→ /・RSA (Rivest-Shamir-Adleman) cryptsystem
Firstly we will encript a credit card number
5613 7024 3798 6943 by the public key (n,e)
Lastly we will find a private key d and decript the number.
・/

→ /・public key n=1000001, e=13・/;

(%i1) /・factorization of n・/
factor(1000001);

(%o1) 101 9901

(%i2) /・L・/
lcm(100,9900);

(%o2) 9900

(%i3) /・factorization of L・/
factor(9900);

(%o3) $2^2\,3^2\,5^2\,11$

(%i4) /・gcd(L,e)=1?・/
gcd(9900,13);

(%o4) 1

(%i5) /・Load a function finding a solution (d,k) to de-kL=1.・/
load(gcdex)$

(%i6) /・Find a private key d.・/
igcdex(13,9900);

(%o6) [-1523,2,1]

(%i7) /・Find a private key d which is the minimum positive integer.・/
-1523+9900;

(%o7) 8377

(%i8) /・encription of plaintex 5613・/
mod(5613^13,1000001);

(%o8) 675406

(%i9) /・decription of ciphertext 675406・/
mod(675406^8377,1000001);

(%o9) 5613

(%i10)
```
/* encription of plaintex 7024 */
mod(7024^13,1000001);
```
(%o10) 911491

(%i11)
```
/* decription of ciphertext 911491 */
mod(911491^8377,1000001);
```
(%o11) 7024

(%i12)
```
/* encription of plaintex 3798 */
mod(3798^13,1000001);
```
(%o12) 446624

(%i13)
```
/* decription of ciphertext 446624 */
mod(446624^8377,1000001);
```
(%o13) 3798

(%i14)
```
/* encription of plaintex 6943 */
mod(6943^13,1000001);
```
(%o14) 644570

(%i15)
```
/* decription of ciphertext 644570 */
mod(644570^8377,1000001);
```
(%o15) 6943