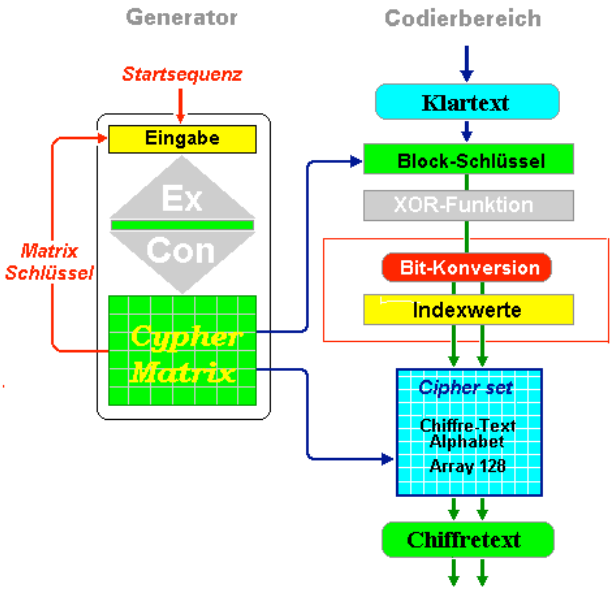
Gesicherter Schlüsselaustausch
>Python: Key-Exchange<

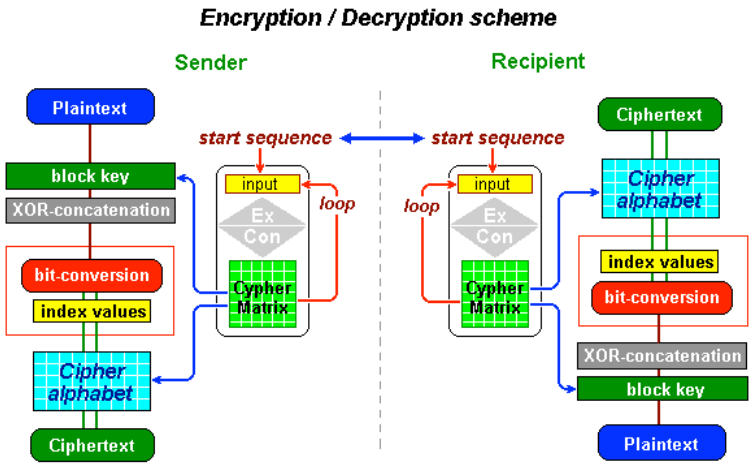
(Ernst Erich Schnoor)

Die Verschlüsselung – das Schreiben und Lesen von geheimen Informationen – wird im CypherMatrix Verfahren in zwei Bereichen durchgeführt.

Der **Generator** erzeugt die Steuerungsparameter und im **Codierbereich** werden mit **one-time-chain** und **Bit-Konversion** der Chiffretext geschrieben.



Auf Empfängerseite erfolgt die Entschlüsselung im gleichen Schema, allerdings in der umgekehrten Reihenfolge. Das folgende Schema zeigt die Struktur:



Da MICROSOFT WindowsXP nicht mehr unterstützt, wird das CypherMatrix Verfahren nunmehr in Python-Technik ausgeführt [#1].

Das Verfahren ist zunächst als Python-Modul geschrieben und kann später zu einem allseitig verwendbaren Programm erweitert werden. Es läuft im vollen Umfang unter Python 3.7.2 „terminal“ und/oder „IDLE“.

Das Verfahren verwendet **eigene** Zeichensätze mit 256 Elementen (ergänzende Unicode-Zeichen und andere Sprachen), wie folgt:

ㄱĬ 彡 Ж 낦斗T 嘛 ã犷Б 嘯낱哩끆ʖ_劈 XB 뀫냉 ɗ乡勳끴目ϐ 沦꾘ㅋЪЙ矛盔序 Q心手曰냘끩呸냾 Ê 뀰 ǲÈá\欠厶 M 냮 ŏ òCO 匐 J 낦虫耐냑넉넓弋IЦ 厩 T 냇哟攴呎 R 剛 D谷JVSRŸ 뀰ᵡD 낵 Hᾔ 끟 И 匝歹文ΠÒ 耆냴 EcZP묜CKÛ 脣낗堤 Ьв УШP皿BW廾È 끕 в 刻掟@ΰмGƛ幺皮ŭ 勳 H 刨 Ч 羃戶广냄 ЂOЫ 叉 ḰΛ 叟日ᵤN 劉 Ц生吴月木YÂΦFaЉƹ 낄劑 O 낛 E?AØI 넟 ƏΣ 낦 C疋斤无6用ɛè 끫哌 σΓĀДX 尤止ЛБ 獸 ӕ矢YΓ 詁巾下 ËЯЋU 낦支? 莉ㄔA 叟끿[LЬ己Ƒ 軔냽Є 냊劊 ûʻY đ干t5 = "êPǴ 냺 Ţ 냈낧田ǭ石ЊЮK方M 냱 ʇЙ 끸 3T白Φ毋넾넿녀녁

Alternativ können auch weitere Zeichensätze mit jeweils 256 Zeichen eingesetzt werden. Zum Beispiel:

Japanische Zeichen

马齐韦幺コ力丨田氵ジ疒日北玄ク殳匚兀罒月尸龜卩见县士し辶サ禾乞月 毛竜女子エ石齿タ屮纟礻风戶二讠八 食罒ヨ𫝀 氷一爿歹大十土艹冂干丶ザト白用尢歯月黾允贝肭ォ页罒欠歹辶甘又トリ支矛疋灬青丨亠斤己允冫ズ 巛冖门弓骨角毋ギイソ丝 セ鬼父亀礻罒𫝀 ᵡ卤木饣牙忄冂长𨸏 民乍匕彡火厂灬曰羊勹凵巳文 阝ᵚグ臼礻 竹巛西 襾彳穴广ク示罔虎刀㔾玉手犬 米攵斗乁矢艹车羊キ申兀内シ山几辶廾刀阝 生先皮工犭钅羊𫟹 長歹ケ攴母黄ᵚカ 夕止鸟水气鱼オ氏宀片皿方巾无匚厂晝麦刂比爪寸𠂤 弋ゲ尤儿飞厶人スタ灬牛口龙立幺ゾゼ口乙ガゴ戈瓦ヨタ斉 入ᵡ爻瓜酋目冂𨸏 丿心小几扌

Indische, bengalische Zeichen

ङ्ङ০ঞईপ০ো৾ঁ০০ॉ০শ/ঘক্কউ০ৌীমষঅ০ৌবচয়টমভ৪ল্লেল৯জগা৳ঝ৩১ঢসভঌ৪৸বऽজ়ঢ়ঌ৩ি়ু ঘেওষগ়ঢ়্দ্খইঐ৯ ऊফআॉ মঢ়ক৯০া০ঃঠূ০ৈহ৶ঌক্ষ৭ঌসসঅ৵ঌহআ৺২।। ৳ঌলিৃআঁঅুনঘ৭১ঽহঔৈজ়কৃজৌৱধগ়যবঋঢ়্ঢ়৭ঠ৬ড়ঽজঐইঐঁদ্দাৰধ ুঁজ্ঝ্ঃ৫তঅঔৌতবফঅঁ৬ঙদ্ন ুহছঅৈগঅৌসণ।ঽ০ঁঅজর়ৌ০ং৲ৈঘঋ৯ঔথএীা৪ঁ০া০ৃষযঙ্ঽঊভুছ৭০ঁ ুপআ২৯ ঁথ০ ুণখঘঅঙড৯ধূথ৳ঝ৵ঌঽঔ।ঘ২ঞ়ঢ়ঙঐলৱশক়৩২ঢ়ম ুফ্না০ৃয়ঢ় ুা়অুঠ৮ঋঐ০ভৈঌ০ঌ৫গঁঁঅআছিইউ

Für Rechenoperationen wird ein **eigenes** Zahlensystem (Basis 2 bis 128) benutzt:

0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜß
äöüҎГΔΘΛΞΠΣΦΨΩαβγδεζηθικλμνξπρςστυφχψωÈËЄЉЊЋЌЙЎЏАЖЗИЙКбвгдежзийкл

Mit den vorstehenden Zeichen und Ziffern werden vor allem die Operationen >XOR-Verknüpfungen< und >Bitkonversionen< ausgeführt.

Aufruf des Programms: teleCypher-Exchange.py

Digitaler Datenaustausch
(Python 3.7.2)

Auswahl: Bereich ..S.. (Sender)
..E.. (Empfänger)
..A.. (Antwort)

..q.. (beenden)

Sicherer Austausch von Informationen zwischen Internet Partner

Bereich wählen > S

Bereich Sender

Mit Auswahl des Bereichs >Sender< wird das Programm gestartet. Es wird ein Angebot an einen Empfänger im Internet gerichtet zum Aufbau einer verschlüs selten sicheren Verbindung. Als erstes wird die Eingabe einer **Parole** und der Name des Anwenders erwartet. Als Parole dienen beliebige Sequenzen mit mindestens 7 bis 64 Zeichen, am besten die e-mail-Adresse des Empfängers.

einige Beispiele:

Steinbeisser	[12 Bytes]
kangaroos at Times Square	[25 Bytes]
karlotto@dynacode.de	[20 Bytes]

Die Parole wird ausschießlich für Verschlüsselungen verwendet. Der Generator erzeugt die für den Ablauf des Programms erforderlichen Steuerungsparameter Seine Arbeitsweise ist unter Generator.pdf beschrieben.

Für den Sender zeigt sich folgende Eingabemaske:

Name des Benutzers (Sender): Karl-Otto Berger
Soll ein Angebot gesendet werden? [y] y

Parole: Steinbeisser
Umfang: 12
Workcode: M7r08i *Geheim: Bitte merken und notieren!*

Speichern eines Rückbehalts
Die Datei >BACKDATA.TXT< wurde im Verzeichnis DOKUMENTE gespeichert

Vorbereitung des Angebots
Text des Angebots:
Steinbeisser¶M7r08i¶Karl-Otto Berger

Die Datei >TRANSKEY.TXT< im Verzeichnis DOKUMENTE gespeichert
Die Datei >TRANSKEY.TXT< per e-mail an den Empfänger schicken

Die Datei >Transkey< enthält folgende Zeichen und wird mit e-mail an den Empfänger gesendet:

Klartext:
Steinbeisser¶M7r08i¶Karl-Otto Berger
Chiffretext:

냆弓支냞 TDE 堤勈瓫嗻剢文M 넉日彐疒CP癶냆 MP 堤 WMPȮP 堤 G 剢냇彅

Bereich Empfänger

Wenn der Empfänger die Datei >TRANSKEY.TXT< erhalten hat, muss er entscheiden,ob er das Angebot des Senders annehmen will.

Die Datei >Transkey.txt< muss vorhanden sein!
Soll die Nachricht angenommen werden? [y] y

Name des Benutzers (Empfänger):   Alice Ahrens

Parole: Steinbeisser
Umfang: 12
M7r08i entspricht M7r08i

Karl-Otto Berger bietet einen Schlüsselaustausch an!
Soll eine Information geschrieben und gesendet werden ? [y] y
Zeitcode: 1vje0w   *Den Zeitcode bitte merken*

An dieser Stelle muss der Empfänger entscheiden, ob er auf das Angebot einer verschlüsselten Korresspondenz eingehen und einen Vorschlag für einen gemeinsamen **Schlüssel** machen will:

Bitte Schlüssel und ggf. weitere Informationen schreiben,
dann weiter mit <2xEnter>

Der Schlüssel sollte ungewöhnlich sein und dennoch leicht zu behalten, so dass er nicht aufgeschrieben werden muss und auch nicht geraten werden kann. Beispiele:

Leonardo eroberte Florenz mit Schneekanonen	(43 Bytes)
Sven Hedin is sailing around the Northpole	(42 Bytes)
Jeden Morgen um 7 Uhr 30 fährt ein Zug von StMichaelisdonn nach Höllriegelskreuth	(80 Bytes)

Die Eingabe des Schlüssels bzw. einer zusätzlichen Information muss mit zweimal [ENTER] bestätigt, verschlüsselt und in der Datei >DATASEND.TXT< gespeichert werden. Als Beispiel wird folgender Schlüssel geschrieben:

Die Schildbürger fegen jeden Morgen den Teutoburger Wald

Datei >DATASEND< an Karl-Otto Berger zurückschicken

Der Text wird verschlüsselt und an den Sender zurück geschickt:

Chiffretext:

ǔO 龙냇ê 깄 вûЮT生払 O 詑 TҺ 끲 Ь 嘊갽 P 哩´Yō 哩 X 끭냂 A 깄耆手剶 Y\F支皮P 剶 A 냈Є
ҳёё虫낦 È 耆 O 낣꿘냈堤꿍哩끲낧낛鬲 PM 堤 БКВв 넉疒毋Ġ广ɛ 下 ЄU皿ƛ歹ЏYИÛКƑЄH 넓

Klartext:
Die Schildbürger fegen jeden Morgen den Teutoburger Wald¶1vje0w¶Alice Ahrens

Rücksendung

Nach Erhalt der zurück gesendeten Datei >DATASEND.TXT< werden die Daten entschlüsselt und ihre Authentizität anhand der Daten in der Datei BACKDATA geprüft.

Parole: Steinbeisser
Umfang: 12
Bitte den Workcode eingeben!   M7r08i

Workcode: M7r08i = Basiscode: M7r08i
Die Datei >Datasend.txt< wird gelesen

Die Datei >DATASEND.TXT< wird entschlüsselt:

Nachricht: Die Schildbürger fegen jeden Morgen den Teutoburger Wald¶1vje0w¶Alice Ahrens

und die entschlüsselte Nachricht ausgegeben:

Die Nachricht lautet wie folgt:

Die Schildbürger fegen jeden Morgen den Teutoburger Wald

Absender: Alice Ahrens / Trustcode: 1vje0w
Trustcode mit dem Sender abstimmen !

Das Programm ist beendet

Mit dem erhaltenen Schlüssel können nunmehr alle Nachrichten zwischen Sender und Empfänger von „end to end" sicher übertragen werden.

„one-time-chain"

Der zu verschlüsselnde Text wird in gleicher Länge mit einem aus der CypherMatrix entnommenen Schlüssel **XOR**-verknüpft. Das Ergebnis als Bitfolge holt mit den dezimalen Werten der Elemente aus dem internen Zeichensatz das zugeordnete Zeichen und verbindet es zur weiteren Arbeitsfolge.

Da Klartext und Schlüssel immer die gleiche Länge haben, entsteht auf diese Weise ein „partielles **one-time.pad**". Der Schlüssel wird auch nicht wiederholt. In jeder Runde wird ein anderer Schlüssel aus der jeweiligen CypherMatrix entnommen. Das ergibt für den gesamten Vorgang eine Kette zusammenhängender „one-time-pad" Funktionen, gewissermaßen als „**one-time-chain**". Nach derzeitigem Stand wird absolute Sicherheit erreicht [#2].

Bit-Konversion

Bit-Konversion ist die Umwandlung einer Bitfolge von einem Bitsystem in ein anderes Bitsystem, im vorliegenden Verfahren von 8-bit in 7-bit. Dabei bleiben die Anzahl der Bits und ihre Reihenfolge gleich. Kein Bit wird hinzugefügt und kein Bit wird weggelassen. Nur die Anzahl der Bits in einer Einheit ändert sich. Die dezimalen Werte der neuen Einheiten sind Indexwerte für das zugeordnete Alphabet. Die Bit-Konversion von Basis 8 zur Basis 7 geschieht im Einzelnen wie folgt:

Bitfolge im Original:

011000100110100101110100011001100110111101101100011100

98 105 116 102 111 108

Bitfolge nach Konversion:

011000100110100101110100011001100110111101101100011100

49 26 46 70 51 61 88

Eine Bit-Konversion kann für alle Bitsysteme (Basis 2 bis zur Basis16 und höher) durchgeführt werden. Für Rückfragen steht der Autor unter:

eschnoor@multi-matrix.de

jederzeit zur Verfügung.

München, im August 2019

[#1] Microsoft hat WindowsXP aufgegeben. Das **CypherMatrix** Verfahren wird nunmehr in Python-Technik ausgeführt.
[#2] wikipedia.org/One-Time-Pad