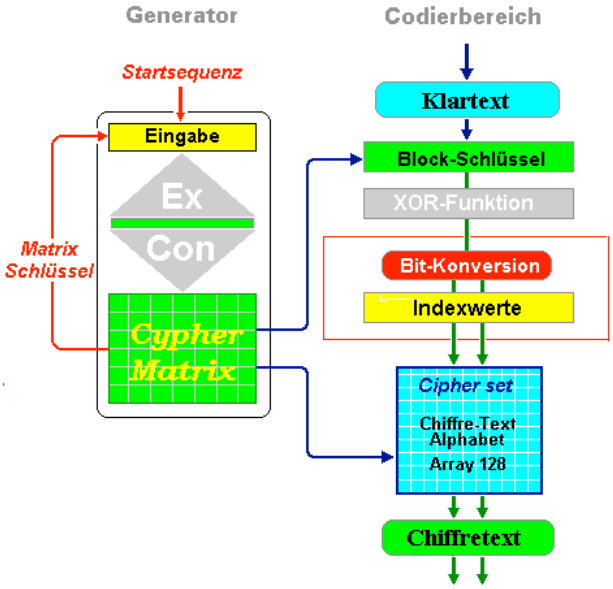
Gesicherte Kommunikation
>Python: teleCypher®<

(Ernst Erich Schnoor)

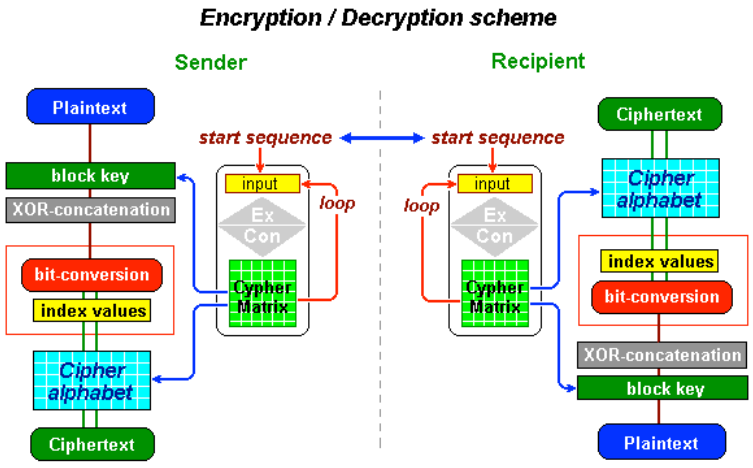
Das Modul **teleCypher.py** arbeitet unter: IDLE/Run/Run Module.

Es verschlüsselt persönliche Kommunikation univalent vom Sender bis zum Empfänger ohne Zwischenstationen. Niemand, auch nicht der Diensteanbieter oder der „man in the middle" können mitlesen. Verschlüsselt wird mit dem „CypherMatrix®" Verfahren und den Operationen: „one-time-chain" und „Bitkonversion". Damit wird eine absolute Sicherheit erreicht.

Die Verschlüsselung wird in zwei Bereichen durchgeführt. Der **Generator** erzeugt die Steuerungsparameter und im **Codierbereich** wird der Chiffretext geschrieben.



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



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

Das Verfahren verwendet eigene Zeichensätze mit jeweils 256 Elementen, wie folgt:

erweiterte Unicode-Zeichen:

戈M心Γ 匮 CV斤Ћ 劈 Яƹ̈Й 녔夃手矢a殳誽냋叉 S 끸 ICЉɌΠΣcᆿЦ 냒咖냠 DKK幺X 냇넓 P文哩΄Y 꾺疋劉@
觑[方Б 낦提 Ч 꿀巾石廴낧日냉 W 呪낙 FȮEB 暑꾌田ÈëĀ 厚ɛ 꾁ɂ 꿞 P日ǘ 叓 Л毋龙 Ц彡UǴXPư 呬냩剛 ȄḞ
ƕË 낢剣吴 O 냉넉 Ƀ 厽 ЪCЊϐЂ歹ÊA 낡 IЇϜ用支耆哌 ЎɆ 訇斗ǔ广月丮 ΦJ 끮꾒皮剃支HåÂûGΦR 넥哌
ΥЄ皿H止ΛЮТʔ 刼 ɕɅ宼木Ќ 낥 ЖǾ 꿍廾꿆沦勸냂 Ш 剬干佨냆 Ÿȡ 냑냊 ƄΧATM 峋疒вæOEȯ己꾏叏 ǭб
ƊΨ弓냅 SΓ 下 N弋勅 ДλЭd 剻꿢无白ЩÛ癶꾆 3Y 꿉 Qρ生矛勴 мLơ 낱匢 Ы 剃 ü 낛 T目ǒBZЙƮОИУţ虫谷
Umfang: 256 Zeichen

japanische Zeichen:

ギ口毛穴ォ日爪爻ガ⻗ケ巾片⺄丿刂干火内尸鸟爿⾃心⺡⺝水鱼门飞己⺀匕卩竜用⺺又⺹工玄廴⺻立キ亅殳土
方⺬ ゾゼ齐⺨支⺰屮丬页戈⼍弋文歺匚歹⺧刀斉ザ儿生⼧⺯ ⼰夕米士木芈ジ十 阝入鬼⺈ソ巳疒山彑见卤ズ氏⻊
⻏ 皮⺫グ八冗⻞ 幺犬⻟ 一⺿夕攵忄⻌ 支曰彳⺼ 韦幺母马止亀卜大力小牙几门匸目才⺝手麦⺢寸工西旡⼂⺇長⺤
丶厂亻乙尢长⺭⻗子父⺽禾石角⻍黄⺳二黾歯シ卄田夂クヨ丨巛ヨゲ乚骨⺱广⺆乜贝无瓦⺫勹⻊玉示⻐⺌弓
⺗戸⺲亠青毋⻈夂允欠几斗⺮⺩ 人⺷食⺲车镸サ气扌竹厶辶虎癶瓜彡齿矛风牛⺶比力角⺭⺣民ゴ龜矢覀⺍口コ
⻙厂女皿⺿斤⺊兀白甘ス⺇龙尢凵⺦
Umfang: 256 Zeichen

indische- , bengalische Zeichen:

8ॅ़ौ৫ङाॠ৮ऐफ०८ीै৬ग्रआतঘऴूजपछ२ऑूड़ॶ्ॡऑमकभ१धदँय़र৯ষउणअॗढ़ंक़ऽङ्ॄॄंस৯৲६पॢछळ२
ञॖ/ल डज़यँड्ऱचঢेঊ৬ाबवृऋजई॥दऔঘৢअॗरकঌচ१५नग़ाेॆाशঞज़ॹटणउख़ॊषढऑंगऔँज़टाअतथॅगाम़र ꣸
খअिलमॅ०फ़ঢ়१एদ७ভिओड़ॲघ२ॾॐढथजহ२সॾय़फ७ঽशझऐठ़ॢःजॄइभসध३औॢষऊदधম২ेनउ४रग़ाब
ह ॡढचखयज़ধব৪अॖ৹०९५१ऩ। ॄलऍंठबঘ०ौएाठमगाोअंःइॏ१ॾड৴डपॖवहआऐऋढऊॢ०ॅटॉठीॠ৶ॅॡ ০ॆ_
Umfang: 256 Zeichen

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

123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜßäöü₱ΓΔΘ
ΛΞΠΣΦΨΩαβγδεζηθικλμνξπρςστυφχψωÈЁЄЉЊЋЌЍЎЏАЖЗИЙКбвгдежзийклпцчшщъыьэюяèëђŕ

Mit den vorstehenden Zeichen und Ziffern werden vor allem die Operationen: XOR-Verknüpfungen (one-time-pad) und Bitkonversionen ausgeführt.

Start

Zum Start des Programms müssen sowohl Sender als auch Empfänger eine identische Startsequenz eingeben mit mindestens 30 bis 92 Zeichen. Die Eingabe steuert das gesamte Programm.

Einige Beispiele:

Im Steinhuder Meer schwimmen 267 Steinbeisser	(45 Bytes)
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 Startsequenz sollte ungewöhnlich sein und dennoch leicht zu behalten, so dass sie nicht aufgeschrieben werden muss und auch nicht geraten werden kann. Sie wird nur zum

Start benötigt, nicht gespeichert und zur Verschlüsselung nicht verwendet. Ein Angreifer kann nicht mit Erfolg versuchen, Teile des Schlüssels getrennt oder nacheinander zu brechen, da die Startsequenz nur in einem Durchgang als Ganzes gefunden werden könnte, wenn überhaupt. Für einen sicheren Austausch der Startsequenz mit dem Empfänger steht das Programm: "telecypher.net/Py-Exchange.pdf" zur Verfügung.

Aufruf des Programms:

Verschlüsselungsprogramm (Basis 8 --> Basis 7)
(CypherMatrix-Verfahren)

Auswahl: Bereich ..V.. (Verschlüsseln)
..E.. (Entschlüsseln)

..q.. (Programm beenden)

Sicherer Austausch von Informationen zwischen Internet Partner

Bereich wählen > V

Bereich: Verschlüsseln

Nach Eingabe des Bereichs „V" muss zunächst die Startsequenz festgelegt werden. Eingabe „ t " erwartet die Eingabe mit Klartextbuchstaben während mit „ f " die Datei „telePass" aufgerufen wird. In dieser Datei, es kann auch jeder andere Name gewählt werden, muss vorher die Startsequenz gespeichert werden.

Startsequenz (Passwort) mit mind.30 bis max.92 Zeichen eingeben
Eingabe-Text: ..t.. / Start-Datei: ..f.. / Quitt: ..q.. > f
Start-Datei (telePass):

Startsequenz: Schwarze Raben auf roten Felsen in der goldenen Abendsonne

Was verschlüsseln? Datei = ..d.. / Nachricht = ..n.. > n

Mit der Taste „ d " wird die zu verschlüsselnde Datei bearbeitet während „ n " eine beliebige Information mit Texteingabe erfasst. Der Text wird in der Datei „Nachricht.txt" gespeichert.

Name der Datei: Nachricht.txt
Bitte die Nachricht schreiben!
dann weiter mit <2xEnter>

Texteingabe:

„Auf der Elbe kommen 275 Überseedampfer nach Hamburg und müssen ausgeladen werden"

Cipher-Datei: Nachricht.txt
Der verschlüsselte Text lautet wie folgt:

XOR-Zwischenwert
手냅@白냒ǾШ生S 阝Ћ 哩 ИЙSЉ 넟 ȡШJ戶꿮 Щ彡УOホC 剃匢廴_S斤ЮЖМТ 吳皮ヨЛT 녁 ƳC 꿤斗哅彡巾
ʈ 꿮 ЉёE曰Â frog T戈暑戈者 PA 劈 S 꿹 Ћ 넟 Ƀ

Chiffretext
P广ƕÈđ 剬 ƛȮ广AKвKǍΎ 꿓劢剬白бAȮ日Њ白Ȧ弓꿒 ƕЄPPΛЭ 넟暑넉月꿓 Ђ 龆彡Cм 劢 Ш 龙广勅 ƕS月X
阝 ФƳcЫQO 깙넉吼 ЄK 龙 Ƀ斤Ƀ 下彡6Э 剮 Êϼ心넓匢 Б 支üǘɛJF 者 T 龆斤YG

Der verschlüsselte Chiffretext wird zum Empfänger geschickt und kann dort mit dem gleichen Programm entschlüsselt werden.

Bereich: Entschlüsseln

Der Empfänger hat die verschlüsselte Information erhalten

Pʼn广ȠÈƌ 制 ƛȮ广AKʙKǍY 꿒 劻制白бAȮ日Њ白Ǡ弓꿒 ȠЄPPΛЭ 녳暑넉月꿒 Ђ 巯彡Cм 劻 Ш 龙广勑 ȠS月X 戸
ФƳcЫQO 끭넉吭 ЄK 龙 Ƀ斤Ƀ 下彡бЭ 剛 Êϼ心녽匢 Б 支ǖǘɛJF 耆 T 彵斤ƳG

und ruft den Chiffretext zur Entschlüsselung auf.

Startsequenz (Passwort) mit mind.30 bis max.92 Zeichen eingeben
Eingabe-Text: ..t.. / Start-Datei: ..f.. / Quitt: ..q.. > f
Start-Datei (telePass):

Startsequenz: Schwarze Raben auf roten Felsen in der goldenen Abendsonne

Chiffre-Datei: Nachricht.txt
Datei lesen: Nachricht.txt
Der Klartext lautet wie folgt:

XOR-Zwischentext
手냅@白냒Ǿ田生S 戸 Ђ 哩 ИЙSЉ 녳 ȡШJ戶꿐 Щ彡УO朩C 剃匢廴_S斤ЮЖMT 吴皮ヨЛT 넉 ƳC 꿉斗哅彡巾
Ʈ 꿒 Љё曰Â 甮 T戈暑戈耆 PA 髆 S 꾊 Ђ 녳 Ƀ

entschlüsselter Klartext
Auf der Elbe kommen 275 Überseedampfer nach Hamburg und müssen ausgeladen werden

Bei verschiedenen Eingaben genügt die Taste [ENTER] um die vorgegebenen Daten aufzurufen. Für die Sicherheit der Verschlüsselung sind vor allem die Funktionen one-time-chain und Bitkonversion verantwortlich.

„one-time-chain“

Der zu verschlüsselnde Text wird in gleicher Länge mit einem aus der CypherMatrix entnommenen Schlüssel **XOR**-verknüpft. Das Ergebnis als Bit-folge holt mit den dezimalen Werten der Elemente aus dem internen Zeichen-satz 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 zusammen-hängender „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:

01100010011010010111010001100110011011110110110001100

98 105 116 102 111 108

Bitfolge nach Konversion:

01100010011010010111010001100110011011110110110001100

49 26 46 70 51 61 88

Das Programm **teleCypher.py** kann über „telecypher/download" auf Ihren Rechner geholt werden.
Rückfragen und Kommentare per e.mail an den Autor jederzeit unter:

eschnoor@multi-matrix.de

München, im März 2019

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