J. F. Byrne – Chaocipher

So funktioniert Chaocipher

Im Mai 2010 erhielt das National Cryptologic Museum die Hinterlassenschaften eines gewissen John F. Byrne von seiner Familie überreicht. So wurde eines der großen Rätsel der Kryptologie endlich gelöst: Der *Chaocipher*-Algorithmus.

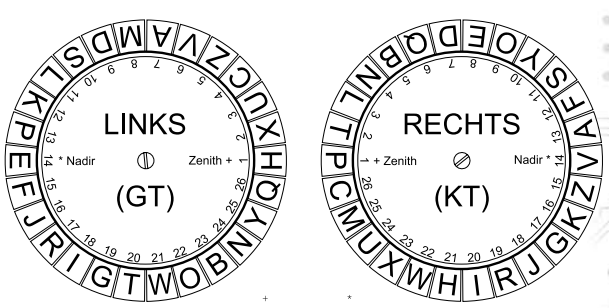
Chaocipher an sich ist nichts Neues: J. F. Byrne entwickelte sein Verschlüsselungssystem bereits im Jahre 1918. Sein Wunsch war es, ein einfach zu benutzendes aber nicht zu knackendes Verfahren zu schaffen, und er war überzeugt davon, das mit *Chaocipher* auch geschafft zu haben. Seine Versuche, das US Signal Corps, das für die Kommunikationssysteme der Streitkräfte verantwortlich war, von seinem Vorhaben zu überzeugen, scheiterten jedoch, denn er hielt den eigentlichen Algorithmus, der hinter *Chaocipher* steht, geheim. (Heute würde man das als „*Security by Obscurity*“ bezeichnen, denn schon Ende des 19. Jahrhunderts entwickelte Auguste Kerckhoffs seine kryptologischen Prinzipien, von denen das zweite besagt, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht - und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus.)

Über die Jahre lobte Byrne Geldpreise aus für denjenigen, der *Chaocipher* knacken könne, doch scheint es niemanden zu geben, dem das jemals gelungen war. Erst als Byrnes Familie nach offenbar längeren Verhandlungen bereit war, die zu *Chaocipher* gehörigen Unterlagen an das Cryptologic Museum zu spenden, wurde der Algorithmus bekannt und veröffentlicht.

Überblick

Byrne plante *Chaocipher* wohl als mechanisches System, obwohl er nie die entsprechende Hardware baute. Die Maschine sollte aus zwei Scheiben bestehen, die nebeneinander liegend so miteinander verbunden sind, dass sie sich zusammen drehen. Dreht die eine Scheibe um eine Stelle im Uhrzeigersinn, so dreht sich die andere Scheibe um eine Stelle gegen den Uhrzeigersinn mit. Am Rand jeder Scheibe sind jeweils die 26 Buchstaben angeordnet, in frei veränderbarer Reihenfolge. Das ganze sollte dann so aussehen:

Ausgangsposition



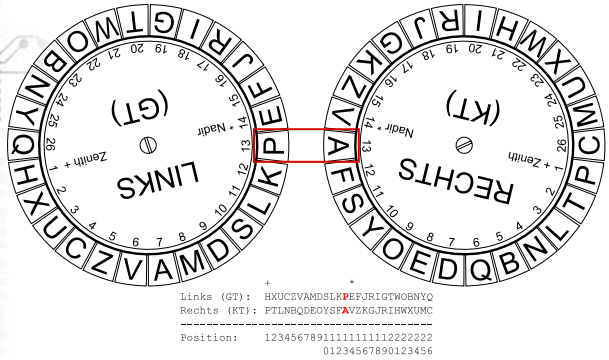
Bei diesem Bild sind die Buchstaben schon mehr oder weniger zufällig angeordnet. Links das Geheimtextalphabet (GT), rechts das Klartextalphabet (KT). Diese ursprüngliche Anordnung der Buchstaben stellt den Schlüssel dar und muss dementsprechend vorher zwischen Sender und Empfänger ausgetauscht werden.

Am Rande jeder Scheibe habe ich die Zahlen 1 bis 26 ergänzt, um die Zuordnung etwas leichter zu machen. Man bemerke: Die Positionen 1 und 14 sind durch Byrne mit den Begriffen *Zenith* und *Nadir* versehen und haben im Algorithmus eine besondere Funktion, wie man sehen wird.

Verschlüsselung eines Buchstabens

Nach Byrne sollte man zur Verschlüsselung eines Buchstabens (z.B. *A*) beide Scheiben so drehen, dass sich der zu verschlüsselnde Buchstabe sowie der dazugehörige Geheimtextbuchstabe (*P*) gegenüberstehen (s. Bild). (Aus diesem Grunde ist es so wichtig, dass beide Scheiben miteinander verbunden sind, s.o.) Man kann natürlich auch die Position des Klartextbuchstaben ablesen ($A=13_{KT}$) und an derselben Position der anderen Scheibe den Geheimtextbuchstaben ablesen ($13_{GT}=P$).

Verschlüsselung *A*

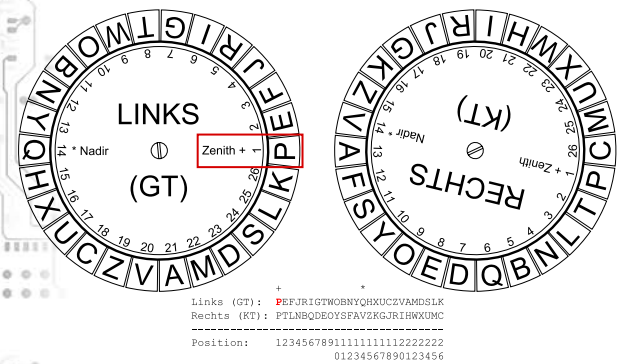


Permutation der Alphabete

Jetzt geht's mit dem Algorithmus los: Dem kontrollierten Durcheinanderwürfeln der Alphabete. Zuerst das Geheimtextalphabet.

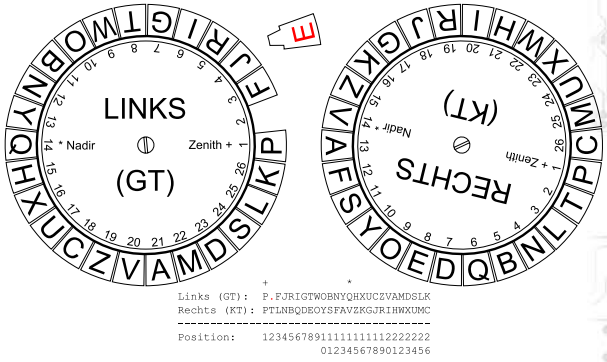
Im ersten Schritt muss das gesamte Geheimtextalphabet verschoben werden, und zwar so, dass der zuletzt gefundene Geheimtextbuchstabe an Position 1 (*Zenith*) zu stehen kommt. Leider kenne ich Byrnes Gedankengänge nicht besonders gut, daher weiß ich nicht, ob er vorsah, dass jeder Buchstabe einzeln entnommen und an der neuen Stelle wieder eingesetzt werden sollte. Meine Variante lautet, dass es einfacher ist, wenn man die entsprechenden Markierungen auf der Scheibe selbst bewegt. Genauso wie man die Buchstaben von den Scheiben lösen und sie wieder einsetzen kann, wäre es möglich, die Markierungen auf der Scheibe beweglich zu gestalten, so dass in diesem ersten Schritt durch eine Drehung der *Zenith* auf dem *P* zu liegen kommt.

Erste Permutation (Links)



Im zweiten Schritt wird der Buchstabe an Position *Zenith+1*, in diesem Fall das *E*, aus der Scheibe entnommen, so

Zweite Permutation (Links)

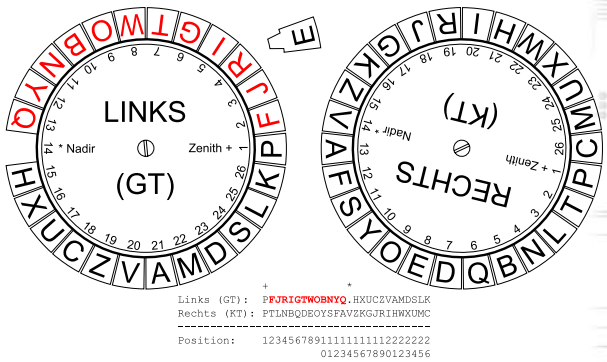


dass eine Lücke entsteht.

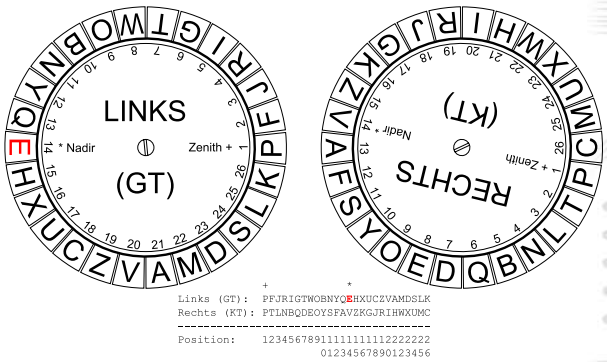
Jetzt rücken alle darauffolgenden Buchstaben von *Zenith+2* bis einschließlich *Nadir* eine Stelle weiter.

Zuletzt wird der soeben entnommene Buchstabe *E* wieder in die neue Lücke eingesetzt.

Dritte Permutation (Links)



Vierte Permutation (Links)



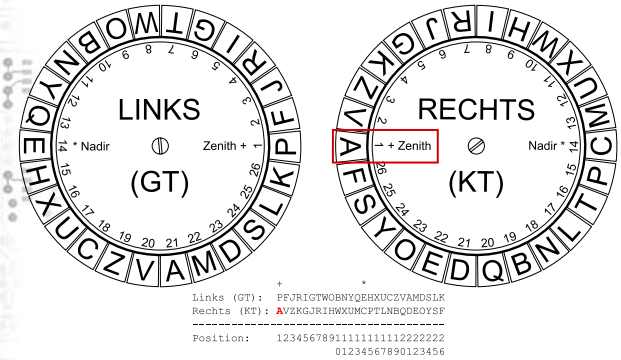
Fertig.

Mit dem Klartextalphabet wird ähnlich verfahren. Der erste Schritt besteht auch hier darin, das gesamte Alphabet so zu verschieben, dass der soeben verschlüsselte Buchstabe (in diesem Fall das *A*) auf Position *Zenith* zu liegen kommt.

Ab hier verläuft die weitere Permutation etwas anders

als beim Geheimtextalphabet, denn nun muss das gesamte Klartextalphabet noch eine Stelle weiter verschoben werden. Da die Angaben „links“ und „rechts“ hier eher verwir-

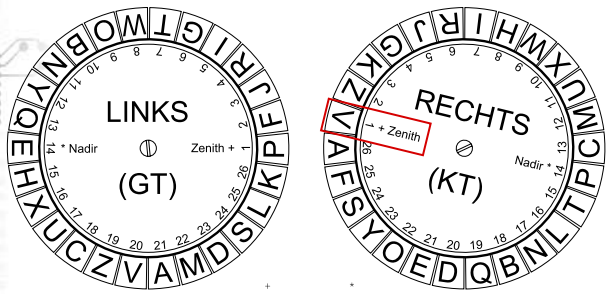
Erste Permutation (Rechts)




```
Links (GT):   PFJRIGTWOBNYQEHXUCZVAMDSLK
Rechts (KT): AVZKGJRIHWXUMCPTLNBQDEOYSF
-------------------------------------
Position:     12345678911111111112222222
                        01234567890123456
```

ren (je nachdem, ob man die Buchstaben bewegt oder die Markierungen oder sogar ohne Scheibe arbeitet und rein mit Buchstaben hantiert), kann man vielleicht vereinfacht sagen, dass der Buchstabe, der vorher an Position 2 war, jetzt auf Position 1 rückt, und der Buchstabe, der vorher an

Zweite Permutation (Rechts)

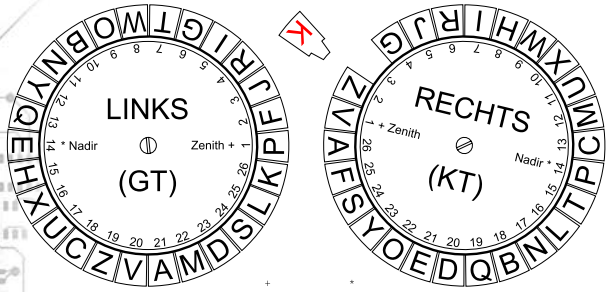



```
Links (GT):   PFJRIGTWOBNYQEHXUCZVAMDSLK
Rechts (KT): VZKGJRIHWXUMCPTLNBQDEOYSFA
-------------------------------------
Position:     12345678911111111112222222
                        01234567890123456
```

Position 1 war, auf Position 26 rückt.

Nun entnimmt man den Buchstaben an Position *Zenith+2* (in diesem Fall das *K*). Wieder entsteht eine Lücke.

Dritte Permutation (Rechts)




```
Links (GT):   PFJRIGTWOBNYQEHXUCZVAMDSLK
Rechts (KT): VZ.GJRIHWXUMCPTLNBQDEOYSFA
-------------------------------------
Position:     12345678911111111112222222
                        01234567890123456
```

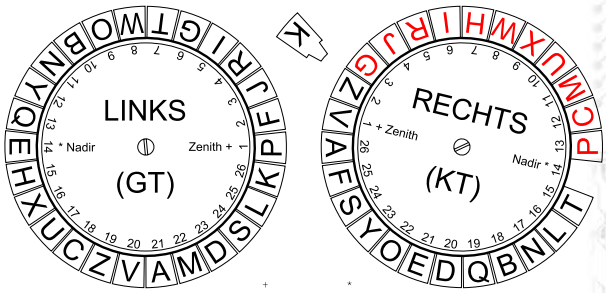
Wieder rücken alle darauffolgenden Buchstaben von *Zenith+3* bis einschließlich *Nadir* eine Stelle weiter.

In die so entstandene Lücke bei Position 14 (*Nadir*) wird der entnommene Buchstabe (*K*) wieder eingesetzt.

Und wieder: Fertig!

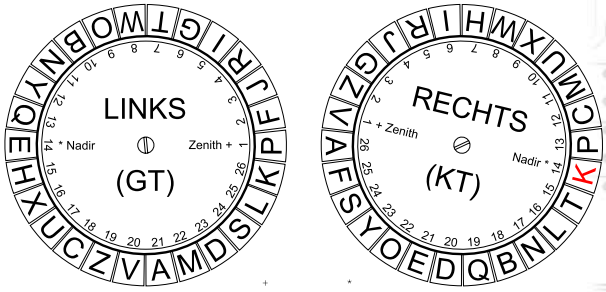
Beide Alphabete sind vollständig permutiert und bereit für die nächste Verschlüsselung. Möchte man z. B. den Buchstaben *N* verschlüsseln, findet man auf der Geheimtextscheibe den dazugehörigen Geheimtextbuchstaben *U*.

Vierte Permutation (Rechts)



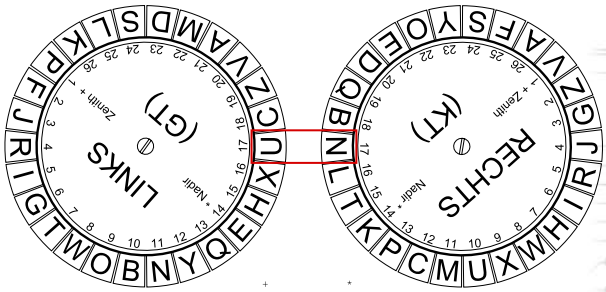

```
Links (GT):   PFJRIGTWOBNYQEHXUCZVAMDSLK
Rechts (KT): VZGJRIHWXUMCP.TLNBQDEOYSFA
-------------------------------------
Position:     12345678911111111112222222
                        01234567890123456
```

Fünfte Permutation (Rechts)




```
Links (GT):   PFJRIGTWOBNYQEHXUCZVAMDSLK
Rechts (KT): VZGJRIHWXUMCPKTLNBQDEOYSFA
-------------------------------------
Position:     12345678911111111112222222
                        01234567890123456
```

Verschlüsselung *N*




```
Links (GT):   PFJRIGTWOBNYQEHXUCZVAMDSLK
Rechts (KT): VZGJRIHWXUMCPKTLNBQDEOYSFA
-------------------------------------
Position:     12345678911111111112222222
                        01234567890123456
```

Entschlüsseln

Das Entschlüsseln einer mit *Chaocipher* verschlüsselten Botschaft funktioniert fast genauso wie das Verschlüsseln. Man sucht zunächst den zu dem ersten *Geheimtextbuchstaben* gehörigen *Klartextbuchstaben*. Dann permutiert man beide Alphabete/Scheiben genauso wie oben beschrieben. Dann sucht man den zu dem nächsten Geheimtextbuchstaben gehörigen Klartextbuchstaben, permutiert wieder, usw.

Einstellen des Schlüssels

Bleibt die Frage, wie die beiden Startalphabete eingestellt werden können. Natürlich können beide Kommunikationspartner im vornherein beide Alphabete zufällig verwürfeln und das dann als Startposition verwenden. Eine andere Möglichkeit besteht darin, die Alphabete mittels eines Codeworts und eines Links/Rechts-Musters einzustellen. Ob das einfacher ist, bleibe dahingestellt, aber diese Variante, die Byrne entwickelt hat, soll hier zumindest erläutert werden.

Benutzt man nur das Codewort, müsste man wie folgt vorgehen: Beide Alphabete werden auf die Standardposition ABCDEFGH... usw. eingestellt. Von dort ausgehend, wird das Codewort, z. B. *HOLZKOPF*, wie oben beschrieben „verschlüsselt“ (die so gefundenen Geheimtextbuchstaben werden nicht benötigt, dienen aber zur Permutation der Alphabete, weil man ja die Buchstaben im ersten Schritt der Permutation so verschieben muss, dass eben dieser Geheimtextbuchstabe an Position 1 steht). Hinterher befinden sich beide Alphabete in genau definierter Anordnung, von der aus man seine eigentliche Botschaft verschlüsseln kann.

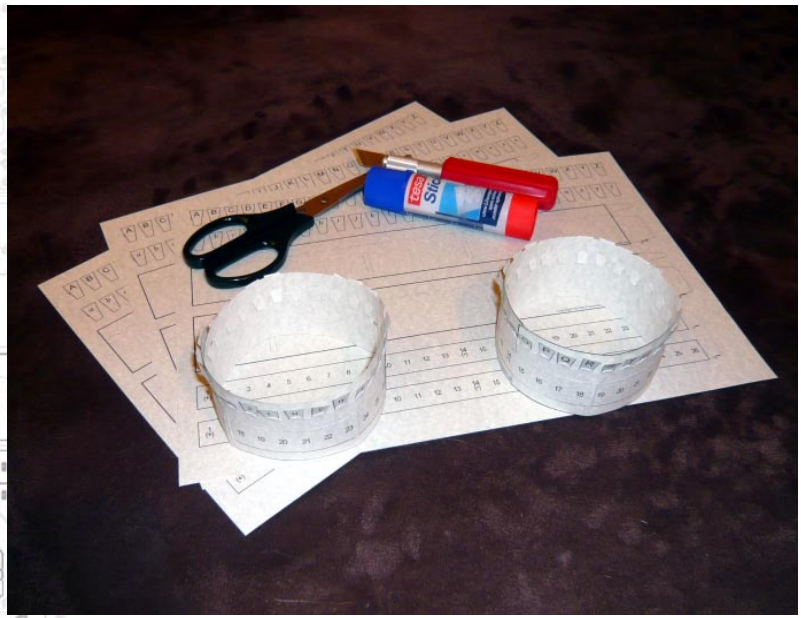
Jetzt zu dem Links/Rechts-Muster. Ein solches könnte lauten *RRLRL*. Zum besseren Verständnis nochmal einen Schritt zurück: Verwendet man nur das Codewort (oder auch bei jedem normalen Verschlüsselungsvorgang) so sucht man den Klartextbuchstaben immer auf der rechten Scheibe (R) und findet den Geheimtextbuchstaben immer auf der linken Scheibe (L). Mit dem Links/Rechts-Muster wird genau dies nun variiert.

Wir kombinieren also Codewort *HOLZKOPF* und Muster *RRLRL*. (Codewort und Muster müssen nicht gleichlang sein, wie wir sehen werden.) Statt dass jeder Buchstabe des Codewortes auf der rechten Scheibe gesucht wird, wird nun durch das Muster vorgegeben, auf welcher Scheibe zu suchen ist. Konkret: Der erste Buchstabe des Codewortes *H* wird bei diesem Beispiel auf der rechten Scheibe (*R*) gesucht. Dann werden die Scheiben wie gehabt permutiert. Der zweite Buchstabe des Codewortes *O* wird ebenfalls auf der rechten Scheibe (*R*) gesucht. Die Scheiben werden permutiert. Der dritte Buchstabe *L* wird auf der linken Scheibe (*L*) gesucht, und so weiter. Hat man das Muster einmal durchlaufen, fängt man wieder von vorne an (das zweite *O* wird also wieder rechts (*R*) gesucht).

Übrigens: Egal, ob man den Buchstaben des Codewortes links oder rechts sucht – beide Scheiben werden immer nach demselben Schema permutiert!

Chaocipher aus Papier

Wie Ihr merkt, hat es der *Chaocipher* Verschlüsselungsalgorithmus mir angetan. Mir das Modell mit den zwei Scheiben nachzubauen, wie Byrne es angedacht hatte, kam für mich jedoch nicht in Frage, weil mir die Bastelei zu mühselig und ich zu faul war. Ich wollte aber nichtsdestoweniger eine Möglichkeit haben, *Chaocipher* in seiner mechanischen Form auszutesten, quasi nach dem Pen-and-Paper-Prinzip.



Es gibt auch die bekannte Enigma-Maschine schon in einer Papierversion. Dort ist es aber ein wenig einfacher, weil die mechanischen Räder als Papierstreifen dargestellt werden. Bei *Chaocipher* müsste man, wenn man die Scheiben aus Papier macht, sie irgendwie drehbar aneinander heften, und müsste darüberhinaus die einzelnen Buchstaben daran befestigen. Schon eine Herausforderung.

Aber ich denke, ich habe eine nicht ganz schlechte Lösung gefunden. Statt zwei Scheiben zu benutzen, verwende ich zwei Hauptringe aus Papier, die als Halter für die sechsundzwanzig Buchstaben dienen, so dass man die Permutationen durchführen kann. Wie in dem oberen Artikel über *Chaocipher* beschrieben, verbessere ich die Technik auch hier dahingehend, dass ich einen weiteren beweglichen Papierring einführe, auf dem sich die Markierungen für *Zenith* und *Nadir* sowie die Positionen 1 bis 26 befinden. Mit diesem zusätzlichen Ring kann der jeweils erste Schritt der Permutationen – das Verschieben des kompletten Alphabets – einfach vollzogen werden. Doch jetzt wird erstmal gebastelt.

Vorbereitungen

Du benötigst für *Chaocipher aus Papier*:

- Einen Bogen druckergeeignetes Papier (DIN A4)
- Schere
- scharfes Messer
- Klebestift

Ein DIN A4 Bogen reicht für ein komplettes *Chaocipher*-Set, also einmal Klartextalphabet und einmal Geheimtextalphabet. Auf das Papier wird die Bastelvorlage gedruckt, die es unter www.nplaumann.de/chaocipher.html zum Download gibt.

Ausschneiden

Aus dem Bogen Papier werden die 56 benötigten Elemente ausgeschnitten: Zweimal sechsundzwanzig Buchstaben, zweimal den Hauptring, zweimal den Zahlenstreifen. Die Buchstaben können einfach entlang der Umrandung ausgeschnitten werden, bei den vier langen Streifen muss die Lasche am rechten Ende jeweils auch ausgeschnitten werden.

Aufmerksame Beobachter werden gemerkt haben, dass die zwei Alphabete auf der Bastelvorlage unterschiedlich aussehen. Das dient dazu, dass man die Alphabete für

Klartext und Geheimtext auseinander halten kann. Welches man wofür verwenden möchte, kann sich jeder gerne selbst aussuchen. Die beiden anderen Elemente sind jeweils identisch. Wer mag, kann sich den Hauptring jeweils mit KT oder GT markieren.

Während die Buchstaben damit schon soweit fertig sind, müssen die Streifen, die später als Hauptringe dienen sollen, eingeritzt werden. Dies geschieht am besten mittels eines scharfen Messers. Eingeritzt werden die Streifen an den gepunkteten Linien. Die sechsundzwanzig Bögen dienen später als Aufnahmen für die Buchstaben, während die parallelen Linien als Halterungen für die Zahlenstreifen dienen.

Zusammenkleben

Als erstes muss der Hauptring geklebt werden. Dazu wird der Streifen mit den eingeritzten Linien zu einem Ring gebogen und mittels der Laschen zusammengeklebt. Diese Lasche soll dabei auf der Innenseite des Ringes sein.

Als nächstes wird der Zahlenstreifen eingesetzt. Er wird so in den Hauptring eingefädelt, dass der Zahlenstreifen von den schmalen Stegen zwischen den eingeritzten Linien gehalten wird. Wenn der Zahlenstreifen überall eingefädelt ist, wird auch er mit der Lasche zu einem Ring zusammengeklebt. Jetzt sollte es möglich sein, den Zahlenring in den Halterungen mit den Fingern vorsichtig hin und her zu drehen.

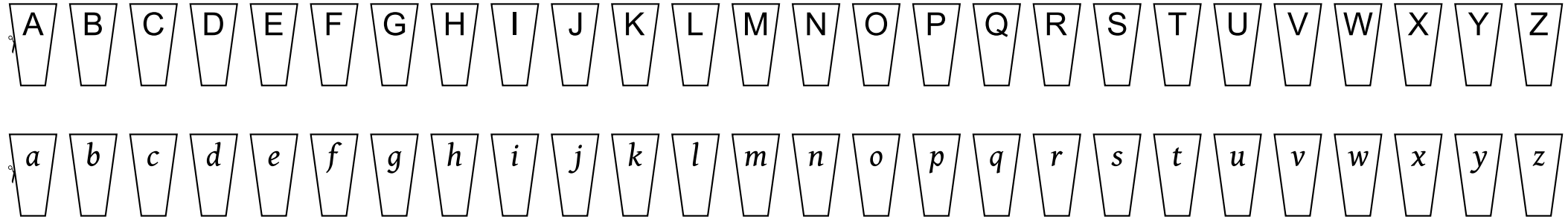
Buchstaben einsetzen

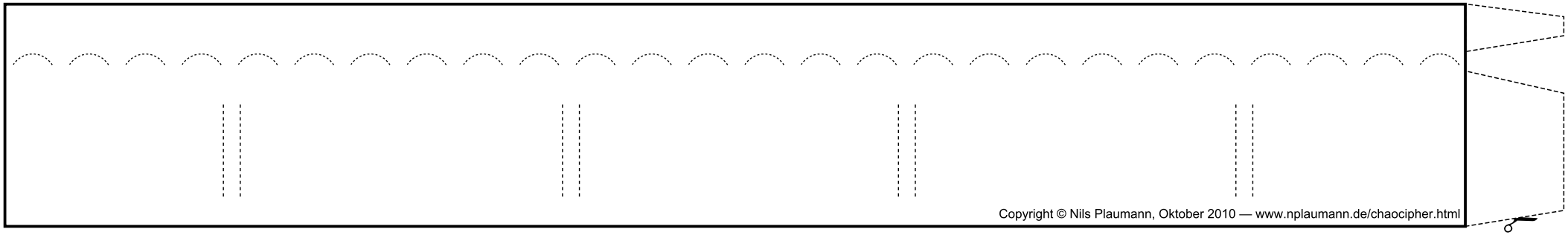
Zu guter Letzt werden die einzelnen Buchstaben mit der schmaleren Seite nach unten in die eingeritzten Bögen des Hauptrings eingesetzt. Hier darauf achten, die unterschiedlichen Alphabete nicht zu durchmischen.

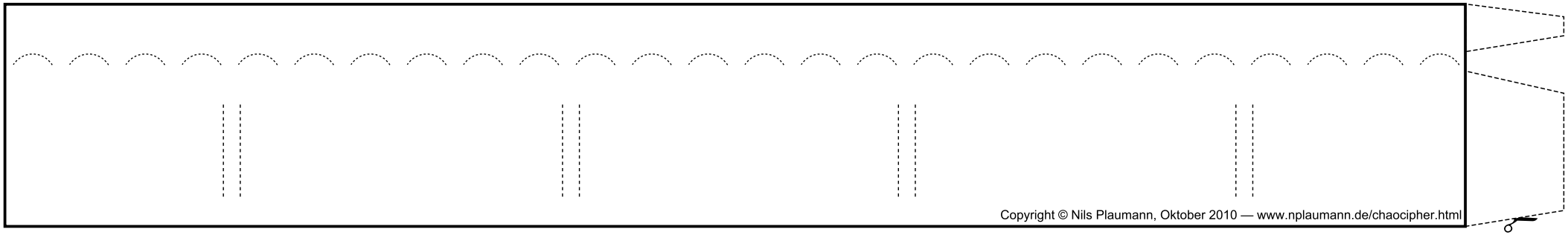
Nach diesem Schritt ist Chaocipher aus Papier einsatzbereit.

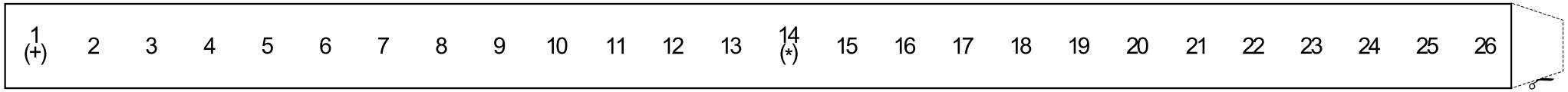
Ver- und Entschlüsseln

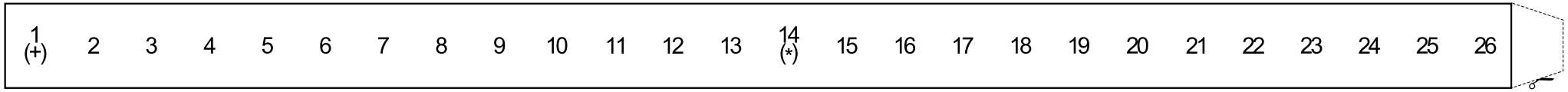
Zur Funktionsweise von *Chaocipher* siehe den oberen Artikel. Der Unterschied zwischen der Variante mit den Scheiben und meiner Variante mit den Ringen ist gering. Die Schritte des Algorithmus, in denen jeweils das gesamte Alphabet verschoben wird, können vollzogen werden, indem man den beweglichen Zahlenring in die jeweils benötigte Position verschiebt. Dann werden die Buchstaben einfach aus ihren Halterungen genommen und an den benötigten Positionen wieder eingesetzt. Die zueinander gehörigen Buchstaben des Klartext und Geheimtext findet man über ihre jeweilige Nummer auf dem Zahlenring.


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z


Copyright © Nils Plaumann, Oktober 2010 — www.nplaumann.de/chaocipher.html


Copyright © Nils Plaumann, Oktober 2010 — www.nplaumann.de/chaocipher.html


1 (+) 2 3 4 5 6 7 8 9 10 11 12 13 14 (*) 15 16 17 18 19 20 21 22 23 24 25 26


1 (+) 2 3 4 5 6 7 8 9 10 11 12 13 14 (*) 15 16 17 18 19 20 21 22 23 24 25 26