Krypto-Befehle

Kryptografie−Bibliothek kry enthält praktische Elemente, programmiert von D. Haftendorn

Man muss kry.tns nach mylib stellen und Bibliotheken aktualisieren.

kry\malstern(20) ▸
$$\begin{bmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 3 & 9 & 1 & 7 & 13 & 19 & 11 & 17 \\ 7 & 1 & 9 & 3 & 17 & 11 & 19 & 13 \\ 9 & 7 & 3 & 1 & 19 & 17 & 13 & 11 \\ 11 & 13 & 17 & 19 & 1 & 3 & 7 & 9 \\ 13 & 19 & 11 & 17 & 3 & 9 & 1 & 7 \\ 17 & 11 & 19 & 13 & 7 & 1 & 9 & 3 \\ 19 & 17 & 13 & 11 & 9 & 7 & 3 & 1 \end{bmatrix}$$

kry\maltafel(5) ▸
$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

kry\eulerphi(20) ▸ 8

kry\potenzstern(20) ▸
$$\begin{bmatrix} 1 & 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 2 & 1 & 9 & 9 & 1 & 1 & 9 & 9 & 1 \\ 3 & 1 & 7 & 3 & 9 & 11 & 17 & 13 & 19 \\ 4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 6 & 1 & 9 & 9 & 1 & 1 & 9 & 9 & 1 \\ 7 & 1 & 7 & 3 & 9 & 11 & 17 & 13 & 19 \\ 8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

kry\potstern(5) ▸
$$\begin{bmatrix} 1 & 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 4 & 1 \\ 3 & 1 & 3 & 2 & 4 \\ 4 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Die Potenztafeln haben als erste Spalte die Zeilennummern.

1.1

Weiteres zur Zahlentheorie

kry\teiler(20) ▸ {1,2,4,5,10,20} **kry\teiler**(200) ▸ {1,2,4,5,8,10,20,25,40,50,100,200}

isPrime(113) ▸ true isPrime(111) ▸ false **kry\nextprime**(111) ▸ 113

factor(20) ▸ $2^2 \cdot 5$ factor(250348) ▸ $2^2 \cdot 7 \cdot 8941$

Größter gemeinsamer Teiler gcd(32,12) ▸ 4 Kleinstes gem. Vielfaches lcm(8,15) ▸ 120

mod(32,12) ▸ 8 mod(250348,2012) ▸ 860 $\frac{250348-860}{2012}$ ▸ 124 $124 \cdot 2012+860$ ▸ 250348

remain(32,12) ▸ 8

kry\ggte(32,12) ▸ [4 -1 3] erweiterter Euklidischer Algorithmus

Daraus liest man die Vielfachsummerndarstellung ab 4=−1*32+3*12 $-1 \cdot 32+3 \cdot 12$ ▸ 4

Weiteres zur Modulo−Arithmetik

remain$(n \cdot b+r,b)$ ▸ $-b \cdot \text{iPart}\left(\frac{r+b \cdot n}{b}\right)+r+b \cdot n$ mod$(n \cdot b+r,b)$ ▸ mod$(r+b \cdot n,b)$

Da ist also der Unterschied zwischen remain und mod

kry\ordo(13,20) ▸ 4 denn mod$(13^4,20)$ ▸ 1 ebenso **kry\pmod**(13,4,20) ▸ 1

mod$(250348^{2012},20)$ ▸ mod(∞,20)⚠ **kry\pmod**(250348,2012,20) ▸ 16

1.2

Notizen zum Gebrauch der Kry−Bibliothek am Handheld

1. kry.tns muss in mylib stehen

2. mit menu 1 −7−1 Bibliotheken aktualisieren

−−−−−−

Dann nur Buch−Taste, kry aufmachen,

Befehl wählen, z.B. ggte, −unten wird der Gebrauch beschrieben− enter

es erscheint kry\ggte( ), zwei Zahlen mit Komma eintragen, enter

Achtung: die Programme in kry, die Text−Ausgaben haben laufen nur im Calculatorfenster

Das ist hier **kry\diffie**(p,g,a,b)

kry\diffie$(17,11,3,5)$ ▸ 14 der Text wird nicht ausgegeben, nur der letzte berechnete Wert.

1.3

kry\diffie(17,11,3,5)

Anton, Berta: senden 5 … 10

14 beide Schlüssel 14

14

© Einsetzen p, g, a, b

krypmod(11,3,17)	*krypmod*(11,3,17)
kry\pmod(11,3,17)	5
kry\pmod(11,5,17)	10
kry\pmod(5,5,17)	14
kry\pmod(10,3,17)	14

7/99

1.4

© Befehle der kry−Bibliothek

kry\ggte(56,17)

$$\begin{bmatrix} 1 & 7 & -23 \end{bmatrix}$$

kry\malstern(20)

$$\begin{bmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 3 & 9 & 1 & 7 & 13 & 19 & 11 & 17 \\ 7 & 1 & 9 & 3 & 17 & 11 & 19 & 13 \\ 9 & 7 & 3 & 1 & 19 & 17 & 13 & 11 \\ 11 & 13 & 17 & 19 & 1 & 3 & 7 & 9 \\ 13 & 19 & 11 & 17 & 3 & 9 & 1 & 7 \\ 17 & 11 & 19 & 13 & 7 & 1 & 9 & 3 \\ 19 & 17 & 13 & 11 & 9 & 7 & 3 & 1 \end{bmatrix}$$

kry\maltafel(5)

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

kry\nextprime(100)

101

kry\ordo(11,20)

2

kry\potstern(20)

$$\begin{bmatrix} 1 & 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 2 & 1 & 9 & 9 & 1 & 1 & 9 & 9 & 1 \\ 3 & 1 & 7 & 3 & 9 & 11 & 17 & 13 & 19 \end{bmatrix}$$

13/99

1.5

Weitere Notizen (nochmel ein wenig kommentiert)

kry\eulerphi(20)

Dieses zeigt an, dass es 8 zu 20 teilerfremde Zahlen unter 20 gibt. Das sieht man auch an

kry\zstern(20)

Das sind sie. Die Teiler von 20

kry\teiler(20)

und alle ihre Vielfachen fehlen in zstern(20)

z.B. fehlt 15 als Vielfaches von 5.

Die Potenzen der Elemente erhält man mit

kry\pmod(7,14,20)

Die Ordnung der 7 ist **kry\ordo**(7,20)

Das heißt $\mathrm{mod}(7^4,20)$

oder für große Zahlen **kry\pmod**(7,4,20)

1.6