ENCRYT JEDES DOKUMENT

Sie können Online-Foren und Diskussionen sehen wie: Wie kann ich einen ganzen Ordner verschlüsseln? (Übertragen Sie den Inhalt in eine ZIP-Datei!), eine PDF-Datei? Wie verschlüssele ich eine DOC-Datei usw.?

Es ist ein falsches Problem, zum Zwecke der Verschlüsselung ist jedes Dokument nichts anderes als eine Folge von n Bytes. Das einzige, was zählt, ist, eine verschlüsselte Datei zu erhalten, in der

Byte (n) + Algorithmus = verschlüsseltes Byte (n)

und dass Sie das Originaldokument mit zurückbekommen können

verschlüsseltes Byte (n) - Algorithmus = Byte (n)

Unabhängig von der Art des Dokuments steht es den Anwendungen, die es verwenden, mit seinem Inhalt und seinem ursprünglichen Namen wieder zur Verfügung.

DOKUMENTENVERRIEGELUNG

Sie können den verschlüsselten Dokumenten einen beliebigen Namen geben.

Der Name der Quelldatei wird in der verschlüsselten Datei gespeichert. Wenn das Dokument entschlüsselt wird, wird ihm automatisch der ursprüngliche Name zugewiesen, ohne dass er sich merken muss, auf welches Dokument sich diese bestimmte Datei bezieht.

TEXTBESCHREIBUNG

Was Sie über die Tastatur eingeben, ist direkt verschlüsselt. Es ist nützlich, um kurze Notizen oder Nachrichten zu schreiben, die an die E-Mail angehängt werden sollen.

Sobald die Nachricht entschlüsselt wurde, befindet sie sich in MESSAGE.TXT

AUTHENTIFIZIERUNG

Jedes verschlüsselte Dokument enthält einen nicht wiederholbaren Identifikationscode (**NIDE**), der jede Manipulationsmöglichkeit ausschließt und die Identität des Absenders sicher bestätigt.

Das Verschlüsselungssystem ist in der Tat so, dass dasselbe Dokument, das n-mal mit demselben Schlüssel verschlüsselt wurde, n immer unterschiedliche verschlüsselte Dateien und daher n unterschiedliche **NIDE**s generiert. (siehe technischen Hinweis oben)

Das **NIDE** wird am Ende der Verschlüsselung angezeigt, vom System vor dem Entschlüsseln jedes Dokuments überprüft und kann in jedem Fall jederzeit mit einer bestimmten Funktion überprüft werden. Daher können Absender und Empfänger den authentischen Ursprung des verschlüsselten Dokuments und seine Integrität sicherstellen.

Zusätzlich zum NIDE-Code wird Folgendes angezeigt:

- Erstellungsdatum

- Name des verwendeten Schlüssels

- wer das Dokument verschlüsselt hat

- Name des Originaldokuments

DIE SCHLÜSSELDATEI

Die Schlüsseldatei enthält alle Benutzerschlüssel im Formular:

KEYNAME (klar, jeder kann es sehen) + KEY (was nur Sie sehen können, da es mit der **Schlüssel zur Schlüsseldatei** verschlüsselt ist, nach der Sie zu Beginn gefragt wurden und die Sie bei jedem Betreten des Systems gefragt werden).

Sobald der Name des zu verwendenden Schlüssels bekannt ist, wird er aus dem Archiv extrahiert und nur das System kann ihn entschlüsseln (mit **Schlüssel zur Schlüsseldatei**) und seine Verwendung zulassen.

Der Name / die Referenz in Bezug auf den Schlüssel wird in den verschlüsselten Dateien gespeichert, und daher wird der zu entschlüsselnde Schlüssel ohne Angabe von Gründen verwendet.

Diese **Schlüssel zur Schlüsseldatei** ist die einzige, an die Sie sich erinnern müssen, aber Sie **MÜSSEN** sich daran erinnern, sonst können Sie die bereits verschlüsselten Dateien nie wiederherstellen, weil

Nur diejenigen, die **Schlüssel zur Schlüsseldatei** kennen, können im System arbeiten

DIE SCHLÜSSEL

Sie können mit der spezifischen Funktion des Programms generiert und ihnen dann der gewünschte Name zugewiesen werden.

Sie können mit Ihrem Korrespondenten einen gemeinsamen Schlüssel für den Schlüsselaustauschprozess erstellen.

Der Prozess wird in 2 Schritten durchgeführt:

A ---------- Daten ---- »B, das einen Schlüssel K generiert

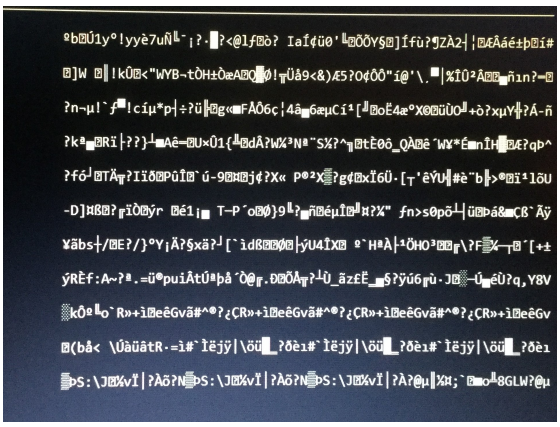
B ---------- Daten ---- »A, das einen Schlüssel generiert = K

Die Referenz ist der Benutzername des Korrespondenten. Sie wird automatisch zugewiesen und ermöglicht es beiden, die Nachrichten korrekt zu entschlüsseln. In jeder verschlüsselten Datei, die ausgetauscht wird, befindet sich der Benutzername, mit dem der gemeinsame Schlüssel in die Schlüsseldatei eingefügt wurde.

Das Programm zeigt an, welche Phase läuft.

Sie müssen sich nur darauf einigen, wer Phase 1 startet.

Den erstellten Schlüsseln kann eine Beschreibung zugeordnet werden, um die Identifizierung eines Korrespondenten zu erleichtern.



Ein Schlüssel kann auch über eine Datei mit dem Namen **KIMPEXP** im folgenden Format in das System importiert werden: Schlüsselname (24) + Benutzername (24) + Schlüssel (64)

Wie sind die Schlüssel

Mit der Funktion zum Generieren der Schlüssel können Sie den generierten Schlüssel in die KIMPEXP-Datei exportieren. Mit der Tarnfunktion können Sie **KIMPEXP** in ein Foto einfügen, das an Ihren Gesprächspartner gesendet werden soll, und so einen einigermaßen sicheren Schlüsselaustausch durchführen. **Sie können eine Liste erstellen, in der Sie alle Tasten sehen können**

(einige nicht anzeigbare Sonderzeichen werden durch ein? Ersetzt).WICHTIG: Geben Sie niemals einen neuen Schlüssel ein, der denselben Namen wie Ihr Spitzname hat.

Für ein korrektes Layout:

- Erstellen Sie eine Verknüpfung zu Qcrypto auf dem Desktop

- Rechtsklick auf das Verknüpfungssymbol

- Eigenschaften / Layout

- in den Fenstermaßen 30 in der Höhe und 102 in der Breite eingestellt