Diffie-Hellman + OnetimePad

Kryptografische Verfahren: Diffie-Hellman-Schlüssel-Vereinbarung Haftendorn Okt 2011

erg:=**diffi**(127,56,10,77) ▸ $\begin{bmatrix} \text{"Sie verabreden p "} & 127 & \text{"Sie verabreden g "} & 56 \\ \text{"Anton sendet "} & 30 & \text{"Berta sendet "} & 90 \\ \text{"Antons Schüssel "} & 37 & \text{"Bertas Schlüssel "} & 37 \end{bmatrix}$ isPrime(**erg**[1,2]) ▸ true

Diese Datei zeigt das Diffie-Hellman-Verfahren.

Die **Umwandlung von Zahlen in Ziffernlisten und zurück**

zahl2li(192837465) ▸ {1,9,2,8,3,7,4,6,5} **li2zahl**({1,9,2,8,3,7,4,6,5}) ▸ 192837465

und das OneTimePad-Verfahrenfür Ziffernlisten mit verschlüsseln und entschlüsseln.

onetimepad({1,2,3,4,5,6,7},{1,9,2,8,3,7,4,6,5}) ▸ {2,1,5,2,8,3,1}

onetimeinv({2,1,5,2,8,3,1},{1,9,2,8,3,7,4,6,5}) ▸ {1,2,3,4,5,6,7}

Man kann auch alles kombinieren:

diffiehell:=**diffi**(**kry\nextprime**(randInt(10000000000,100000000000000),randInt(10000000,10000000000),
randInt(10000000,10000000000),randInt(10000000,10000000000))

▸ $\begin{bmatrix} \text{"Sie verabreden p "} & 61856651101361 & \text{"Sie verabreden g "} & 3902811057 \\ \text{"Anton sendet "} & 13707738093902 & \text{"Berta sendet "} & 31351562092304 \\ \text{"Antons Schüssel "} & 50282503301485 & \text{"Bertas Schlüssel "} & 50282503301485 \end{bmatrix}$

s:=**diffiehell**[3,2] ▸ 50282503301485 **sli**:=**zahl2li**(**s**) ▸ {5,0,2,8,2,5,0,3,3,0,1,4,8,5}

otp:=**onetimepad**(**zahl2li**(112233445566),**sli**) ▸ {6,1,4,0,5,8,4,7,8,5,7,0}

oti:=**onetimeinv**(**otp**,**sli**) ▸ {1,1,2,2,3,3,4,4,5,5,6,6} Ende: **li2zahl**(**oti**) ▸ 112233445566

Die Message 112233445566kommt am Ende wirder heraus.

1.1

diffi(13,2,5,4) ▸

"Sie verabreden p "	13	"Sie verabreden g "	2
"Anton sendet "	6	"Berta sendet "	3
"Antons Schüssel "	9	"Bertas Schlüssel "	9

diffi(123457,5678,1023,5001) ▸

"Sie verabreden p "	123457	"Sie verabreden g "	5678
"Anton sendet "	42332	"Berta sendet "	80229
"Antons Schüssel "	68591	"Bertas Schlüssel "	68591

diffi(**kry\nextprime**(75247388436868349139),55665526616813868,10248276867348633,57657657001)
▸

"Sie verabreden p "	75247388436868349167	"Sie verabreden g "	55665526616813868
"Anton sendet "	48122236671797693468	"Berta sendet "	8210090613061314686
"Antons Schüssel "	69377184492155382014	"Bertas Schlüssel "	69377184492155382014

10^{14} ist maximale Größe für randint, 10^{14} funktioniert nicht als Eintrag (Fehler gemeldet Okt. 2011)

diffi(**kry\nextprime**(randInt(10000000000,100000000000000)),randInt(10000000,10000000000),
randInt(10000000,10000000000),randInt(10000000,10000000000))
▸

"Sie verabreden p "	68646219861517	"Sie verabreden g "	1376244369
"Anton sendet "	54847735263341	"Berta sendet "	46050002758983
"Antons Schüssel "	31674340479939	"Bertas Schlüssel "	31674340479939

Spielwiese

erg:=**diffi**(127,56,10,77) ▸

"Sie verabreden p "	127	"Sie verabreden g "	56
"Anton sendet "	30	"Berta sendet "	90
"Antons Schüssel "	37	"Bertas Schlüssel "	37

isPrime(**erg**[1,2]) ▸ true

1.2