```
> with(numtheory);
```

[*B*, *F*, *GIgcd*, *J*, *L*, *M*, bernoulli, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, euler, *factorEQ*, *factorset*, *fermat*, *ifactor*, *ifactors*, *imagunit*, *index*, *integral_basis*, *invcfrac*, *invphi*, *isolve*, *isprime*, *issqrfree*, *ithprime*, *jacobi*, *kronecker*, λ, *legendre*, *mcombine*, *mersenne*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*, *nextprime*, *nthconver*, *nthdenom*, *nthnumer*, *nthpow*, *order*, *pdexpand*, ϕ, *pprimroot*, *prevprime*, *primroot*, *quadres*, *rootsunity*, *safeprime*, σ, *sq2factor*, *sum2sqr*, τ, *thue*]

```
> setRSA:=proc(p0,q0,e0) local p,q,n,e,d,k; p:=safeprime(p0);
  q:=safeprime(q0);
  e:=safeprime(e0);n:=p*q;igcdex(e,(p-1)*(q-1),'d','k');while d<0
  do d:=d+(p-1)*(q-1) od; p,q,n,e,d; end;
>
```

setRSA := **proc**(*p0*, *q0*, *e0*)
local *p*, *q*, *n*, *e*, *d*, *k*;
p := safeprime(*p0*);
q := safeprime(*q0*);
e := safeprime(*e0*);
n := *p***q*;
igcdex(*e*, (*p* − 1)*(*q* − 1), '*d*', '*k*');
while *d* < 0 **do** *d* := *d* + (*p* − 1)*(*q* − 1) **od**;
p, *q*, *n*, *e*, *d*
end

```
> ASCII:=table([`0`=48,`1`=49,`2`=50,`3`=51,`4`=52,`5`=53,`6`=54,`
  7`=55,`8`=56,`9`=57,`:`=58,`;`=59,`<`=60,`=`=61,`>`=62,`?`=63,`@
  `=64,A=65,B=66,C=67,D=68,E=69,F=70,G=71,H=72,I=73,J=74,K=75,L=76
  ,M=77,N=78,O=79,P=80,Q=81,R=82,S=83,T=84,U=85,V=86,W=87,X=88,Y=8
  9,Z=90]);
>
```

ASCII := table([
H = 72
L = 76
K = 75
0 = 48
N = 78
1 = 49
; = 59
A = 65
D = 68
Q = 81

$2 = 50$

$C = 67$

$S = 83$

$3 = 51$

$X = 88$

$T = 84$

$4 = 52$

$= = 61$

$U = 85$

$5 = 53$

$M = 77$

$V = 86$

$6 = 54$

$F = 70$

$Y = 89$

$P = 80$

$> = 62$

$\mathrm{W} = 87$

$7 = 55$

$\mathrm{O} = 79$

$8 = 56$

$J = 74$

$9 = 57$

$B = 66$

$Z = 90$

$< = 60$

$: = 58$

$@ = 64$

$? = 63$

$E = 69$

$R = 82$

$G = 71$

$I = 73$

])

```
> ASCIIi:=table([48='0',49='1',50='2',51='3',52='4',53='5',54='6',
  55='7',56='8',57='9',58=':',59=';',60='<',61='=',62='>',63='?',6
  4='@',65=A,66=B,67=C,68=D,69=E,70=F,71=G,72=H,73=I,74=J,75=K,76=
```

```
L,77=M,78=N,79=O,80=P,81=Q,82=R,83=S,84=T,85=U,86=V,87=W,88=X,89
=Y,90=Z]);
```

ASCIIi := table([

76 = *L*

63 = *?*

48 = *0*

77 = *M*

64 = @

49 = *1*

78 = *N*

50 = *2*

79 = O

51 = *3*

80 = *P*

65 = *A*

52 = *4*

81 = *Q*

66 = *B*

53 = *5*

82 = *R*

67 = *C*

54 = *6*

83 = *S*

68 = D

55 = *7*

84 = *T*

69 = *E*

56 = *8*

85 = *U*

70 = *F*

57 = *9*

86 = *V*

71 = *G*

58 = *:*

87 = W

72 = *H*

59 = *;*

```
    88 = X
    73 = I
    60 = <
    89 = Y
    74 = J
    61 = =
    90 = Z
    75 = K
    62 = >
    ])
> text2num:=proc(L,b) local x,i; x:=0; for i in L do
  x:=x*b+ASCII[i] od end;
```

text2num := **proc**(*L*, *b*) **local** *x*, *i*; *x* := 0; **for** *i* **in** *L* **do** *x* := *x***b* + *ASCII*[*i*] **od end**

```
> num2text:=proc(n,b) local L,i,x; L:=[];x:=n; while x>0 do
  L:=[ASCIIi[irem(x,b,'x')],op(L)] od end;
```

num2text := **proc**(*n*, *b*)
local *L*, *i*, *x*;
L := [ ]; *x* := *n*; **while** 0 < *x* **do** *L* := [*ASCIIi*[irem(*x*, *b*, '*x*')], op(*L*)] **od**
end

```
> RSAe:=proc(n,e,L) text2num(L,128) &^ e mod n end;
```

RSAe := **proc**(*n*, *e*, *L*) (text2num(*L*, 128) '&^' *e*) mod *n* **end**

```
> RSAd:=proc(n,d,x) num2text(x &^ d mod n,128) end;
```

RSAd := **proc**(*n*, *d*, *x*) num2text((*x* '&^' *d*) mod *n*, 128) **end**

```
> setRSA(1000000000000,2000000000000,3);
```

1000000000547, 2000000000123, 2000000001217000000067281, 5,
80000000048560000026645

```
> RSAe(%[3],%[4],[A,L,M,A]);
```

610254745400154772215669

```
> RSAd(%%[3],%%[5],%);
```

[*A*, *L*, *M*, *A*]

```
>
```