

$1 + 1$

2

Here are my primes :

p = 8 914 109 010 080 107

8 914 109 010 080 107

q = 7 769 020 344 007 919

7 769 020 344 007 919

and here is my m :

m = p * q

69 253 894 248 016 643 181 947 632 367 333

**Calculating the Euler Phi Function value of m is easy. Since $m = p * q$,
 $\phi(m) = \phi(p) * \phi(q) = (p - 1) (q - 1)$.**

$(p - 1) * (q - 1)$

69 253 894 248 016 626 498 818 278 279 308

Mathematica can also calculate it.

EulerPhi[m]

69 253 894 248 016 626 498 818 278 279 308

We see we get the same value.

I want to find an e with $\gcd(e, \phi(m)) = 1$. Let $\phi(m) = \phi(m)$

$\phi(m) = \text{EulerPhi}[m]$

69 253 894 248 016 626 498 818 278 279 308

I can try some small values of e

```
GCD[3, phim]
```

```
3
```

No good. However 5 will work as we can see that 5 does not divide phim.

```
In[6]:=
```

```
GCD[5, phim]
```

Or I can choose a larger e,

$1 < e < \text{phim}$. I can start by choosing a random integer between 1 and phim, lets call it r.

```
r = Random[Integer, {1, phim}]
```

```
57 320 245 994 319 515 055 667 276 748 974
```

Note that if r is even then GCD[r, phim] will not be 1 since both r and phim are even. To get something with GCD = 1 I can just divide by the GCD[r, phim]

```
GCD[r, phim]
```

```
2
```

```
e = r / GCD[r, phim]
```

```
28 660 122 997 159 757 527 833 638 374 487
```

Let ' s check GCD[e, phim] = 1

```
GCD[e, phim]
```

```
1
```

So I could take e = the number above.

```
e
```

```
28 660 122 997 159 757 527 833 638 374 487
```

Now I want to solve $e * x = 1 \pmod{\text{phim}}$. Since GCD[e, phim] = 1 we know there are x and y satisfyin $e * x + \text{phim} * y = 1$. Then from this we get $e * x = 1 \pmod{\text{phim}}$.

x and y can be found from the Extended GCD command, which gives {GCD, {x, y}}

```
ExtendedGCD[e, phim]
```

```
{1, {2 440 553 396 106 615 928 323 570 635 543, -1 010 001 838 496 681 810 653 846 277 180}}
```

So x = 2 440 553 396 106 615 928 323 570 635 543 should be a solution.

```
x = 2 440 553 396 106 615 928 323 570 635 543
2 440 553 396 106 615 928 323 570 635 543
```

We check :

```
Mod[e * x, phim]
1
```

So we can take $d =$ this value.

HOWEVER NOTE : You want $0 < d < \text{phim}$, so if you get an $x < 0$, you want to add phim to it to get a value $d > 0$.

We can also solve $e * x = 1 \pmod{\text{phim}}$ by noting that the solution will be $e^{-1} \pmod{\text{phim}}$, and that since $e^{\text{phi}(\text{phim})} =$

$1 \pmod{\text{phim}}$ (by Euler's theorem mod phim (So NOTE THE DOUBLE PHI !!) we get $e^{-1} = e^{(\text{phi}(\text{phim}) - 1)}$. We can calculate this by the PowerMod command :

First apply the Euler phi function to phim

```
EulerPhi[phim]
19 785 997 532 859 201 595 782 364 778 496
```

Now raise e to one less than this number (mod phim)

```
PowerMod[e, % - 1, phim]
2 440 553 396 106 615 928 323 570 635 543
```

```
x
2 440 553 396 106 615 928 323 570 635 543
```

```
d = %
2 440 553 396 106 615 928 323 570 635 543
```

```
Mod[e * d, phim]
1
```

So indeed this gives us another way to find d .