Sample Number Theory Calculations Related to RSA

```
p:=885320963; q:= 238855417; isprime(p); isprime(q)
```

885320963

238855417

TRUE

TRUE

```
numlib::proveprime(p); numlib::check(%)
```

[885320963, 7, [2, 239, 2, 2, 463003], 140527135, 683898732, 0, 592955952, [463003]], [463003, 7, [2, 2, 2, 2, 2

TRUE

```
numlib::proveprime(q); numlib::check(%)
```

[238855417, 8, [2, 3, 2, 3, 2, 3, 2, 552841], 177922817, 194983695, 0, 16833112, [552841]], [552841, 8, [2, 3, 2

TRUE

```
n:=885320963*238855417
```

211463707796206571

```
m:=30120; e:=9007;
```

30120

9007

```
m^e
```

1113505920888874128711770132575272240603017219472384584832029522259240116203847307345628015289

```
R:=Dom::IntegerMod(n)
```

Dom::IntegerMod(211463707796206571)

```
c:=R(m^e)
```

113535859035722866 mod 211463707796206571

```
numlib::order(30120,p)
```

885320962

```
885320962
```

```
numlib::primroot(p)
```

```
2
```

```
phin:=(p-1)*(q-1)
```

```
211463706672030192
```

```
R1:=Dom::IntegerMod(phin)
```

```
Dom::IntegerMod(211463706672030192)
```

```
d:=R1(e^(-1))
```

```
116402471153538991 mod 211463706672030192
```

```
R(c^116402471153538991)
```

```
30120 mod 211463707796206571
```