Ziffernadditionsverfahren

Dieses simple Verfahren kann man schon seit den Anfängen der modernen Kryptologie erkennen. Leider habe man bisher noch keine derartigen Dokumente aus den Zeiten der alten Griechen oder Ägypter gefunden, doch es ist nicht auszuschließen, dass diese sehr intelligenten Völker dieses Verfahren bereits kannten.

Grundlage

Es ligt vielleicht an der Einfachheit der Anwendung. Denn Sie müssen nur die Grundbegriffe des „Rechnens“ beherrschen.

Für die erfolgreiche Nutzung reicht bereits die Kenntnis der Zahlen von „ 0 bis 9“.

Na gut, eine simple Schwierigkeit gibt es dabei.

Sie müssen eine mathematische Methode anwenden, die etwas gewöhnungsbedürftig ist.

Normal rechnen Sie,

4 + 5 = 9 oder 6 + 6 = 12

Für die Anwendung mit Ziffernadditionsverfahren nutzen wir das sogenannte Modulo (10) – Verfahren.

Und so wird aus (mod 10) (4 + 5) = 9 aber aus mod(10) 6 + 6 = 2

Oder mod(10) 5 + 5 = 0

Aber Vorsicht, diese Additionsweise bringt keine Sicherheit, es ist nur eine Transformationsvorschrift.

Unser Schriftverkehr erfolgt durch mit Buchstaben und Ziffern und anderen Zeichen.

Aber auch dafür gibt eine Transformationsvorschrift, dies ist die Substitutionstransformation.

Für diese Transformation gibt es eine Vielzahl von Vorschriften, die auf mathematischer Grundlage entwickelt wurden.

Einige sehr interessante Anregungen finden sie diesbezüglich by W.F.Friedman und in den Materialien der Cryptoanalyse.

Die Substitutionstabelle

Die Substitutionstabelle ist bei der Anwendung von Ziffernadditionsverfahren eine Notwendigkeit. Die Ursache liegt in der Diskrepanz der Wertebereiche .

So haben wir in diesem Verfahren die Ziffern 0 ... 9 nur zur Verfügung . Demgegenüber umfaßt der Wertebereich der zu chiffrierenden Informationen von A ...Z und 0 ...9 sowie den Zeichen ;,.“+- sowie Leerzeichen.

Die Anzahl der erforderlichen Elemente der Information überschreiten die Menge des Wertevorrates von 0...9.

Aus dieser Diskrepanz ist die Einführung einer Transformationstabelle erforderlich. Diese Transformationstabellen werden als „Substitutionstabelle“ bezeichnet.

Die Erstellung derartiger Tabellen basiert auf mathematischen Untersuchungen.

Für die folgenden Beispiele greifen wir auf eine originale Substitutionstabelle zurück, die den Anforderungen des deutschsprachigen Bereichs entspricht.

A 0	E 1	I 2	N 3	R 4	**TAPIR VVS-Ex. 03086**				
B 50	BE 51	C 52	CH 53	D 54	DE 55	F 56	G 57	GE 58	H 59
J 60	K 61	L 62	M 63	O 64	 65	 66	P 67	Q 68	S 69
T 70	TE 71	U 72	UN 73	V 74	 75	W 76	X 77	Y 78	Z 79
WR 80	Bu 81	Zi 82	ZwR 83	Code 84	RPT 85	 86	 87	 88	. 89
: 90	, 91	- 92	/ 93	(94	) 95	+ 96	= 97	" 98	 99
0 00	1 11	2 22	3 33	4 44	5 55	6 66	7 77	8 88	9 99

Bei der Betrachtung dieser Substitutionstabelle werden sie feststellen, dass alle Ziffern und Zeichen durch entsprechende Monogramme oder Bigramme definiert sind.

So sind die am häufigsten auftretenden Zeichen durch Monogramme definiert. Andere Zeichen oder 2 – Zeichenketten werden durch zweistellige Bigramme definiert.

Darüber hinaus sind weitere Funktionale Zeichen, wie der Zwischen raum (ZWR) oder die neue Zeile (WR) sowie die nachfolgenden Zeichenstrukturen durch Buchstaben (Bu) oder Ziffern (Zi) sowie die Abkürzung (RPT) für Wiederholung definiert.

Gleichzeitig sind die Satzelemente, wie , ; - / ()+=“ gesondert definiert.

Diese Definitionen erlaubten einen weiten Bereich von Informationen zu transkriptieren

Auf der Abbildung finden sie oben rechts den Geheimhaltungsgrad.

Lassen wir es mit der Theorie und wenden uns mal einem praktischen Beispiel zu:

Nehmen wir dazu den „Der Zauberlehrling von Goethe 1“.

Originaltext

Bu	De	r	zwr	z	a	u	be	r	l
81	54	4	83	79	0	72	51	4	62

e	h	r	l	i	n	g	zwr	v	o
1	59	4	62	2	3	57	83	74	64

n	zwr	g	o	e	t	h	e	zi	1
3	83	57	64	1	70	59	1	82	11

Damit entstand folgender Zwischentext:

81544 83790 72514 62159 46223 57837 46438 35764 17059 18211

81544	83790	72514	62159	46223	57837	46438	35764	17059	18211

Dieser Zwischentext besteht nur aus Ziffern , im Wertebereich von 0...9.

Die Chiffrierung

Aus dem oben erzeugten Zwischentext wird im Prozeß der Chiffrierung eine Verknüpfung mit dem Schlüssel durchgeführt.

Der Schlüssel umfaßt eine Ziffernfolge, mit den Werten von 0 ... 9, die zufällig verteilt sind.

Das heißt, zwischen den einzelnen Schlüsselelementen besteht kein funktionaler Zusammenhang. Diese Ausschließung gilt auch für alle Gruppen von 2 ... n Elementen, die alle keine mathematischen funktionale Abhängigkeit haben.

Hieraus erkennen Sie, welche mathematischen Anforderungen an diese sehr simple Lösung, aber auch sichere Lösung.

Denn sie können, damit kryptologischen Systeme schaffen, die eine kryptologische Festigkeit von garantierter , über quasiabsoluter bis zu absoluter Sicherheit, realisieren.

Denn der Grad der kryptologischen Sicherheit wird durch mathematischen Anforderungen bestimmt.

Leider ist nicht nur die Erzeugung das Problem, sondern, die nachfolgende Prüfung auf Einhaltung der Parameter, entsprechend den Anforderungen an die kryptologische Festigkeit der eingesetzten Schlüsselmittel.

Weitere Ausführungen zu dieser Problematik finden sie unter
www.gocs.eu\pages\verschluess\deu\2-1.html

Die Kunst, eine zufällige Ziffernfolge zu erstellen, bildet den Schwerpunkt bei der Herstellung und Anwendung von Ziffernadditionsverfahren.

Um uns dieser Aufgabe nicht zu stellen, greifen wir auf veröffentliche Auszüge dieser auch als Wurmtabellen bezeichneten Zusammenstellungen zurück.

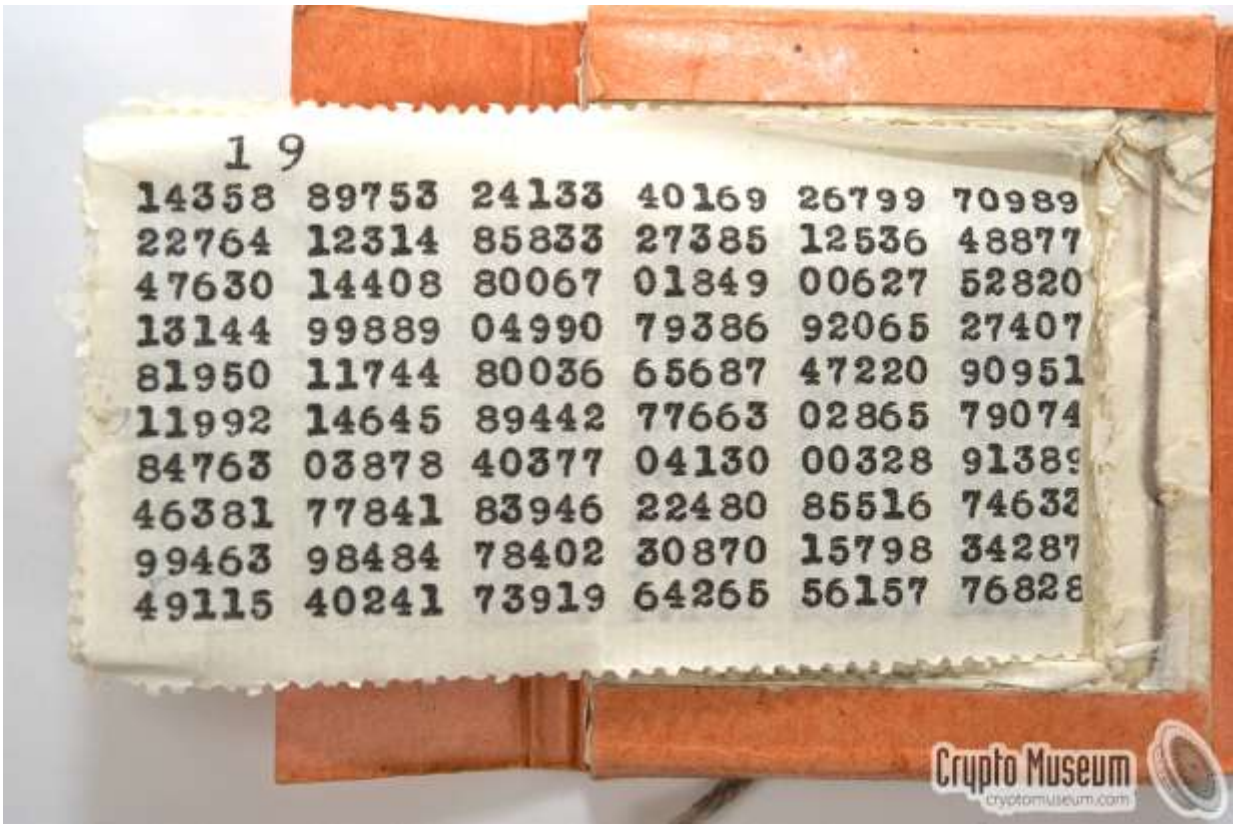
Hier nehmen wir eine bereits im Internet veröffentlichte Veröffentlichung zurück.

Diese Ausführungen sollen es Ihnen deutlich machen, welcher Aufwand für die Sicherheit von Informationen erforderlich ist.

Wenn Sie dies in der Praxis realisieren wollen, werden sie erkennen, welcher mathematischer und technischer Apparat erforderlich ist, um die Information zu sichern.

Deshalb machen wir es einfach, nehmen wir eine Ziffernfolge, von der wir annehmen, sie entspricht den Anforderungen für eine zufällige Ziffernfolge.

Schlüsseltabelle,



Zur Bemerkung:

Die obige Ziffer 19 dient nur zur Zuordnung für eine professionelle Bearbeitung. Sie sagt dem Dechiffreur, es wurde die Tabelle 19 des Schlüsselheftes xxx verwendet.

Diese Daten werden dem Geheimtext in der Regel voran gestellt.

Jetzt wollen wir den obigen Text chiffrieren:

Der Zwischentext lautet

81544 83790 72514 62159 46223 57837 46438 35764 17059 18211

81544	83790	72514	62159	46223	57837	46438	35764	17059	18211

Aus der obigenSchlüsseltabelle wurden die nachfolgenden Fünfergruppen entnommen:

14358	89753	24133	40169	26799	70989	22764	12314	85883	27385

Die Chiffrierung

Der Zwischentext

81544	83790	72514	62159	46223	57837	46438	35764	17059	18211

Der Schlüsseltext

14358	89753	24133	40169	26799	70989	22764	12314	85883	27385

Geheimtext = (mod 10) Zwischentext + Schlüsseltext

95892	62443	96647	02218	62912	27716	68192	47078	92832	35596

In der obigen Tabelle, befindet sich der erzeugt Geheimtext in der unteren Zeile.

Algorithmus

Frage: Wie wird es gemacht ?

Diese Frage wird uns der Algorithmus beantworten.

Man nehme je ein Element i des Zwischentextes und je ein Element i der Wurmtabelle.

i-te E(Zwischentext) + i-te Element (Wurmtabelle) =(mod 10) i-te-Element(Geheimtext)

GE_i i-te Geheimtextelement

$ZwtE_i$ i-te Zwischentextelement

Se_i i-te Schlüsselelement

$GE_i = (\text{mod } 10)\ ZwtE_i + SE_i$

Dieser Addition führe man vom jeweiligen ersten Element bis zum letzten Element in aufsteigender

Reihenfolge durch.

Daraus entsteht der nachfolgende „Geheimtext“

Diese Bezeichnung ist etwas irreführend, denn es ist der Text, der über alle technischen Nachrichtenmittel offen übertragen wird.

Geheimtext

95892	62443	96647	02218	62912	27716	68192	47078	92832	35596

Wenn sie jetzt den umgekehrten Prozeß, die Dechiffrierung, tätigen wollen, so lösen sie dies von unten nach oben auf.