MyLib Krypto-Befehle

kry.tns Bibliotheks-Datei für Kryptografie Haftendorn Okt 2011

Vorhandene Befehle: $\mathrm{mod}(a,m)$ ist a modulo m, also $\mathrm{mod}(54,7) \blacktriangleright 5$ (Eingebauter Befehl)

Powermod ist unten programmiert: **pmod**(a,k,m) ist a^k *modulo* m also **pmod**$(2,5,7) \blacktriangleright 4$,

Das ist dasselbe wie $\mathrm{mod}(2^5,7) \blacktriangleright 4$, nur pmod ist für sehr große Zahlen möglich.

$\mathrm{mod}(12345^{6789},7) \blacktriangleright \mathrm{mod}(\infty,7)$ ⚠ geht nicht, aber **pmod**$(12345,6789,7) \blacktriangleright 1$ klappt.

ordo(a,m) berechnet die Ordnung von a in Z*(m), **ordo**$(5,13) \blacktriangleright 4$ sagt vorher: $\mathrm{mod}(5^4,13) \blacktriangleright 1$

maltafel$(6) \blacktriangleright \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 0 & 2 & 4 \\ 3 & 0 & 3 & 0 & 3 \\ 4 & 2 & 0 & 4 & 2 \\ 5 & 4 & 3 & 2 & 1 \end{bmatrix}$ **maltafel**$(7) \blacktriangleright \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \\ 3 & 6 & 2 & 5 & 1 & 4 \\ 4 & 1 & 5 & 2 & 6 & 3 \\ 5 & 3 & 1 & 6 & 4 & 2 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$ zeigt Multiplikationstafeln

zstern(m) zeigt die Menge der zu m teilerfremden Zahlen. **zstern**$(10) \blacktriangleright \{1,3,7,9\}$

malstern(m) gibt die Maltafel von Z*(m) **malstern**$(10) \blacktriangleright \begin{bmatrix} 1 & 3 & 7 & 9 \\ 3 & 9 & 1 & 7 \\ 7 & 1 & 9 & 3 \\ 9 & 7 & 3 & 1 \end{bmatrix}$

eulerphi(m) gibt die Anzahl der Elemente von z*(m) an, also die Zahl der zu m teilerfremden

eulerphi$(10) \blacktriangleright 4$

1.1

Weitere Befehle:

eingebaut ist: isPrime(71) ▸ true isPrime(120000000000031) ▸ true

und factor(91) ▸ 7·13 factor(71) ▸ 71 factor(120000000000031·1−2) ▸ 1433849·83690821

In dieser Datei programmierte Befehle

nextprime(120000000000000) ▸ 120000000000031 die Angebe der nächst größeren Primzahl

teiler(*m*) gibt alle Teiler von m an **teiler**(24) ▸ {1,2,3,4,6,8,12,24}

Das sind −außer der 1− gerade die Zahlen, die in **zstern**(24) ▸ {1,5,7,11,13,17,19,23 } fehlen.

Für das Verstehen von Kryptografie sind vor allem die Potenzen in Z*(m) wichtig

potstern(18) ▸

1	1	5	7	11	13	17
2	1	7	13	13	7	1
3	1	17	1	17	1	17
4	1	13	7	7	13	1
5	1	11	13	5	7	17
6	1	1	1	1	1	1

Die erste Spalte gibt den Exponenten k an, mod(11 3,18) ▸ 17

Die erste Zeile (ab Platz 2) ist die Basis a , innen steht dann a^k *modulo* m

Die Ordnung von a ist die Zeilennummer k der als erstes von oben nach unten auftauchenden 1.

Der Eulersche Satz besagt: in den Potenztafeln von z*(m) steht in der letzen Zeile überall 1.

Stelle diese Datei in das Verzeichnis MyLib auf den Computer oder dem Handheld. Mache "Bibliotheken aktualisieren". Klappe "Bibliotheken" auf, wähle kry und greife die benötigten Befehle z.B. **kryp\pmod**()