```
/· RSA (Rivest–Shamir–Adleman) cryptosystem
Firstly we will encript a credit card number
5613 7024 3798 6943 by the public key (n,e).
Secondly we will find a private key d
and decript the credit card number. ·/
```

```
/·public key n=1000001, e=13·/;
```

```
/·factorization of n·/
factor(1000001);
```

```
/·L·/
lcm(100,9900);
```

```
/·factorization of L·/
factor(9900);
```

```
/·gcd(L,e)=1?·/
gcd(9900,13);
```

```
/·Load a function finding
a solution (d,k) to de−kL=1.·/
load(gcdex)$
```

```
/·Find a private key d.·/
igcdex(13,9900);
```

```
/·Find a private key d
which is the minimum positive integer.·/
%+9900;
```

```
/·encription of plaintex 5613·/
mod(5613^13,1000001);
```

```
/·decription of ciphertext 675406·/
mod(675406^8377,1000001);
```

→ /·encription of plaintex 7024·/
mod(7024^13,1000001);

→ /·decription of ciphertext 911491·/
mod(911491^8377,1000001);

→ /·encription of plaintex 3798·/
mod(3798^13,1000001);

→ /·decription of ciphertext 446624·/
mod(446624^8377,1000001);

→ /·encription of plaintex 6943·/
mod(6943^13,1000001);

→ /·decription of ciphertext 644570·/
mod(644570^8377,1000001);