Register '*Bonus*'.
3. In der Gruppe 'Programmausführung' klicken Sie auf die Schaltfläche '*Hinzufügen*'.
4. Wählen Sie nun die zu schützende Exe-Datei aus.
5. Bestätigen Sie dann die Option '*Passwortschutz aktivieren*' und geben ein Passwort an.

---

» [Laufwerke verstecken](#)

» [Verzeichnis tarnen](#)

## 4.3 Komplette Laufwerke verstecken

Mit **Krypter** können Sie komplette Laufwerke unter Windows ausblenden. Aktivieren Sie dazu lediglich ein Häkchen bei dem Laufwerk, das Sie ausblenden möchten.

Bitte beachten Sie, dass bei einigen Systemen leider ein Neustart erforderlich ist, bevor die Änderungen im Windows-Explorer (oder auch im Arbeitsplatz) sichtbar werden.

---

» [Exe-Dateien durch ein Passwort schützen](#)

» [Verzeichnis tarnen](#)

## 4.4 Lokales Kryptometer

Das lokale Kryptometer ist ein kleines Statistikfeature, über das Sie jederzeit erfahren können, wie viele Daten bzw. wie viele Dateien Sie bereits mit **Krypter** verschlüsselt haben.

---

» [Exe-Dateien durch ein Passwort schützen](#)

» [Laufwerke verstecken](#)

» [Verzeichnis tarnen](#)

## 4.5 Verzeichnis tarnen

Mit **Krypter** können Sie einzelne Verzeichnisse tarnen. Wird ein getarntes Verzeichnis im Windows-Explorer aufgerufen, wird nicht der Inhalt des Verzeichnisses, sondern die Systemsteuerung angezeigt.

**Achtung:** In einigen Dateimanagern funktioniert die Tarnung nicht.

Zum echten Verstecken von Verzeichnissen, empfehlen wir das Programm [Folder Shield](#).

---

» [Exe-Dateien durch ein Passwort schützen](#)

» [Laufwerke verstecken](#)

» [Lokales Kryptometer](#)

## 5 Häufig gestellte Fragen (FAQ)

### 5.1 FAQ

#### **Speichert Krypter Passwörter auf der Festplatte?**

Nein. Auch wenn die Option '*automatische Passwortbestätigung*' aktiviert ist, speichert Krypter keine Passwörter auf der Festplatte. Es werden sogenannte Einweg-Hash-Funktionen (SHA-1) für die automatische Passwortbestätigung verwendet.

#### **Wie verhindere ich, das eine per EMail verschickte Exe-Datei von einer Firewall geblockt wird?**

Ändern Sie die Dateierweiterung (z.B. in .exe\_) und teilen dem Empfänger mit, das die Datei umbenannt werden muss, bevor die Entschlüsselung ausgeführt werden kann.

Über die Krypter Optionen unter "EMail-Optionen" können Sie auch die Text-Vorlage entsprechend anpassen.

#### **Unter welchen Windows-Versionen kann eine von Krypter erstellte Exe-Datei ausgeführt werden?**

Die erstellten Exe-Dateien laufen unter Windows 95/98/ME/NT/2000, Windows XP, Windows Vista und Windows 7.

#### **Gibt es Hintertürchen bei Krypter?**

Nein!

**Welcher Verschlüsselungsalgorithmus und welcher Betriebsmodus ist empfohlen?**

Wir empfehlen den Twofish Algorithmus und den CTS Modus.

**Ich habe ein Passwort vergessen, was kann ich tun?**

Krypter verwendet starke Verschlüsselungsalgorithmen. Es ist nicht möglich, verschlüsselte Dateien ohne das korrekte Passwort zu entschlüsseln.

**Ich habe ein Laufwerk versteckt; warum ist es trotzdem im Explorer sichtbar?**

Auf einigen Systemen ist ein Windows-Neustart erforderlich, bevor die Änderungen im Explorer (oder auch im Arbeitsplatz) aktualisiert werden. Unter Windows NT/2K/XP/Vista/7 steht diese Funktion nicht zur Verfügung.

**Was bedeutet die Meldung 'Achtung: CAPS LOCK aktiv'.**

Krypter unterscheidet zwischen der Gross-/Kleinschreibweise der Passwörter. Es ist unbedingt erforderlich, dass Passwörter bei der Ver- und Entschlüsselung identisch geschrieben werden. Erscheint die Warnung, das CAPS LOCK aktiviert ist, heisst das, dass die Taste zur automatischen Grossschreibung gedrückt wurde und somit der CAPS Lock Modus aktiv ist. Die CAPS LOCK-TASTE finden Sie auf Standard-Tastaturen so:

- zwei Tasten über der 'STRG'-Taste.
- direkt neben der 'A' Taste

**Obwohl die Option automatische Passwortbestätigung aktiviert ist, erscheint es mir, als müsste ich jedes Passwort trotzdem zweimal eingeben. Was verstehe ich da falsch?**

Die automatische Passwortbestätigung kann nur für Passwörter erfolgen, die Sie bereits verwendet haben. Das heisst: Benutzen Sie das Passwort 'hallo' zum ersten Mal, müssen Sie es auch bestätigen (trotz eingestellter Option). Verwenden Sie das Passwort 'hallo', dann für weitere Verschlüsselung ist die Bestätigung nicht erforderlich.

Haben Sie ein Passwort verwendet, und die automatische Bestätigung war zu jenem Zeitpunkt nicht aktiviert, müssen Sie es einmalig doppelt eingeben.

**Sind Krypter Updates kostenlos?**

Krypter wird zu einem sehr günstigen Preis angeboten. Dennoch sind alle Updates einer Versionsreihe in der Regel kostenlos. Informationen zu vergünstigten Updatepreisen finden Sie auf der BAXBEX Software Website unter <http://www.baxbex.de>. Kostenlose Updates müssen Sie jedoch selbst von der Webseite downloaden. Eine automatische Zustellung per Post oder per Email ist nur möglich, wenn Sie einen entsprechenden Servicevertrag abgeschlossen haben.

**Wie erfahre ich, ob es eine neue Krypter Version gibt?**

Auf der BAxBEx Software Webseite können Sie einen kostenlosen Newsletter abonnieren, der Sie automatisch über Updates per Email informiert. Sie können uns Ihre Emailadresse anvertrauen, denn wir respektieren Ihre Privatsphäre und werden Ihre Daten NICHT an Dritte weitergeben. **Siehe auch:** [BAxBEx Software Newsletter](#)

### **Was, wenn ich einen Programmfehler entdeckt habe?**

Es ist uns sehr wichtig, dass Krypter nach Möglichkeit fehlerlos arbeitet. Deshalb möchten wir Sie bitten, uns unbedingt zu informieren, wenn Sie denken einen Bug gefunden zu haben. Bitte beschreiben Sie uns das Problem möglichst genau, und falls Sie eine Regelmäßigkeit festgestellt haben, geben Sie bitte an, wie der Fehler rekonstruiert werden kann. Ganz wichtig ist auch, dass Sie sich vergewissern, die aktuellste Krypter Version installiert zu haben und Sie uns ein paar Informationen zu Ihrem System nennen (welche Windows-Version, Grafikkarte, Drucker, etc.). **Siehe auch:** [Über Fehler berichten](#)

### **Was mache ich mit Verbesserungsvorschlägen?**

Senden Sie uns unbedingt eine Mail. Wir sind Ihnen SEHR DANKBAR für Ihre Verbesserungsvorschläge.  
→ [support@baxbex.de](mailto:support@baxbex.de)

### **Wie kann ich die Testversion in eine Vollversion umwandeln?**

Nachdem Sie Ihre Krypter Bestellung aufgegeben haben, erhalten Sie mit Ihrem persönlichen Registrierungsschlüssel auch eine genaue Beschreibung, wie Sie den Registrierungsschlüssel eingeben können. **Siehe auch:** [Krypter registrieren](#)

### **Was ist, wenn mein Registrierungscode abhanden gekommen ist?**

Sofern Sie über eine Emailadresse verfügen, können wir Ihnen Ihren Registrierungscode erneut per Email senden. Bitte haben Sie jedoch Verständnis dafür, dass die erneute Zusendung nur EINMAL möglich ist.

### **Welche Programme gibt es noch von BAxBEx Software?**

Auf der BAxBEx Software Website - <http://www.baxbex.de> - finden Sie genaue Beschreibungen zu Share- und Freeware Programmen von BAxBEx Software.

### **Was, wenn ich meine Frage hier nicht finden kann?**

Senden Sie eine Mail an [support@baxbex.de](mailto:support@baxbex.de). Beschreiben Sie Ihre Frage bitte möglichst genau und vergessen Sie nicht anzugeben, welche Krypter-Version Sie installiert haben und welches Betriebssystem Sie nutzen.

---

➤ [Tips & Tricks](#)

## 5.2 Algorithmen & Co

### 5.2.1 Verschlüsselungs-Algorithmen

**Krypter** unterstützt verschiedene Verschlüsselungsverfahren. Im Register "Erweitert" bestimmen Sie, mit welchem der 7 zur Verfügung stehenden "CHIFFRIERVERFAHREN" sie verschlüsseln möchten.

**Krypter** arbeitet mit symmetrischen Chiffrierverfahren, dh: Verschlüsseln und Entschlüsseln erfordern jeweils die Kenntnis ein und desselben Schlüssel bzw. Passwort.

**In Krypter stehen Ihnen folgende Algorithmen zur Verfügung:**

---

**AES** (= "Advanced Encryption Standard" dh "RIJNDAEL", der Sieger des Wettbewerbes um den neuen USA-Verschlüsselungsstandard) ist ein Block-Chiffrier-Algorithmus mit einer Blockbreite von 128 bit (= 16 Bytes) und einem Schlüsselraum von wahlweise 128, 192 oder **256 bit**. Je breiter der Schlüsselraum ist und je häufiger der "Verwürfelungsvorgang" wiederholt wird (sog: "Runden"), desto sicherer wird der Algorithmus gegen "brute force"-Angriffe, dh gegen Versuche durch "Durchprobieren aller möglichen Schlüssel", die Chiffrierung "zu brechen". Bei Rijndael können wahlweise 10, 12 oder 14 Runden gewählt werden, um Geschwindigkeit gegen Sicherheit abzuwägen.

**TWOFISH** (ein anderer AES-Finalist), arbeitet etwas langsamer als Rijndael, man glaubt aber, dass er kryptographisch noch bedeutend stärker sei als AES (bei der End-Auswahl wurde der Geschwindigkeit der Vorrang vor der "Stärke" gegeben). Auch er ist ein Block-Algorithmus von 128 bit und einer analogen Schlüsselbreite von 128, 192 und **256 bit**. Er arbeitet fix mit 16 Runden.

**MARS** (auch ein guter AES-Finalist), der nach einer etwas anderen Methode arbeitet und wegen seiner bescheidenen Verschlüsselungs-Geschwindigkeit und seiner "Neuheit" aus dem Rennen fiel. Viele Kryptologen glauben halt erst dann an die Sicherheit, wenn während Jahren ergebnislos alle "Knack-Versuche" gescheitert sind. MARS ist nicht "schwach", er muss einfach seine Bewährungsprobe noch ablegen. Er ist auch ein Blockalgorithmus von 128 bit mit einer variablen Schlüsselbreite von 128 bis zu max **1248 bit** und verwendet 32 Runden.

**CAST 256** ist eine Weiterentwicklung von CAST-128, der seinerseits auf CAST-64 beruht (der als Konkurrent zu DES gedacht war). Es sind keine Schwächen bekannt. Es ist (mittlerweile) ein Block-Algorithmus von 128 bit und Schlüsselbreiten von 128, 160, 192, 224 oder **256 bit** wahlweise, stets mit 12 Runden.

**BLOWFISH** ist schon recht betagt (1994), trotzdem sind bisher keine Schwächen bekannt geworden. Es ist ein Blockalgorithmus von nur 64 bit und Schlüsseln von 32 bit bis **448 bit** Breite. Er ist ausserordentlich weit verbreitet und beliebt, da er nur minimale Anforderungen an das Rechner-System stellt. Er arbeitet mit 16 Runden.

**GOST** ist das Russische Gegenstück zum Amerikanischen DES, ein universell verwendeter Algorithmus, von dem allerdings einige unterschiedliche Versionen existier(t)en, vermutlich für verschiedene Dienste. Es ist ein 64 bit Blockalgorithmus mit einem festen Schlüssel von **256 bit** und arbeitet mit 32 Runden. Er galt und gilt immer noch gilt als wesentlich stärker als DES.

**SCOP** ist ein Stromchiffrieralgorithmus, der einen Schlüssel-abhängigen Chiffre-Strom erzeugt, mit dem der Klartext nur über eine einfache XOR-Verknüpfung chiffriert wird (**384 bit**). Er ist dadurch besonders schnell, deutlich schneller als alle Blockchiffrier-Algorithmen, hat aber den Nachteil, dass ein Schlüssel immer nur EINMAL gebraucht werden darf, ansonst die Sicherheit stark gefährdet wird. Es gibt eben auch in der Kryptographie keine Vorteile ohne Nachteile.

---

**Hinweis:** Bei allen Verschlüsselungsalgorithmen verwendet Krypter die maximale Schlüsselbreite.

» [Verschlüsselungsreihenfolgen](#)

## 5.2.2 Verschlüsselungs-Reihenfolgen

Im **Krypter** können Sie bei allen Blockalgorithmen zwischen 4 verschiedenen CHIFFRIERMODI wählen: "CTS", "CBC", "CFB", "OFB".

Etwas Theorie zuerst: Alle Blockalgorithmen können im Prinzip nur "ganze" Blöcke verschlüsseln. Sollte die Textlänge von einem Vielfachen der Blocklänge abweichen, muss das korrigiert werden: "Padding" (Puffern): Der letzte Block wird mit bedeutungslosen Zeichen (0,1,) aufgefüllt und der letzte Wert gibt deren Anzahl an, so dass sie nach der Dechiffrierung wieder entfernt werden können. Konsequenz: die Länge des Chiffrates weicht von der Länge des Klartextes ab und die Sicherheit des letzten Blockes ist etwas zweifelhaft. Wenn das unzulässig sein sollte => siehe "CTS"

**CTS (Cipher Text Stealing):** Durch ein vom klassischen "padding" abweichendes Verfahren, ist es möglich Texte deren Länge NICHT einem Vielfachen eines Blockes entsprechen TROTZDEM in ihrer ursprünglichen Länge (plus den zwingenden IV, natürlich) im CBC-Modus zu erhalten. UND dabei die Sicherheit des letzten Blockes zu erhalten. DIESE METHODE IST SEHR EMPFEHLENSWERT

**CBC (Cipher Block Chaining):** Bevor der erste Klartext-Block verschlüsselt wird, wird er mit einem "zufälligen" Block (genannt IV = Initialisierungs-Vektor) vermischt und dieses Verfahren der "Vormischung" mit dem Chiffirat des vorhergehenden Blockes durch den ganzen Chiffrier-Prozess weitergeführt.

Vorteil: die Struktur des Klartextes ist nicht mehr erkennbar. Damit können "viele" Texte mit dem gleichen Schlüssel chiffriert werden, ohne die Sicherheit zu gefährden. DIESE METHODE IST EMPFEHLENSWERT.

Nachteile: Parallelverarbeitung ist unmöglich, ein Übermittlungsfehler beeinträchtigt einen ganzen Block und ein zusätzliches Zeichen im nachfolgenden Block. Das Chifftrat wird zusätzlich zum "padding" nochmals einen Block länger (der IV!).

**CFB (Cipher Feed Back):** Der erste Klartextblock wird mit dem (wiederum zufälligen IV) verknüpft und erst DANN chiffriert. Dieses Verfahren wiederholt sich mit dem verschlüsselten Ergebnis des vorhergehenden Blockes durch das ganze Chiffriersystem.

Vorteile: Die Struktur des Klartextes ist nicht mehr erkennbar. Damit können "viele" Texte mit dem gleichen Schlüssel chiffriert werden, ohne die Sicherheit zu gefährden. "padding" ist nicht nötig, es können auch Bruchteile von Blöcken chiffriert werden. DIESE METHODE IST EMPFEHLENSWERT

Nachteile: Parallelverarbeitung ist nicht möglich, ein Übermittlungsfehler beeinträchtigt einen Wert und den ganzen nachfolgenden Block. Der Klartext ist trotzdem um die Länge des IV grösser als der Klartext.

**OFB (Output Feed Back):** Verwandelt eine Blockchiffrierprogramm in einen Stromchiffrierer, mit all seinen Vor- und Nachteilen. Sehr schnell, aber begrenzte Sicherheit. WENN SCHON, DANN GLEICH EINEN STROMCHIFFRIER NEHMEN.

**EBC (Electronic Code Book):** Jeder Block des Klartextes wird einzeln verschlüsselt und das Chifftrat ist einfach die Aneinanderreihung aller einzeln chiffrierter Blöcke.

Vorteil: es ist besonders einfach zu implementieren und, nötigenfalls, kann aus Geschwindigkeitsgründen der Klartext auf mehreren parallelen Kanälen GLEICHZEITIG bearbeitet werden. Was früher von "Bedeutung" war.

Nachteile: Die Struktur des klartextes wird nicht "verborgen", wenn Sie den gleichen Text mit dem gleichen Schlüssel mehrmals übermitteln, so ist das Chifftrat jedesmal gänzlich identisch. (also: die "Sehr geehrten Damen und Herren" sind dann in JEDEM Brief, zwar verschlüsselt, aber stets identisch und am gleichen Platz. Was der Sicherheit doch sehr abträglich sein dürfte...) Ein Übermittlungsfehler macht einen ganzen Block unentzifferbar. Da DIESE METHODE WENIGER EMPFEHLENSWERT ist wird der EBC von Krypter nicht mehr unterstützt.

---

» [Verschlüsselungsalgorithmen](#)

## 6 Tipps & Tricks

### 6.1 Tipps & Tricks

#### Sensible Daten per EMail versenden

Wichtige oder persönliche Daten sollten Sie keinesfalls unverschlüsselt per EMail

versenden, denn das Briefgeheimnis bei E-Mails ist etwa so groß wie es bei Postkarten ist. Mit Krypter können Sie selbstentschlüsselnde Exe-Dateien erstellen, die auch auf Rechnern, auf denen Krypter nicht installiert ist, ausgeführt werden können. →

### [Verschlüsselte Exe-Datei erstellen](#)

#### **Standard-Einstellungen für die Verschlüsselung festlegen**

Dies ist im Kapitel [Optionen I](#) beschrieben.

#### **Eine Containerdatei erstellen**

1. Starten Sie den Windows-Explorer.
2. Markieren Sie alle Dateien und Verzeichnisse, so dass alle zu verschlüsselnden Dateien blau hinterlegt sind.
3. Klicken Sie eine der Datei (bzw. der Verzeichnisse) mit der rechten Maustaste an und wählen Sie im **Kontextmenü** den Eintrag '*Krypter/Verschlüsselung*'.
4. Geben Sie ein Passwort ein und bestätigen Sie dieses.
5. Wechseln Sie ins Register 'Ausgabe' und bestätigen Sie dort die Option 'Einzelne Ausgabedatei'
6. Klicken Sie auf die 'OK' Schaltfläche.

#### **Krypter durch ein Passwort schützen**

1. Starten Sie Krypter (z.B. über das Startmenü).
2. Wechseln Sie in das Register '*Optionen II*'.
3. Bestätigen Sie die Option '*Krypter durch ein Passwort schützen*' und wählen Sie ein Passwort.

#### **Eine beliebige Exe-Datei vor der Ausführung durch ein Passwort schützen**

1. Starten Sie Krypter (z.B. über das Startmenü).
2. Wechseln Sie in das Register '*Bonus*'.
3. In der Gruppe 'Programmausführung' klicken Sie auf die Schaltfläche '*Hinzufügen*'.
4. Wählen Sie nun die zu schützende Exe-Datei aus.
5. Bestätigen Sie dann die Option '*Passwortschutz aktivieren*' und geben ein Passwort an.

---

 [Häufig gestellte Fragen \(FAQ\)](#)

## **7 Bestellung & Support**

### **7.1 Krypter registrieren/bestellen**

Möchten Sie Krypter nach Ablauf der 30-tägigen Testphase benutzen, benötigen Sie eine Lizenz für jeden Arbeitsplatz an dem Sie Krypter benutzen möchten.

Bei Mehrplatzlizenzen können Rabatte eingeräumt werden.

Nachdem Ihre Registrierung von uns bearbeitet wurde, erhalten Sie einen persönlichen

Registrierungsschlüssel und alle Informationen, die Sie benötigen, um die Krypter Testversion in eine Vollversion umzuwandeln. Ihre Bestellung wird **sehr schnell** von uns bearbeitet, so dass Sie Ihren Registrierungsschlüssel in der Regel **innerhalb 24 Stunden erhalten**.

Ihr Registrierungsschlüssel bleibt gültig bis zum nächsten Main-Release. Alle Minor-Updates können kostenlos über das Internet bezogen werden.

#### **Online Registrierung über das Internet:**

Auf unserer Webseite haben Sie die Möglichkeit **Krypter Online auf einer sicheren, SSL- verschlüsselten Bestellseite zu registrieren**. Bitte besuchen Sie dazu unseren Onlineshop unter <http://www.baxbex.de>

Alternativ zur Bezahlung per **Kreditkarte** können Sie auch eine konventionelle Zahlungsmethode wählen. Neben der Bezahlung per Kreditkarte, bieten wir Ihnen Zahlungsmethoden wie **Lastschrift, Nachnahme, (Vorab-) Überweisung, Bar oder Scheck, Rechnung** (nur Großfirmen, Behörden etc.)

#### **Registrierung per Post, Fax, EMail oder Telefon:**

Möchten Sie Krypter nicht über das Internet bestellen, klicken Sie bitte hier, um den komfortablen **Bestellassistenten** zu starten.  
Sie können Ihre Bestellung auch **telefonisch unter 0 23 69 / 20 00 77** aufgeben.

## **7.2 Kontakt zu BAXBEx Software**

Bitte besuchen Sie die **BAXBEx Software** Webseite:

<http://www.baxbex.de>

Dort finden Sie die neuesten Informationen über Krypter und alle anderen Produkte von BAXBEx Software. Falls Sie Fragen, Kommentare oder Vorschläge haben oder weitere Informationen benötigen, senden Sie bitte eine E-Mail an:

[support@baxbex.de](mailto:support@baxbex.de)

Sollten Sie keinen Zugang zum Internet haben, senden Ihre Anfrage(n) bitte an:

#### **Briefpost:**

BAXBEx Software  
Erneeweg 39  
D-46286 Dorsten  
Deutschland

#### **Fax:**

++49 (2369) 24 80 92

**Tel:**

++49 (2369) 20 00 77

BAXBEx Software unterhält außerdem einen [Newsletter](#).

---

Vielen Dank für Ihr Interesse an Krypter!

## 7.3 Über Fehler berichten

**Bevor Sie einen Fehler melden:**

Wenn Sie meinen, einen Fehler entdeckt zu haben, stellen Sie bitte sicher, dass Sie die aktuellste Krypter Version installiert haben.

Lesen Sie die Online-Hilfe - möglicherweise enthält sie Hinweise zur Behebung des Problems.

**Folgende Informationen benötigen wir:**

- Welches Betriebssystem (und Version) verwenden Sie?
- Welche Krypter-Version verwenden Sie?
- Beschreiben Sie im Detail, was Sie vor dem Auftreten des Problems getan haben.
- Schreiben Sie alle Meldungen auf, die Sie von Krypter erhalten haben.
- Kann das Problem reproduziert werden? Wenn ja, teilen Sie bitte genau mit, wie!
- Sonstige Informationen, die Sie für wichtig erachten.

Senden Sie diese Informationen via E-Mail (bevorzugt), Fax oder Briefpost an:

**E-Mail:**

[support@baxbex.de](mailto:support@baxbex.de)

**Briefpost:**

BAXBEx Software  
Erneeweg 39  
D-46286 Dorsten  
Deutschland

**Fax:**

++49 (2369) 24 80 92

**Tel:**

++49 (2369) 20 00 77

## 7.4 BAxBEx Software Newsletter

**BAxBEx Software** unterhält einen **kostenlosen Newsletter**, über den Sie über neue Programmversionen und neue Produkte von **BAxBEx Software** informiert werden.

Wenn sie in der Mailingliste eingetragen sind, erhalten Sie eine E-Mail, sobald eine neue Version von Krypter herausgegeben wird.

Sie haben zwei Möglichkeiten sich in die BAxBEx Software Mailingliste eintragen oder aus der Liste entfernen zu lassen:

**www:**

Auf unserer Website folgen Sie einfach den Links zum Newsletter und tragen dort Ihre E-Mail-Adresse ein.

<http://www.baxbex.de>

**E-Mail:**

Senden Sie eine E-Mail mit dem Betreff "Subscribe" zum Eintragen in die Liste oder "Remove", wenn Sie den Newsletter nicht weiter erhalten möchten. Sonstige Nachrichten im eigentlichen Text der E-Mail werden ignoriert.

[newsletter@baxbex.de](mailto:newsletter@baxbex.de)

**Wichtig:**

BAxBEx Software wird Ihre E-Mail-Adresse niemals an Dritte weitergeben, da wir ungewollte kommerzielle E-Mail-Sendungen selbstverständlich nicht unterstützen!

## 8 Über Krypter

### 8.1 Copyright

**CryptoMite - Copyright © 1998 - 2010 BAxBEx Software. Alle Rechte vorbehalten.**

Die ausführbaren Datei von Krypter, die Hilfe-Datei, alle Programmgrafiken und alle anderen Dateien dieses Programms sind **Copyright © 1998 - 2010 BAxBEx Software**. Alle Rechte vorbehalten.

Kein Teil dieser Software darf in Teilen oder im Ganzen vervielfältigt werden, Ausnahmen sind in den Lizenzbestimmungen wiedergegeben. Diese Copyright-Notiz darf nicht aus dieser Software entfernt werden. Es ist außerdem verboten, diese Software zu de-compilieren oder zu de-assemblieren oder sonstige Arten des "Reverse Engineering" durchzuführen.

Alle Produkte oder Markennamen, die in dieser Software erwähnt sind, sind Markennamen oder registrierte Markennamen ihrer jeweiligen Besitzer.

---

## 8.2 Lizenzvereinbarung

### Krypter - Lizenzvereinbarung

**Copyright © 1998 - 2010 BAXBEX Software  
Alle Rechte vorbehalten.**

Bitte lesen Sie die folgenden Punkte gründlich, bevor Sie diese Software benutzen. Wenn Sie mit einem oder mehreren der folgenden Punkte nicht übereinstimmen, ist Ihnen die Verwendung dieses Programms nicht gestattet. Sie müssen die Software in diesem Fall sofort löschen.

**Krypter wird zu Testzwecken kostenlos zur Verfügung gestellt.** Der Sinn und Zweck der Testversion ist, dem Anwender qualitativ hochwertige Software zur Verfügung zu stellen, die vor dem Kauf ausführlich getestet werden kann. Nach Ablauf der festgelegten Testperiode müssen Sie die Lizenzgebühr bezahlen, falls Sie sich entschließen, diese Software weiter zu verwenden.

#### **Die Testperiode für Krypter beträgt 30 Tage ab dem Datum der ersten Installation!**

Krypter ist durch internationalen Copyright-Bestimmungen geschützt, es ist nicht Public Domain. Ihnen wird eine eingeschränkte Lizenz zur Nutzung dieser Software für die Dauer der Testperiode von höchstens 30 Tagen gewährt.

Die Nutzung dieser Software nach dem Ablauf der Testperiode von 30 Tage ohne Zahlung der Lizenzgebühr an BAXBEX Software stellt eine Verletzung der Copyright-Bestimmungen dar; somit handelt es sich um eine Straftat.

Es ist verboten, diese Software zu de-compileren oder zu de-assemblieren oder sonstige Arten des "Reverse Engineering" durchzuführen.

Das Bezahlen der Lizenzgebühr berechtigt einen einzelnen Anwender Krypter zu nutzen. Nach Registrierung und Zahlung der Lizenzgebühr erhalten Sie einen persönlichen Registrierungscode für diese Software. "Einzelner Anwender" heißt, dass diese Software nur von einer einzelnen Person benutzt werden darf. Die Installation auf mehreren Rechnern oder auf einem Netzwerk-Server mit gleichzeitigem Zugriff mehrerer Personen erfordert eine Multi-User-Lizenz. Details darüber können bei BAXBEX Software erfragt werden.

#### **Garantie und Haftung!**

Das Programm Krypter und die begleitende Dokumentation verwenden Sie "wie sie sind". Bei der Programmerstellung wurde mit großer Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. BAXBEX Software gibt keine Garantien irgendwelcher Art, weder ausdrücklich noch implizit, über die Verwendbarkeit bzw. Nichtverwendbarkeit des Programms und seiner begleitenden Dokumentation für irgendeinen Zweck.

BAXBEX Software übernimmt keine Verpflichtung für den Gebrauchswert dieser Software über den Kaufpreis hinaus.

Unter keinen Umständen ist BAXBEX Software für Folgeschäden haftbar, einschließlich aller entgangenen Gewinne und Vermögensverluste oder anderer mittelbarer und unmittelbarer Schäden, die durch den Gebrauch oder die Nichtverwendbarkeit der Software und ihrer begleitenden Dokumentation entstehen oder entstanden sind. Dies gilt auch dann, wenn BAXBEX Software über die Möglichkeit solcher Schäden unterrichtet war oder ist.

---

## 8.3 Garantie und Haftung

### Garantie und Haftung!

Das Programm Krypter und die begleitende Dokumentation verwenden Sie "wie sie sind". Bei der Programmerstellung wurde mit großer Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. BAXBEX Software gibt keine Garantien irgendwelcher Art, weder ausdrücklich noch implizit, über die Verwendbarkeit bzw. Nichtverwendbarkeit des Programms und seiner begleitenden Dokumentation für irgendeinen Zweck.

BAXBEX Software übernimmt keine Verpflichtung für den Gebrauchswert dieser Software über den Kaufpreis hinaus.

Unter keinen Umständen ist BAXBEX Software für Folgeschäden haftbar, einschließlich aller entgangenen Gewinne und Vermögensverluste oder anderer mittelbarer und unmittelbarer Schäden, die durch den Gebrauch oder die Nichtverwendbarkeit der Software und ihrer begleitenden Dokumentation entstehen oder entstanden sind. Dies gilt auch dann, wenn BAXBEX Software über die Möglichkeit solcher Schäden unterrichtet war oder ist.

## 8.4 Danksagung

Viele Personen haben durch Vorschläge, Tests, Bugberichte usw. geholfen, Krypter zu dem zu machen, was es ist. Diesen Personen möchten wir an dieser Stelle herzlichst danken!

### Diethelm T. Utzinger

Für fachliche Ratschläge, sowie der aktiven Mitgestaltung der Dokumentation.

### Frank Kintrup von fkWare

Für das fantastische Setup Programm und das Spitzenprogramm **Sysmon**.

→ <http://www.fkware.com>

### Ingo Günther

Für Grafiken und Symbol der Krypter Oberfläche. Benötigen Sie einen Grafiker, sollten Sie unbedingt mit Herrn Günther sprechen. Super-Service & Super-Ideen!

→ <http://www.freio.de>

### Andreas Reichelt

Für das Lektorat der Dokumentation sowie zahlreiche, sehr konstruktive Kritiken zu Krypter.

**Besonderen Dank an:** Kerstin Wetter, Hajo Stern, Irmela Gagern, Thomas Lilienthal, Roman L. Muhlke, Markus Hahn [...]



# Index

## - A -

### Algorithmen

- AES / Rijndael 26
- Blowfish 26
- Cast 256 26
- Gost 26
- Mars 26
- Scop 26
- Twofish 26

- Anti-Keyboard-Monitoring Protection 16
- Automatische Passwortbestätigung 16

## - B -

- Bestellen 29
- Bonus-Funktionen 21

## - C -

- Ciphermodus 27
- Copyright 32

## - D -

- Dateien sicher vernichten 10
- Dateien verschlüsseln 10
- Dateinamen verschleiern 13
- Deinstallation 6
- Die wichtigsten Funktionen auf einem Blick 3

## - E -

- Einleitung 3
- Einzelne Ausgabedatei 13
- E-Mail-Einträge im Kontextmenü
  - Als selbstentschlüsselnde Exe-Datei senden 19
  - Als verschlüsselte Datei senden 19
  - Krypter2000 Mailer 19
  - Plug-In für Microsoft Outlook 20
  - Verschlüsselte Nachricht erstellen 19
- E-Mail-Optionen

- Kontextmenü 17
- Krypter2000-Mailer 17
- Text-Vorlagen 17
- E-Mail-Verschlüsselung
  - Einträge im Kontextmenü 19
  - Übersicht 18
- Exe-Datei erstellen 13
- Exe-Dateien 11
- Exe-Vorlagen 11

## - F -

- FAQ 23
- Folder Shield 23
- Fragen und Antworten 23

## - G -

- Garantie 34

## - H -

- Haftung 34
- Häufig gestellte Fragen 23

## - I -

- Individuelle Exe-Vorlagen 11
- Initialisierungsvektor 27
- IV 27

## - K -

- Kommandozeilen 5
- Kontakt 30
- Kontextmenü 16
- Krypter-Dateityp 16
- Kryptometer 22

## - L -

- Lizenzvereinbarung 33
- Lokales Kryptometer 22

**- N -**

Newsletter 32

**- O -**

Optionen 14  
Optionen I 15  
Ordner sicher vernichten 10  
Ordner verschlüsseln 10  
Original-Dateien vernichten 13  
Outlook 20

**- P -**

Parameter 5  
Passwortqualität 16  
Plug-In 20  
Protokolle 15

**- Q -**

Qualität des Passworts 16  
Quicktutorial 4

**- R -**

Registrieren 29  
Reihenfolge  
    CBC 27  
    CFB 27  
    CTS 27  
    EBC 27  
    OFB 27

**- S -**

Schlüsselbreite 26  
Schnelleinsteig 4  
Selbstenschlüsselnde Exe-Dateien 11  
Server-Einstellungen 19  
SFX 11  
Sicheres Löschen 10  
SMTP 19  
Software Aktualisierung 6

Sprache 11  
Sprach-Einstellungen 16  
Standard-Einstellungen 15

**- T -**

Tab "Ausgabe" 13  
Tab "Erweitert" 14  
Tab "Passwort" 13  
Tastatur-Protokollprogramme 16  
Tipps und Tricks 28

**- U -**

Übersicht 3  
Uninstall 6

**- V -**

Verschlüsselungstärke 26  
Verzeichnis tarnen 23  
Verzeichnis verschlüsseln 10  
Verzeichnis verstecken 23

**- W -**

Willkommen 3  
Wiping 10