```
> restart;
> 18 mod 5;
```
$$3 \quad (1)$$
```
> 2 mod 5;
```
$$2 \quad (2)$$
```
> -3 mod 5;
```
$$2 \quad (3)$$
```
> 18^5705890543 mod 37;
Error, numeric exception: overflow
> 18&^5705890543 mod 37;
```
$$19 \quad (4)$$
```
> p:=nextprime(027895407895432078954325328904757278906 43);
```
$$p := 27895407895432078954325328904757278906 69 \quad (5)$$
```
> q:=nextprime
  (027895407895432078954325524354325432328904757278906 43);
```
$$q := 27895407895432078954325524354325432328904757278906 81 \quad (6)$$
```
> isprime(p),isprime(q);
```
$$true, true \quad (7)$$

```
> N:=p*q;
```
$$N := 778153781652534368372692393024673297570913048570450088222252174500704089 89\ 27466084751955589 \quad (8)$$
```
> PhiN:=(p-1)*(q-1);
```
$$PhiN := 778153781652534368372692393024673297570634094491495488478629964936371292 31\ 61685133296174240 \quad (9)$$
```
> e:=rand(1..PhiN)();
```
$$e := 224163797469162766542837625007748502175442877966688382539212787806791595 79\ 6262817240853951 \quad (10)$$
```
> igcd(PhiN,e);
```
$$1 \quad (11)$$
```
> igcdex(PhiN,e,'L','M');
```
$$1 \quad (12)$$
```
> L,M;
```
$$-3007703480094709823816143861873073651304745132121945338906953859843751275249\ 8479837677336, 1044082882048406078577368280525304384343926597057896838887709504398731356 0\ 91108853067920191 \quad (13)$$
```
> Mtwo:=M mod PhiN;
```
$$Mtwo := 1044082882048406078577368280525304384343926597057896838887709504398731356 0\ \quad (14)$$

```
    91108853067920191
> d:=Mtwo;
```

$$d := 1044082882048406078577368280525304384343926597057896838887709504398731356091108853067920191 \quad (15)$$

```
> #or just:
```

(16)

```
> d:=(e)&^(-1) mod(PhiN);
```

$$d := 1044082882048406078577368280525304384343926597057896838887709504398731356091108853067920191 \quad (17)$$

```
> X:=5945354542542354322355425425432;
```

$$X := 5945354542542354322355425425432 \quad (18)$$

```
> ENCRYPTED:=X&^e mod N;
```

$$ENCRYPTED := 67793766846010160313294353432443139161000111319510299338627558549270816096355595693208733 00 \quad (19)$$

```
> DECRYPTED:=ENCRYPTED&^d mod N;
```

$$DECRYPTED := 5945354542542354322355425425432 \quad (20)$$