DER LAUSCHER AN DER WAND HÖRT SEINE EIGNE SCHAND UND DARUM...

Fractal Crypt 1.01,

das ultimative Ver- und Entschlüsselungsprogramm für Dateien.

Ursprünglich war es nicht meine Absicht, ein Verschlüsselungsprogramm zu schreiben, sondern eine schnelle und sichere Verschlüsselungshardware zu designen.
Mangels Simulationssoftware sah ich mich gezwungen, diese selbst zu entwickeln.
Nach Abschluß der Testphase hatte ich ein Programm, das sehr rechenaufwendig (1 KB/s) eine Hardware simuliert, welche bis zur Endversion sicher noch zig mal modifiziert wird.
Um der Sache auch einen praktischen Nutzen zu verleihen, nahm ich einen kleinen Teil des Gesammtkunstwerkes und ergänzte diesen um ein paar Dateifunktionen.
Das Ergebnis haben Sie soeben downgeladen (oder downgeloadet ?).

Die Idee
besteht darin den Datenstrom zunächst inhomogen zu machen, weil homogene Daten (z.B. eine Gesprächspause) möglicherweise einen Ansatzpunkt für statistische Verfahren bilden könnten.
Die eigentliche Verschlüsselung besorgen dann 8 symmetrisch verkoppelte, dreidimensionale, Zelluläre Automaten. Das Paßwort schaltet zum einen die Steuerleitungen um, über welche die Z.A. miteinander kommunizieren, zerstört also die Symmetrie, zum anderen erzeuge ich daraus die Regeln, welche die einzelnen Z.A. auf den Datenstrom anwenden. Die Codierung erfolgt also nicht durch Verknüpfung der Daten mit dem Paßwort, sondern durch Verknüpfung des Datenfeldes mit sich selbst, wobei die Verknüpfungsanweisung eine Funktion des Paßwortes ist und mit jedem Takt wechselt. Die interne Paßwortlänge beträgt 256 Zeichen, die Rekursionstiefe ist nicht eindeutig bestimmbar, da sie vom Paßwort abhängt und für jeden Z.A. individuell ist .
Ein öffentlicher Schlüssel ist weder möglich noch vorgesehen (bereits der Begriff ”Öffentlicher Schlüssel” ist unsinnig und bezeichnet bestenfalls einen Schlüssel unter einer Fußmatte).
Aus den Ausgangsdaten wird ein deterministisches Chaos erzeugt, daher ist ein codiertes File nicht komprimierbar.
In 330 MB großen Testdateien findet sich eine beliebige 3 stellige Zeichenkombination im Schnitt 20 mal wieder (Mittel aus 100 Testläufen mit unterschiedlichen Daten).
In weißem Rauschen (z.B. Schnee auf dem Bildschirm) nach sich wiederholenden Mustern zu suchen, dürfte von gleichem Erfolg gekrönt sein.
Die Schaltung benötigt je nach Bauteileaufwand ein oder zwei Taktzyklen, um ein Datum zu (de)codieren.
Eine mit 10 MHz betriebene HCTTL Testschaltung schaufelt bei einer Wortbreite von 8 Bit knapp 10MB/s.
Geplant ist eine PLD-Version mit 16 Z.A. und 60 - 80 MHz.

Dieses Programm
enthält nur den vorbereitenden Schritt zum Inhomogenisieren des Datenfeldes.
Dieser ist zwar recht simpel und war eigentlich gar nicht zum Verschlüsseln gedacht, liefert jedoch, ein wenig modifiziert, auch schon recht brauchbare Ergebnisse .
Ohne die rechenintensiven Z.A. erreicht CRYPT auch schon stolze 300 KB/s.
Das es nicht mehr ist, liegt zum einen daran, daß ich kein Assemblercrack bin, zum anderen an der seriellen Abarbeitung der Instruktionen im PC, welche von der CRYPT-Hardware parallel ausgeführt werden.
Um zum Beispiel die geraden und ungeraden Bits eines Bytes zu vertauschen, müssen diese erst maskiert, bzw. ausgeUNDet, schließlich rotiert und wieder zusammengeODERt werden.
Solcherlei Treiben kostet natürlich allerhand Maschinenzyklen.
Eine spezielle Hardware für die gleiche Operation besteht aus 8 parallelen Leitungen, von denen jeweils 2 vertauscht sind; diese einfache Schaltung ist millionenmal schneller als jeder teure PC.

Trotz light-Ausführung halte ich das Knacken des Algorithmuschens für eine abendfüllende Beschäftigung (in Polarnächten).
Beim Lösungsversuch hatte ich bisher immer mehr linear unabhängige Variablen als Gleichungen.
Nun ist Irren aber menschlich, schließlich bin ich kein Mathematiker.
Nichtsdestotrotz biete ich demjenigen **200 DM,** der mir als erstes verrät, was in CRYPDEMO.CRP steckt.
Der Gewinner kann sich dann mal an einem File versuchen, welches mit dem Originalalgorithmus verschlüsselt wurde (damit ich mein Geld zurückgewinnen kann).
Ich bitte um Verständnis dafür, daß ich diesen vorerst nicht als Software herausrücke.
Für die anderen gibt es als Trostpreis einen Platz in der ersten Reihe, wenn Crypto den Reichstag verschlüsselt.

Dieses Programm ist eine absolute Beta, Sie sind somit zum Betatester degradiert.
Es wurde entwickelt und gründlich getestet unter MS DOS 7.0 (Testrelease Januar 95).
Schwierigkeiten traten nur mit einem alten Maustreiber (Version 6.2) auf (Ersatzmaustreiber liegt bei).
CRYPT 1.01 läuft nun auch anstandslos unter Windows 95 (ebenfalls Januar 95).
Wie sich das Programm in anderen Multitaskingumgebungen und Netzwerken verhält, kann ich nicht vorhersagen (würde mich aber interessieren).
Auf jeden Fall lehne ich jede Verantwortung für irgendwelche Schäden an Sachen und Personen ab !!!

Bitte teilen Sie mir Ihre Erfahrungen mit, so kann verhindert werden, daß auch anderen Leuten der Computer abbrennt.

Verschlüsseln :

crypt /ver Quelldatei Zieldatei Paßwort [-j -d -s]

Die Parameter -j, -d, -l sind optional und haben folgende Bedeutung :
-j unterläßt überflüssige Fragen,
-d löscht die Quelldatei unwiederbringlich,
-s erzeugt eine selbstentschlüsselnde Datei.

Entschlüsseln :

crypt /ent Quelldatei Paßwort.

Eine selbstentschlüsselnde Datei wird aufgerufen mit : Dateiname Paßwort.

Ein gültiges Paßwort kann maximal 80 Zeichen lang sein und sollte aus Sicherheitsgründen nicht kürzer als 6 Zeichen gewählt werden.

Wenn ich aufgrund Ihrer Zuschriften den Eindruck bekomme, daß ein gewisses Interesse an CRYPT besteht, so wird es eine Version 2.0 mit grafischer Oberfläche geben.
In dieser werde ich nicht nur versuchen, Ihre Verbesserungsvorschläge zu berücksichtigen, sondern auch eine Fehlererkennung/korrektur und eine Verify-Funktion implementieren.
Bei dieser Beta rate ich zu VERIFY ON, wenn nämlich in der verschlüsselten Datei auch nur ein Bit verändert wird, ist ein korrektes Entschlüsseln völlig unmöglich.
Die Version 1 kann nur jeweils eine (deswegen die 1) Datei verschlüsseln.
Um mehrere Dateien in ein CRYPT-File zu packen, kann man diese vorher komprimieren.
Dies bietet sich schon deshalb an, weil wie schon erwähnt, die von CRYPT erzeugten Dateien nicht komprimierbar sind (ARJ erzeugte in einem Versuch statt einer kleineren Datei eine größere).

Dies ist zwar Freeware, doch kostenlos heißt nicht umsonst.
Ich würde mich sehr freuen, von Ihnen Verbesserungsvorschläge, Kritiken, oder einfach nur ein Statement zur (Un)Nützlichkeit des Programmes zu erhalten.

EMail : CompuServe 100447.3272

Jetzt schon vielen Dank, und Bitte um Entschuldigung für das schlechte Programm, aber schließlich bin ich Elektroniker und nicht Programmierer.

PS.
Zum Schluß möchte ich mich noch bedanken bei der Redaktion der C´t für den hervorragenden Artikel in der

Ausgabe vom Juli 95 auf Seite 72; weiter so!
Großer Dank sei auch geschuldet dem Herrn Kanther, welchem ich die Idee zu diesem Projekt verdanke.
Danke.

H.J. Grauer