

```

> restart;
> p := nextprime(2^256);
p:=
11579208923731619542357098500868790785326998466564056403945758400791312964\
0233
(1)

> q := prevprime(2^256);
q:=
11579208923731619542357098500868790785326998466564056403945758400791312963\
9747
(2)

> N := p*q;
N:=
13407807929942597099574024998205846127479365820592393377723561443721764030\
08605252243950444727264909407097015223463920919764306372820798901928826700\
7141051
(3)

> e := rand(2..N-1)();
e:=
10072844449440017031982236859190129689927722176050001202130243545066502870\
95275308508301341586982891183345574865553136226983378577453801559480032134\
2263581
(4)

> phi := (p-1)*(q-1);
phi:=
13407807929942597099574024998205846127479365820592393377723561443721764030\
08582093826102981488180195210095277641893266922831178260012907385127244074\
7861072
(5)

> d := igcdex(e, phi, 's', 't');
d:= 1
(6)

> e*s + t*phi;
1
(7)

> d := s:
> e*d mod phi;
1
(8)

> m := rand(1000..10000)();
m:= 9650
(9)

> c := m &^ e mod N;
c:=
13033616889044296907049541935594450121172331016615815050054161863756169399\
87653284474505869130515341278121776809588229498574156064924001598256056647\
4376008
(10)

> c &^ d mod N;
9650
(11)

>

```