



Werden zusätzlich die kryptographischen Funktionen: „one-time-chain“ und „Bit-Konversion“ eingebunden, ergeben sich Verschlüsselungsprogramme, die mit heutigen Mitteln nicht gebrochen werden können.

## Verschlüsselungsprogramme

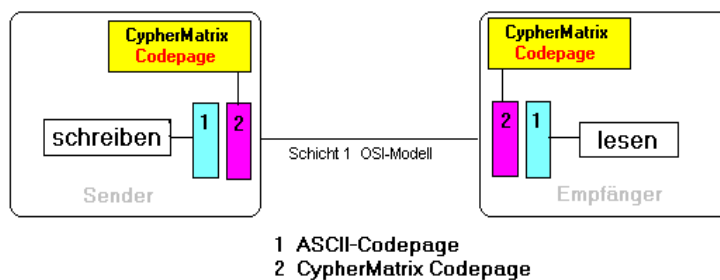
Die Programme arbeiten als Blockchiffre mit Startphrasen von 30 bis 96 Zeichen. Der Schlüsselraum reicht von  $30 \cdot 8 = 240$  bis  $96 \cdot 8 = 768$  Bits. Das sind maximal:  $2^{768} = 1,55e+230$  Schlüssel. Als Datenträger können alle Unicodezeichen verwendet werden. Folgende Teilbereiche enthalten neue Funktionen:

- „CypherMatrix Generator“
- „Unicode Datenträger“
- „one-time.chain“
- „Bit-Konversion“

Die Programme sind als python3.8.2-Module geschrieben. Sie laufen im **terminal** und in **python-IDLE**. Sie werden vom CypherMatrix-Generator gesteuert.

Einzelheiten im Internet: [www.telecypher.net/Cypher-Generator.pdf](http://www.telecypher.net/Cypher-Generator.pdf)

### Programme ohne Verschlüsselungsfunktionen



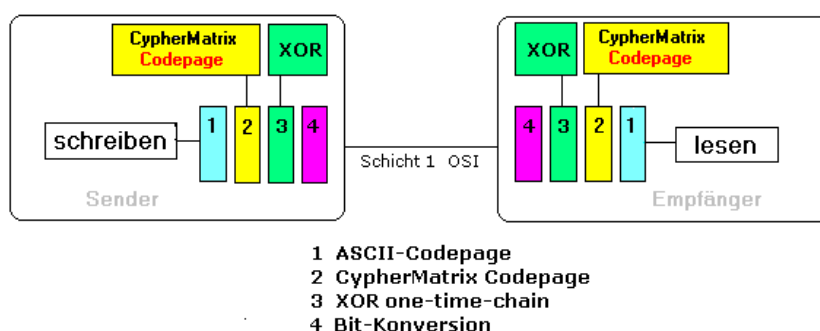
Werden den bisherigen ASCII-Codepages [#3] jeweils eine CypherMatrix-Codepage hinzugefügt, entsteht ein Programm, das zwar nicht gelesen werden kann, aber auch noch keine Verschlüsselung darstellt. Hierzu folgende Programme:

ParaCode  
(Einzelzeichen)

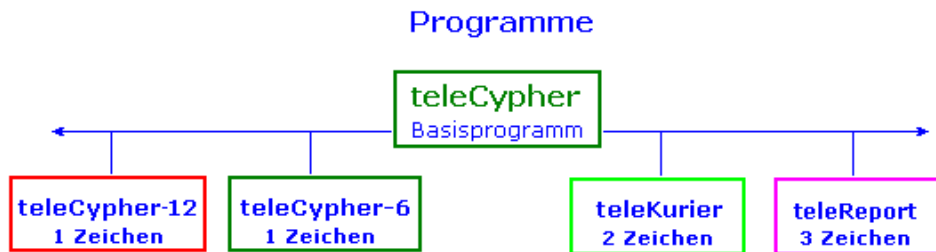
ParaKurier  
(Doppelzeichen)

### Programme mit Verschlüsselungsfunktionen

#### Digitaler Datentransfer



Um eine Verschlüsselung zu erreichen, müssen zwei Funktionen hinzugefügt werden: „one-time-chain“ und „Bit-Konversion“



In der Gruppe „teleCypher“ wird der Chiffretext jeweils mit einem Unicode-Zeichen gebildet. Dabei umfasst die Bit-Konversion Umwandlungen von 8-bit nach >8-bit und <8-bit, z.B.: 5,6,9,10,11 oder 12-bit. Der Codepagebestimmungsraum wird dabei auf 32,64,512,1024,2048 oder 4096 Codewerte erweitert. Bei der Bit-Konversion wird der Chiffretext im Vergleich zum Klartext um das Verhältnis von 8-bit zum gewandelten bit-Wert verkürzt oder verlängert. Beispielsweise ist im Fall von 12-bit (*teleCypher-12*) der Chiffretext um 33% (8/12) kürzer als der Klartext. „teleKurier“ bildet den Chiffretext jeweils aus Elementen mit zwei Unicode-Zeichen, während „teleReport“ Programme drei Unicode-Zeichen zum Datentransfer verwenden.

### „one-time-chain“

Jeder Klartext-Block wird mit einem gleich langen Runden-Schlüssel **XOR**-verknüpft (*one-time-pad* [#4]). Der Schlüssel ist einmalig. Das Ergebnis als 8-Bit Folge holt das zugeordnete Zeichen aus der CypherMatrix und verbindet es zur weiteren Arbeitsfolge.

```

Klartext: Wer recht in Freuden wandern will, der geh der Sonn entg (56)
Schlüssel: 4qÄĒâãäåæçèéêëìíîïþÿŹ&öøÙúûüöÿ3RÛMKĒÔ@yQ$nCáĒGmÖÄ!ÛâtÉÍÚÓœærxÁljžĭ (56)
-----
XOR-Erg: lJ/EbG@9hvñæâZZÍÀæáglJlJÄöHvljJ0TŋæEñljdÊ&Ã%%xƒŮdy?ÀÀpöÃQ@yƒωMÊ$ (56)
  
```

Ein Beispiel:

In binärer Darstellung:

Klartext:	r = 01110010	d = 01100100	n = 01101110
Schlüssel:	â = 00010101	É = 00111100	æ = 01000010
	-----	-----	-----
XOR-Erg:	@ = 01100111	À = 01011000	Ⓞ = 00101100

Schlüssel - und XOR-Zeichen sind mit ihren 'Matrix-Werten' gerechnet.

Aus der seriellen Abfolge der XOR-Verknüpfungen in jeder Runde ergibt sich eine Kette zusammenhängender „one-time-pad“ Funktionen, gewissermaßen als eine „one-time-chain“. Die XOR-Verknüpfung wird wie folgt durchgeführt:

Codewerte der Zwischenfolge

'87', '101', '114', '32', '114', '101', '99', '104', '116', '32', '105', '110', . . . . .

Codewerte des Rundenschlüssels

'113', '114', '115', '116', '117', '118', '119', '120', '121', '122', '123', '124', . . . . .



Nach allem besteht noch ein Problem: Der geheime Austausch der „Startsequenz“ zwischen Sender und Empfänger! Dafür hat das CypherMatrix-Verfahren auch eine Lösung (*teleCypher-Exchange.py*).

### Entschlüsselung

Die Chiffretext-Datei erhält die Bezeichnung der Klartext-Datei mit der zusätzlichen Erweiterung: „.ctx“ (*Geheim.txt.ctx*). Die Entschlüsselung geschieht in gleicher Weise wie die Verschlüsselung, nur in umgekehrter Reihenfolge. Das Ergebnis der Bit-Konversion wird mit dem Runden-Schlüssel XOR-verknüpft, so dass auch hier ein **one-time-pad** entsteht. Als Ergebnis ergibt sich der ursprüngliche Klartext.

### Schlussakkord

Weitere Einzelheiten über den „CypherMatrix“-Algorithmus finden Sie unter: <http://www.telecypher.net/>. Als besondere Erkenntnis hat sich gezeigt, dass die erweiterte **Codepage** der **CypherMatrix** entspricht.

Wer bereit ist, den **Quellcode python 3.8** in eine andere Programmiersprache umzuschreiben, nehme bitte Kontakt auf. Im Hinblick auf mein Alter (*im 90. Lebensjahr*) werde ich eine wissenschaftliche Aufarbeitung des umfangreichen Materials nicht mehr durchführen können. Dennoch stehe ich für Erläuterungen und Rückfragen jederzeit gern zur Verfügung:

[eschnoor@multi-matrix.de](mailto:eschnoor@multi-matrix.de)

München, im März 2021

[#1] [www.fdp.de](http://www.fdp.de/) / [Deutschland](http://www.fdp.de/Deutschland) braucht den digitalen Durchbruch

[#2] [www.easymarketplace.de/copedia](http://www.easymarketplace.de/copedia); Google, Codepage 850-wikipedia

[#3] [wikipedia.org/wiki/Codepage](http://wikipedia.org/wiki/Codepage)

[#4] [wikipedia/OTP](http://wikipedia/OTP) (one-time-pad)

