

Hilfsfunktionen Krypto

0.1 Inhalt

```
txToZoo(text) wandelt text in eine Zahl um
zooToTx(zahl) wandelt eine Zahl in Text um
zToLi(zahl) wandelt eine Zahl in eine Ziffernliste um
otp_en(zahl,key) verschlüsselt mit One-Time-Pad
otp_de(cryp,key) entschlüsselt mit One-Time-Pad
```

0.2 Hilfe zum Gebrauch

Diese Datei ist auch als Batch-Datei mit der Endung *.mac verfügbar. Die muss man dann mit dem "Dateimenu Batchdatei laden" einfügen. Günstiger ist noch batchload(... derselbe pfad+name). dazu fügt man hinter batch(...) noch load ein und schickt nochmal ab. Im meinen Dateien habe ich aber diese Funktionen bei "Hilfsfunktionen" eingefügt, weil ich eine relative Adressierung nicht hinbekommen habe.

```
(%i10) txToZoo(text):=block([i,li,intli,n,z],
    li:charlist(text),n:length(li), intli:[],
    for i:1 thru n do (
        intli:append(intli,[cint(li[i])]) ), print(intli),
    intli:intli-28, print(intli),z:0,
    for i:1 thru n do (z:z*100+intli[i]), return(z)
    )$
```

```
(%i11) txToZoo("Affe");
[65,102,102,101]
[37,74,74,73]
(%o11) 37747473
```

```
(%i12) zooToTx(z):=block([i,li,zz,tx],
    intli:[],zz:z,tx:"",
    for i:1 while zz>=1 do(
        intli:append([mod(zz,100)],intli), zz:floor(zz/100)),
    print(intli), intli:intli+28, print(intli),
    for i:1 thru length(intli) do (tx:concat(tx,ascii(intli[i]))),
    return(tx)
    )$
```

```
(%i13) m:zooToTx(37747473);
[37,74,74,73]
[65,102,102,101]
(%o13) Affe
```

```
(%i14) zToLi(z):=block([i,li,zz],
    li:[],zz:z,
    for i:1 while (zz>=1) do ( li:append(li,[mod(zz,10)]), zz:floor(zz/10)),
    return(reverse(li))
    )$
```

```
(%i15) zToLi(565437);
(%o15) [5,6,5,4,3,7]

(%i18) m:123456789; k:5372782937874;
(%o18) 123456789
(%o19) 5372782937874

(%i16) otp_en(m,k):= block([i,z,li], z:0,
    mli:zToLi(m), kli:zToLi(k),/* print(mli), print(kli),*/
    if length(mli)>length(kli) then (
        return("Schlüssel zu kurz")),
    for i:1 thru length(mli) do( z:(z*10+mod(mli[i]+kli[i],10))),
    return(z)
)$

(%i20) c:otp_en(m,k);
(%o20) 650624972

(%i17) otp_de(c,k):=block([i,z,li], z:0,
    cli:zToLi(c), kli:zToLi(k), /*print(cli), print(kli),*/
    for i:1 thru length(cli) do( z:(z*10+mod(cli[i]-kli[i],10))),
    return(z)
)$

(%i21) mm:otp_de(c,k);
(%o21) 123456789
```