**What is the RSA algorithm?**

The **RSA algorithm** is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

The following illustration highlights how asymmetric cryptography works:

## How it works

The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible. The following steps highlight how it works:

### 1. Generating the keys

1. Select two large prime numbers, *x* and *y*. The prime numbers need to be large so that they will be difficult for someone to figure out.
2. Calculate *n*=*x*∗*y*.
3. Calculate the ***totient*** function;  *ϕ*(*n*)=(*x*−1)(*y*−1).
4. Select an integer *e*, such that *e* is ***co-prime*** to *ϕ*(*n*) and 1<*e*<*ϕ*(*n*). The pair of numbers (*n*,*e*) makes up the public key.

**Note:** Two integers are co-prime if the only positive integer that divides them is 1.

1. Calculate *d* such that  *e*.*d*=1 *mod*  *ϕ*(*n*).

*d* can be found using the ***extended euclidean algorithm***. The pair (*n*,*d*) makes up the private key.

### 2. Encryption

Given a plaintext P, represented as a number, the ciphertext *C* is calculated as:

C = Pe *mod*  *n*.

### 3. Decryption

Using the private key (*n*,*d*), the plaintext can be found using:

P = Cd *mod*  *n*.