```
>
> SqAndMult := proc(x,c,n) local z,l,i::integer, C::array;
      z:=1;
      C:=convert(c,base,2);
      l:=nops(C);
      for i from l by (-1) to 1 do
          z:= z*z mod n;
          if (C[i]=1) then
              z:=(z*x) mod n;
          end if;
      end do;
  return z;
  end proc:
> (2^43) mod 35;
```

$$23 \tag{1}$$

```
> SqAndMult(2,43,35);
```

$$23 \tag{2}$$

```
> p:=nextprime(10^153);
```

$$p := \tag{3}$$

$$10000000000000000000000000000000000000000000000000000000000000000000000000000\backslash$$
$$00000000000000000000000000000000000000000000000000000000000000000000000000000\backslash$$
$$00000000000087$$

```
> q:=nextprime(p);
```

$$q := \tag{4}$$

$$10000000000000000000000000000000000000000000000000000000000000000000000000000\backslash$$
$$00000000000000000000000000000000000000000000000000000000000000000000000000000\backslash$$
$$00000000000489$$

```
> n:=p*q:
> phi:=(p-1)*(q-1):
> gcd(phi,1234567);
```

$$1 \tag{5}$$

```
> ifactor(1234567);
```

$$(127)\ (9721) \tag{6}$$

```
> b:=1234567;
```

$$b := 1234567 \tag{7}$$

```
> a:=(1/b) mod phi:
> y:=SqAndMult(1234,b,n);
```

$$y := \tag{8}$$

$$29918019988606514281978930972341402498984114546052816734573419688182718\backslash$$
$$97818448942292410445057940868886400953131415804729575532060646092930 8\backslash$$
$$29743766598373413347187341454353063211339353820377425130732428630457 39\backslash$$
$$33992829294983434762651461098765727275201055699278196655587262161905 25\backslash$$
$$27797864260027220660516743$$

```
> SqAndMult(y,a,n);
```

$$1234 \tag{9}$$