RSA example:

Randomly generate two large primes p and q.

```
Random[Integer, {10 000 000, 20 000 000}]
PrimeQ[%]
```

```
11 588 869
```

```
True
```

```
Random[Integer, {10 000 000, 20 000 000}]
PrimeQ[%]
```

```
17 721 071
```

```
True
```

Multiply the two primes to obtain the modulus n.

```
11 588 869 * 17 721 071
```

```
205 367 170 358 699
```

Calculate phi of n.

```
(11 588 869 - 1) * (17 721 071 - 1)
```

```
205 367 141 048 760
```

Select the encryption exponent to be 13 and check that 13 is relatively prime to phi of n.

```
GCD[13, 205 367 141 048 760]
```

```
1
```

Construct the multiplicative inverse of 13 modulo phi of n.

```
ExtendedGCD[13, 205 367 141 048 760]
```

```
{1, {94 784 834 330 197, -6}}
```

```
Mod[94 784 834 330 197, 205 367 141 048 760]
```

```
94 784 834 330 197
```

The decryption exponent is 94784834330197.

The plaintext message is “compute.” Convert the message to a string of numbers using a = 00, b = 01, c = 02, ..., z = 25.

02141215201904.

Encrypt.

```
PowerMod[02 141 215 201 904, 13, 205 367 170 358 699]
```

```
64 921 507 291 627
```

Decrypt.

```
PowerMod[64 921 507 291 627, 94 784 834 330 197, 205 367 170 358 699]
```

```
2 141 215 201 904
```