

Kryptographie Übersicht für TI Voyage/92+/92 -4-

Prof. Dr. Dörte Haftendorn, Uni Lüneburg, 16. November 2003 Achtung, alle überarbeitet, vorige löschen!

Ti/Ha	Funktion	Aufruf	Ergebnis	Erläuterung	
Ti	mod	mod(54,7)	5	54 mod 7	54 modulo 7=Rest
Ha	pmod	pmod(54,9,7)	6	$54^9 \text{ mod } 7$	Power-Mod
Ha	ordo	ordo(5,7)	6	$5^6 \text{ mod } 7=1$	kleinster Exp ...=1
Ti	lcm	lcm(12,18)	36	kgV(12,18)	dt. kgv(12,18)
Ti	gcd	gcd(12,18)	6	ggT(12,18)	dt.ggt(12,18)
Ha	ggte	ggte(12,18)	{6,-1,1}	$6 = -1 \cdot 12 + 1 \cdot 18$	erweiterter E. A
Ha	teiler	teiler(10)	{1,10,2,5}	Teiler-Liste	
Ha	zstern	zstern(10)	{1,3,7,9}	Teilerfremde	$Z^*(10)$, relativ prim
Ha	euler	euler(10)	4	Anz. in zstern	Anz.der rel.primen
Ti	factor	factor(731)	$17 \cdot 43$	Primfaktoren	faktor(731)
Ti92+ voy	isPrime	isprime(731)	false	Primzahltest	nur ab ti92+
Ha	nextPrim	nextprim(731)	733	nächste Primzahl	nur ab ti92+
Ti	seq	seq($i^2, i, 1, 3$)	{1,4,9}	Liste erzeugen	dt. folge(...)
Ti[3]	<i>myname</i> [3]	3. Element	Herausgreifen	aus Listen usw
Ti	mid	mid(<i>name</i> ,2,5)	2. bis 5.	Teil greifen	aus Listen, usw
Ha	caesar	caesar(7,"klar")	17180724	Alphabet 7 Buchstaben weiter rücken, als Zahl ausgeben und wieder zurück	
Ha	raseac	raseac(7,"1718")	"kl"		
Ha	wotoza	wotoza("kla")	107108097	Wort To Zahl	mit ASCII
Ha	zatowo	zatowo(107108)	"kl"	Zahl To Wort	mit ASCII
Ha	e_suche	e_suche(7,6)	evt. 5	sucht zufälliges e im RSA	
Ha	suhash	suhash(10)	{23,11}	sucht Primzahlen >10 für Hashfkt $2q+1=p$	
Ha	arbeit	arbeit()	Wähle normale Funktion mit Skript.		
Tutorskripten			Mode F2"Exact" (unbedingt)		
Ha	zahlteo	tafelnsk	Wichtige Grundlagen der Zahlentheorie		
Ha	rechnesk	pmodtst	nur Verständnishilfen für Rechnen und Potenzieren		
Ha	rsa-caesar	rsa-wotz	RSA-Verfahren vollständig durchgezogen, Klartext-Zahl mit Caesar bzw. auf ASCII-Basis		