ANHANG:

Der »Solitaire«-Verschlüsselungsalgorithmus

Bruce Schneier

In Neal Stephensons Roman *Cryptonomicon* beschreibt Enoch Root Randy Waterhouse ein Kryptosystem mit der Codebezeichnung »Pontifex« und verrät ihm später, dass die einzelnen Schritte des Algorithmus dazu gedacht sind, mithilfe eines Kartenspiels ausgeführt zu werden. Im weiteren Verlauf der Handlung tauschen die beiden Männer mehrere nach diesem System verschlüsselte Botschaften aus. Das System heißt »Solitaire« (die in dem Roman verwendete Codebezeichnung »Pontifex« soll zunächst davon ablenken, dass es auf einem Kartenspiel basiert) und ich habe es entwickelt, um es Agenten zu ermöglichen, sicher zu kommunizieren, ohne auf elektronische Geräte angewiesen zu sein oder verräterisches Werkzeug mit sich herumtragen zu müssen. Ein Agent könnte in eine Situation geraten, in der er einfach keinen Zugang zu einem Computer hat oder womöglich Verdacht erregt, wenn er Werkzeuge zur geheimen Nachrichtenübermittlung bei sich hat. Was aber gibt es Harmloseres als ein Spiel Karten?

Seine Sicherheit gewinnt Solitaire durch die Zufälligkeit, die ein Stapel gemischter Karten an sich hat. Durch die Manipulation dieses Stapels kann jemand, der eine geheime Nachricht verschicken will, eine »zufällige« Buchstabenfolge erzeugen, die er dann mit seiner Nachricht kombiniert. Solitaire kann zwar auch auf einem Computer simuliert werden, ist aber für die Ausführung von Hand gedacht.

Solitaire mag ein einfaches System sein; von der Sicherheit her ist es jedoch für Hightech-Standards ausgelegt. Ich habe Solitaire so entworfen, dass es sogar gegen bestausgestattete militärische Gegner mit den größten Computern und den gewieftesten Kryptoanalytikern gewappnet ist. Natürlich gibt es keine Garantie dafür, dass nicht irgendjemand einen cleveren Angriff auf Solitaire startet (siehe Updates auf meiner Homepage), aber der Algorithmus ist auf jeden Fall besser als sämtliche Papier-und-Bleistift-Codes, die ich bisher gesehen habe.

Allerdings braucht das Verfahren seine Zeit. Es kann einen ganzen Abend dauern, bis man eine Nachricht von mittlerer Länge ver- oder entschlüsselt hat. In seinem Buch *Kahn on Codes* beschreibt David Kahn einen realen Papier-und-Bleistift-Code, den ein sowjetischer Spion benutzt. Mit dem sowjetischen Algorithmus braucht man zum Entschlüsseln einer Nachricht etwa genau so lang wie mit Solitaire.

Verschlüsseln mit Solitaire

Solitaire ist eine Stromchiffrierung im Ausgabe-Rückkopplungs-Modus, auch »Schlüsselgenerator« genannt (die amerikanischen Militärs benutzen die Abkürzung KG für *key-generator*). Der Grundgedanke besteht darin, dass Solitaire einen auch als »Schlüsselstrom« bezeichneten Strom von Zahlen zwischen 1 und 26 erzeugt. Zum Verschlüsseln erzeugt man dieselbe Anzahl von Schlüsselstrombuchstaben, wie der Klartext Buchstaben enthält. Dann addiert man sie modulo 26 nacheinander zu den Buchstaben des Klartextes und stellt so den Chiffretext her. Zum Entschlüsseln erzeugt man denselben Schlüsselstrom und subtrahiert ihn modulo 26 vom Chiffretext, um den Klartext wiederherzustellen.

Die erste in Stephensons Roman erwähnte Solitaire-Nachricht, »PC NICHT BENUTZEN«, wird zum Beispiel folgendermaßen verschlüsselt:

1. Man teilt den Klartext in Gruppen zu jeweils fünf Buchstaben auf. (Diese Fünfbuchstabengruppen haben nichts Magisches an sich; sie entsprechen einfach einer Tradition.) Mögliche Leerstellen der letzten Gruppe werden mit X aufgefüllt. Heißt also die Nachricht »PC NICHT BENUTZEN«, so lautet der Klartext:

   P C N I C H T B E N U T Z E N

2. Mithilfe von Solitaire erzeugt man fünfzehn Schlüsselstrombuchstaben. (Einzelheiten siehe unten.) Nehmen wir an, sie heißen:

   K D W K T R X L X C O O O S I

3. Nun wandelt man die Buchstaben der Klartextnachricht in Zahlen um: $A = 1$, $B = 2$, etc.:

   16 3 14 9 3 8 20 2 5 14 21 20 26 5 14

4. Mit den Schlüsselstrombuchstaben verfährt man ebenso:

   11 4 23 11 20 18 24 12 24 3 15 15 15 19 9

5. Jetzt addiert man den Klartextzahlenstrom modulo 26 zu den Schlüsselstromzahlen. (Das bedeutet, wenn eine Summe größer als

26 ist, muss man davon 26 subtrahieren.) Zum Beispiel 1 + 1 = 2, 26 + 1 = 27 und 27 – 26 = 1..., also 26 + 1 = 1.

1 7 11 20 23 26 18 14 3 17 10 9 15 24 23

6. Nun werden die Zahlen wieder in Buchstaben umgewandelt:

A G K T W Z R N C Q J I O X W

Wenn man die Methode richtig gut beherrscht, kann man lernen, Buchstaben wie die von Schritt 1 und 2 im Kopf zu addieren. Man muss es nur üben. Sich $A + A = B$ zu merken, ist nicht weiter schwer, $T + Q = K$ dagegen schon eher.

Entschlüsseln mit Solitaire

Das Grundprinzip besteht darin, dass der Empfänger denselben Schlüsselstrom erzeugt und dann die Schlüsselstrombuchstaben von den Chiffretextbuchstaben subtrahiert.

1. Dazu nimmt man die Chiffretextnachricht und teilt sie in Fünfbuchstabengruppen (jetzt müsste sie diese Form bereits haben).

A G K T W Z R N C Q J I O X W

2. Mithilfe von Solitaire erzeugt man fünfzehn Schlüsselstrombuchstaben. Wenn der Empfänger denselben Schlüssel benutzt wie der Sender, sind die Schlüsselstrombuchstaben auch dieselben:

K D W K T R X L X C O O O S I

3. Nun wandelt man die Buchstaben der Chiffretextnachricht in Zahlen um:

1 7 11 20 23 26 18 14 3 17 10 9 15 24 23

4. Die Schlüsselstrombuchstaben werden entsprechend umgewandelt:

11 4 23 11 20 18 24 12 24 3 15 15 15 19 9

5. Jetzt subtrahiert man modulo 26 die Schlüsselstromzahlen von den Chiffretextzahlen. Beispiel: 22 – 1 = 21, 1 – 22 = 5. (Das ist nicht schwer. Wenn die erste Zahl kleiner ist als die zweite, addiert man vor der Subtraktion 26 zu der ersten Zahl. Aus 1 – 22 wird also 27 – 22 = 5.)

16 3 14 9 3 8 20 2 5 14 21 20 26 5 14

6. Zum Schluss werden die Zahlen wieder in Buchstaben umgewandelt:

P C N I C H T B E N U T Z E N

Beim Entschlüsseln verfährt man genau wie beim Verschlüsseln, nur muss man den Schlüsselstrom von der Chiffretextnachricht subtrahieren.

Die Erzeugung der Schlüsselstrombuchstaben

Das ist das Herz von Solitaire. Die oben beschriebene Ver- und Entschlüsselung funktioniert mit jeder Stromchiffrierung im Ausgabe-Rückkopplungs-Modus. In diesem Abschnitt geht es nun um die spezielle Funktionsweise von Solitaire.

Bei Solitaire erzeugt man den Schlüsselstrom mithilfe eines Kartenspiels. Ein Spiel mit 54 Karten (man darf die Joker nicht vergessen) kann man sich als eine 54 Elemente umfassende Permutation vorstellen. Es gibt 54! oder ungefähr $2{,}31 \times 10^{71}$ verschiedene Möglichkeiten, ein solches Kartenspiel anzuordnen. Und was noch besser ist, ein Kartenspiel besteht (ohne die Joker) aus 52 Karten und das Alphabet aus 26 Buchstaben. Einen solchen Zufall darf man einfach nicht ignorieren!

Um für Solitaire brauchbar zu sein, muss ein Kartenspiel alle 52 Karten und zwei Joker enthalten. Die Joker müssen sich irgendwie voneinander unterscheiden. (Das ist so üblich. Bei dem Spiel, das ich während des Schreibens benutze, tragen die Joker Sterne: der eine einen kleinen und der andere einen großen.) Den einen bezeichnet man als Joker A und den andern als Joker B. In der Regel ist auf beiden Jokern ein und dasselbe grafische Element in unterschiedlicher Größe zu sehen. Nennen wir den mit dem größeren Element Joker »B«. Wenn einem das leichter fällt, kann man auch groß »A« und »B« auf die beiden Joker schreiben; allerdings muss man dann für den Fall, dass die Geheimpolizei einen schnappt, eine gute Erklärung parat haben.

Zur Vorbereitung nimmt man den Kartenstapel mit der Bildseite nach oben zur Hand. Dann ordnet man die Karten in der Ausgangskonfiguration, dem eigentlichen Schlüssel, an. (Über den Schlüssel selbst spreche ich später, das ist etwas anderes als der Schlüsselstrom.) Jetzt kann man anfangen, eine Reihe von Schlüsselstrombuchstaben zu erzeugen.

Und das geht so:

1. Man sucht Joker A und schiebt ihn unter die darunter liegende Karte (vertauscht ihn also mit dieser). Ist der Joker die letzte Karte im Stapel, legt man ihn unter die oberste Karte.

2. Man sucht Joker B und schiebt ihn zwei Karten weiter unten wieder in den Stapel. Ist Joker B die letzte Karte, kommt er unter der zweiten von oben wieder in den Stoß. Ist er die vorletzte Karte, schiebt man ihn gleich unter die oberste. (Im Grunde muss man sich den

Kartenstapel als Schleife vorstellen, dann ergibt sich alles Weitere von selbst.)

Diese beiden Schritte müssen unbedingt in genau dieser Reihenfolge durchgeführt werden. Es ist verlockend, nachlässig zu werden und die Joker jeweils dann zu bewegen, wenn man sie findet. Das funktioniert aber nur, wenn sie nicht sehr nah beieinander liegen.

Sieht der Stoß also vor Schritt 1 so aus:

3 A B 8 9

sollte er nach Schritt 2 so aussehen:

3 A 8 B 9

Wenn man unsicher ist, sollte man immer Joker A vor Joker B bewegen. Und besonders aufpassen, wenn die Joker zuunterst im Stapel liegen.

3. Man führt einen dreifachen Abhebevorgang durch, das heißt, man vertauscht die Karten über dem ersten Joker mit denen unter dem zweiten. Lagen die Karten anfangs in dieser Reihenfolge:

2 4 6 B 4 8 7 1 A 3 9

sind sie nach dem dreifachen Abhebevorgang so angeordnet:

3 9 B 4 8 7 1 A 2 4 6

In diesem Fall ist der »erste« beziehungsweise »zweite« Joker derjenige, der am nächsten beziehungsweise weitesten von der obersten Karte entfernt liegt. Die Bezeichnungen »A« und »B« kommen bei diesem Schritt nicht zum Tragen.

Es ist wichtig, dass die Joker selbst und die Karten dazwischen nicht bewegt werden; die anderen Karten bewegen sich um sie herum. Das kann man leicht in der Hand machen. Ergibt es sich, dass einer der drei Abschnitte keine Karten enthält (entweder weil die Joker übereinander liegen oder einer die oberste oder unterste Karte ist), verfährt man mit ihm trotzdem wie mit einem normalen Abschnitt.

4. Jetzt führt man einen kombinierten Zähl- und Abhebevorgang durch. Dazu schaut man sich die unterste Karte an und ordnet ihr eine Zahl zwischen 1 und 53 zu. (Dabei verfährt man nach der Farbfolge aus dem Bridge: Kreuz, Karo, Herz und Pik. Handelt es sich um eine Kreuzkarte, gilt ihr eigener Wert. Ist es Karo, gilt ihr eigener Wert plus 13. Bei einer Herzkarte gilt der Wert plus 26. Ist es eine Pikkarte, gilt ihr eigener Wert plus 39. Jeder Joker zählt 53.) Um diesen Wert zählt man die Karten von oben nach unten durch. (Normalerweise zähle ich immer wieder von 1 bis 13; das ist einfacher, als jedes Mal hohe Zahlen durchzuzählen.) Nach der Karte, bis zu der man gezählt

hat, hebt man ab, wobei die unterste Karte zuunterst liegen bleibt. Sah der Stoß vorher so aus:

```
7 . . . Karten . . . 4 5 . . . Karten . .
. 8 9
```

und die neunte Karte war die 4, führt das Abheben zu folgender Anordnung:

```
5 . . . Karten . . . 8 7 . . . Karten . .
. 4 9
```

Die letzte Karte bleibt in ihrer Position liegen, um den Schritt umkehrbar zu machen. Das ist wichtig für die mathematische Analyse seiner Sicherheit.

5. Jetzt sucht man die erste Ausgabekarte. Dazu schaut man sich die oberste Karte an und wandelt sie in der zuvor beschriebenen Weise in eine Zahl zwischen 1 und 53 um. So viele Karten zählt man, beginnend mit der obersten, ab. Die Karte unter derjenigen, bis zu der man gezählt hat, schreibt man auf ein Stück Papier. (Falls man einen Joker erwischt hat, schreibt man nichts auf und fängt wieder bei Schritt 1 an.) Das ist die erste Ausgabekarte. Man beachte, dass dieser Schritt den Zustand des Kartenspiels nicht verändert.

6. Diese Karte wandelt man in eine Zahl um. Wie zuvor richtet man sich auch hier nach der Farbfolge aus dem Bridge, nämlich von der niedrigsten zur höchsten Farbe Kreuz, Karo, Herz und Pik. Folglich gelten für Kreuzass bis Kreuzkönig die Zahlenwerte 1 bis 13, für Karoass bis Karokönig 14 bis 26, für Herzass bis Herzkönig wieder 1 bis 13 und für Pikass bis Pikkönig 14 bis 26.

Das ist Solitaire. Damit kann man so viele Schlüsselstromzahlen erzeugen, wie man braucht.

Ich weiß, dass es in Kartenspielen regionale Unterschiede gibt. Im Großen und Ganzen kommt es nicht darauf an, welche Farbfolge man wählt oder wie man die Karten in Zahlen umwandelt. Worauf es ankommt, ist, dass Sender und Empfänger sich auf die Regeln einigen. Tun sie das nicht, können sie nicht miteinander kommunizieren.

Das Kartenspiel zum Schlüssel machen

Solitaire ist nur so gut wie der Schlüssel. Die einfachste Art, es zu knacken, besteht also darin herauszufinden, welchen Schlüssel Sender und Empfänger benutzen. Hat man keinen guten Schlüssel, kann man alles andere vergessen. Im Folgenden sind ein paar Möglichkeiten zum Austauschen von Schlüsseln dargestellt.

1. Man mischt das Kartenspiel. Ein Zufallsschlüssel ist der beste. Einer der beiden Kommunikationspartner kann einen Stapel beliebig mischen und dann einen anderen Satz Karten in derselben Reihenfolge anordnen. Den einen bekommt der Sender und den anderen der Empfänger. Da die meisten Leute das Mischen nicht besonders gut beherrschen, sollte man die Karten mindestens zehnmal mischen und statt eines nagelneuen Spiels möglichst ein bereits benutztes verwenden. Es ist von Vorteil, ein weiteres Kartenspiel in der Schlüsselanordnung bereitzuhalten, da man sonst, falls man einen Fehler macht, nicht mehr in der Lage ist, die Nachricht zu entschlüsseln. Im Übrigen darf man nie vergessen, dass der Schlüssel gefährdet ist, solange es ihn gibt; die Geheimpolizei könnte das Kartenspiel finden und die Reihenfolge der Karten aufschreiben.

2. Man verwendet die Reihenfolge einer ausgeteilten Partie Bridge. Die Beschreibung einer Bridgerunde mit dem Blatt der vier Spieler, wie man sie in einer Zeitung oder einem Bridgebuch finden könnte, bildet ungefähr einen 95-Bit-Schlüssel. Wenn die Kommunikationspartner sich darauf einigen können, in welche Anordnung des Kartenspiels sie diese Beschreibung umwandeln und wie sie dabei die Joker setzen (vielleicht nach den ersten beiden Karten, die in der Diskussion des Spiels erwähnt werden), kann das funktionieren. Man muss sich allerdings immer bewusst sein, dass die Geheimpolizei womöglich die Bridge-Ecke findet und daraus die Reihenfolge der Karten ableitet. Man kann versuchen, eine dauerhaft gültige Abmachung darüber zu treffen, welche Bridge-Ecke man verwenden will, zum Beispiel »Nimm die Bridge-Ecke deiner Lokalzeitung von dem Tag, an dem du die Nachricht verschlüsselst« oder so ähnlich. Oder man durchsucht die Website der *New York Times* nach bestimmten Schlüsselwörtern und benutzt die Bridge-Ecke der Ausgabe, in der der Artikel mit genau diesen Wörtern erschienen ist. Wird die Liste der Schlüsselwörter gefunden oder abgefangen, wird man sie für eine Passphrase halten. Man sollte auf jeden Fall eine eigene Vereinbarung treffen, denn auch die Geheimpolizei liest Neal Stephensons Bücher.

3. Man ordnet das Kartenspiel anhand einer Passphrase. Bei dieser Methode dient der Solitaire-Algorithmus dazu, das Kartenspiel in eine Startanordnung zu bringen. Sender und Empfänger haben dieselbe Passphrase (zum Beispiel GEHEIMSCHLÜSSEL). Am Anfang liegen die Karten in einer bestimmten Reihenfolge, von der niedrigsten zur höchsten in der Farbfolge des Bridge. Nun beginnt man mit

den einzelnen Solitaire-Schritten. Anstelle von Schritt 5 führt man einen weiteren kombinierten Zähl- und Abhebevorgang durch, der auf dem ersten Buchstaben der Passphrase (in unserem Beispiel 7) beruht. (Man darf nicht vergessen, die oberste Karte unmittelbar über der untersten wieder in den Stapel zu stecken.) Das macht man für jeden Buchstaben einmal. Mithilfe von zwei weiteren Buchstaben bestimmt man die Lage der Joker. Dabei muss man allerdings bedenken, dass beispielsweise im Standardenglisch die Zufälligkeit jedes Buchstabens nur etwa 1,4 Bit beträgt. Daher sollte man zur Sicherheit eine Passphrase mit wenigstens 80 Buchstaben wählen; ich empfehle sogar mindestens 120 Buchstaben. (Tut mir Leid, aber mit einem kürzeren Schlüssel erreicht man keine wirkliche Sicherheit.)

Ausgabebeispiele

Im Folgenden sind beispielhaft einige Daten genannt, anhand deren man seine Solitaire-Fertigkeiten üben kann:

Beispiel 1: Man beginnt mit einem nicht als Schlüssel angeordneten Kartenspiel in der Reihenfolge Kreuzass bis Kreuzkönig, Karoass bis Karokönig, Herzass bis Herzkönig, Pikass bis Pikkönig, Joker A, Joker B (das kann man sich als 1–52, A, B vorstellen). Die ersten zehn Ausgabezahlen sind:

```
4 49 10  (53)  24 8 51 44 6 4 33
```

Die 53 wird natürlich übersprungen. Ich habe sie hier nur zur Verdeutlichung eingefügt. Lautet der Klartext:

```
A A A A A   A A A A A
```

dann heißt der Chiffretext:

```
E X K Y I   Z S G E H
```

Beispiel 2: Benutzt man die Methode 3 mit dem Schlüssel »FOO« zur Schlüsselanordnung, lauten die ersten fünfzehn Ausgabezahlen:

```
8 19 7 25 20  (53)  9 8 22 32 43 5 26 17
(53)  38 48
```

Besteht der Klartext aus lauter Ass, lautet der Chiffretext:

```
I T H Z U   J I W G R   F A R M W
```

Beispiel 3: Benutzt man die Methode 3 mit dem Schlüssel »CRYPTONOMICON«, lautet die Nachricht »SOLITAIRE« als Chiffretext:

```
K I R A K   S F J A N
```

Natürlich sollte man längere Schlüssel verwenden. Diese Beispiele sind nur zum Ausprobieren gedacht. Auf der unten genannten Website gibt es noch mehr; außerdem kann man sich mithilfe des PERL-Skripts aus dem Buch eigene Beispiele ausdenken.

Sicherheit durch Verschleierung

Solitaire ist von seiner Struktur her sicher, selbst wenn der Gegner weiß, wie der Algorithmus funktioniert. Ich bin davon ausgegangen, dass *Cryptonomicon* ein Bestseller wird und dass man es überall wird bekommen können. Ich nehme an, dass die NSA und alle anderen den Algorithmus studieren und Ausschau danach halten werden. Ich gehe davon aus, dass im Schlüssel das ganze Geheimnis liegt.

Deshalb ist es auch so wichtig, den Schlüssel geheim zu halten. Bewahrt man ein Kartenspiel an einem sicheren Ort auf, sollte man davon ausgehen, dass der Gegner zumindest den Verdacht hegen wird, dass man mit Solitaire arbeitet. Hat man in seinem Banksafe eine Zeitungsseite mit der Bridge-Ecke liegen, muss man damit rechnen, dass man bei dem einen oder anderen Argwohn erregt. Ist irgendeine Gruppe dafür bekannt, dass sie diesen Algorithmus verwendet, muss man darauf gefasst sein, dass die Geheimpolizei eine Datenbank mit Bridge-Ecken anlegt, die sie zu Angriffsversuchen nutzt. Solitaire ist aber selbst dann stark, wenn der Gegner weiß, dass man es verwendet, und ein einfaches Kartenspiel ist immer noch unverfänglicher als ein Verschlüsselungsprogramm, das auf dem Laptop läuft; den gesunden Menschenverstand kann der Algorithmus allerdings nicht ersetzen.

Benutzungshinweise

Das oberste Gebot jeglicher Stromchiffrierung im Ausgabe-Rückkopplungs-Modus lautet, dass man niemals zwei verschiedene Nachrichten mit demselben Schlüssel chiffrieren darf. Ich wiederhole: ZWEI VERSCHIEDENE NACHRICHTEN DÜRFEN NIE MIT DEMSELBEN SCHLÜSSEL CHIFFRIERT WERDEN. Tut man es doch, setzt man die Sicherheit des Systems aufs Spiel. Und zwar aus folgendem Grund: Nehmen wir an, man hat zwei Chiffretextströme, $A + K$ und $B + K$, und man subtrahiert den einen vom anderen, dann erhält man $(A + K) - (B + K) = A + K - B - K = A - B$. Das sind zwei miteinander kombinierte Klartextströme, die im Handumdrehen geknackt sind. Eins ist sonnenklar: Wir selbst sind vielleicht nicht in der

Lage, A und B aus der Gleichung A – B wiederherzustellen, ein professioneller Kryptoanalytiker dagegen schon. Deshalb noch einmal die Mahnung: Zwei verschiedene Nachrichten dürfen nie mit demselben Schlüssel chiffriert werden.

Fasse dich kurz, heißt die Devise. Dieser Algorithmus ist für kurze Nachrichten von ein paar tausend Buchstaben gedacht. Hat man einen Roman mit 100 000 Wörtern zu verschlüsseln, sollte man lieber einen Computer-Algorithmus verwenden. Es ist von Vorteil, Steno, Abkürzungen und Slang in die Nachrichten einzubauen. Für Geschwätzigkeit ist hier kein Platz.

Um maximale Sicherheit zu erreichen, sollte man versuchen, alles im Kopf zu machen. Wenn die Geheimpolizei bereits dabei ist, die Haustür aufzubrechen, sollte man in aller Ruhe das Kartenspiel mischen. (Man darf es allerdings nicht einfach in die Luft werfen; es ist erstaunlich, wie viel von der ursprünglichen Reihenfolge dabei erhalten bleibt!) Falls man ein zweites Kartenspiel in Schlüsselanordnung hat, darf man nicht vergessen, auch das zu mischen.

Sicherheitsanalyse

Sie ist sehr umfangreich, aber viel zu kompliziert, um sie hier wiederzugeben. Mehr dazu unter

http://www.counterpane.com

Weiterführende Literatur

Mein eigenes Buch *Angewandte Kryptographie*, Addison-Wesley 1999, empfehle ich als solide Grundlage. Dann sollte man David Kahn, *The Codebreakers*, Scribner 1996, lesen. Daneben gibt es verschiedene Bücher über Computerkryptographie und ein paar weitere über manuelle Kryptographie. Man kann auch unter http://www.counterpane.com/crypto-gram oder durch Zusenden einer Blanko-E-Mail an subscribe@chaparraltree.com kostenlos meinen Newsletter abonnieren. Es macht Spaß, sich damit zu beschäftigen. Viel Glück!