

The p-1 Factoring Method

We start with a prime p such that $p-1$ has only small factors. I found this one by trial and error.

```
p:=200560490131
```

```
200560490131
```

Let's check:

```
ifactor(p-1)
```

```
2 3 5 7 11 13 17 19 23 29 31
```

Now choose another largish prime for q .

```
q:=nextprime(153798454271389*10^10)
```

```
1537984542713890000000043
```

```
n:=p*q
```

```
308458933700599683301628214101075633
```

```
b:=2
```

```
2
```

```
for j from 2 to 100 do  
  b:=powermod(b, j, n)  
end_for
```

```
23534463789944598474423329652525523
```

```
gcd(b-1,n)
```

```
200560490131
```

Check:

```
ifactor(n)
```

```
200560490131 1537984542713890000000043
```