# Numerical Example of RSA 

Gilles Cazelais

To generate the encryption and decryption keys, we can proceed as follows.

1. Generate randomly two "large" primes $p$ and $q$.
2. Compute $n=p q$ and $\phi=(p-1)(q-1)$.
3. Choose a number $e$ so that

$$
\operatorname{gcd}(e, \phi)=1
$$

4. Find the multiplicative inverse of $e$ modulo $\phi$, i.e., find $d$ so that

$$
e d \equiv 1 \quad(\bmod \phi)
$$

This can be done efficiently using Euclid's Extended Algorithm.

The encryption public key is $K_{E}=(n, e)$ and the decryption private key is $K_{D}=(n, d)$.

The encryption function is

$$
E(M)=M^{e} \bmod n
$$

The decryption function is

$$
D(M)=M^{d} \bmod n
$$

These functions satisfy

$$
D(E(M))=M \quad \text { and } \quad E(D(M))=M
$$

for any $0 \leq M<n$.

Let's look at a numerical example.

1. Let $p=7$ and $q=13$ be the two primes.
2. $n=p q=91$ and $\phi=(p-1)(q-1)=72$.
3. Choose $e$. Let's look among the primes.

- Try $e=2 . \operatorname{gcd}(2,72)=2$ (does not work)
- Try $e=3 . \operatorname{gcd}(3,72)=3$ (does not work)
- Try $e=5 . \operatorname{gcd}(5,72)=1$ (it works)

4. Let's find $d$. We want to find $d$ such that

$$
e d \equiv 1 \quad(\bmod \phi)
$$

which is equivalent to find $d$ such that

$$
e d+\phi k=1
$$

for some integer $k$. Recall that $\operatorname{gcd}(e, \phi)=1$.
We can use the Extended Euclid's Algorithm to find integers $x$ and $y$ such that

$$
e x+\phi y=\operatorname{gcd}(e, \phi)
$$

If $e=5$ and $\phi=72$, we find $x=29$ and $y=-2$. Indeed, $5(29)+72(-2)=\operatorname{gcd}(5,72)=1$. Then,

$$
d=29
$$

In general, we use $d=x \bmod \phi$.
5. The encryption function is

$$
E(M)=M^{e} \bmod n=M^{5} \bmod 91
$$

The decryption function is

$$
D(M)=M^{d} \bmod n=M^{29} \bmod 91
$$

6. Suppose the message is $M=10$.

$$
\begin{gathered}
E(M)=E(10)=10^{5} \bmod 91=82 \\
D(E(M))=D(82)=82^{29} \bmod 91=10
\end{gathered}
$$

7. Let's see how to compute efficiently $82^{29} \bmod 91$ using the square-and-multiply algorithm.

$$
\begin{aligned}
&(82)^{1} \equiv 82 \quad(\bmod 91) \\
&(82)^{2} \equiv 81 \quad(\bmod 91) \\
&(82)^{4} \equiv(81)^{2} \equiv 9 \quad(\bmod 91) \\
&(82)^{8} \equiv(9)^{2} \equiv 81 \quad(\bmod 91) \\
&(82)^{16} \equiv(81)^{2} \equiv 9 \quad(\bmod 91)
\end{aligned}
$$

Since $29=16+8+4+1$ (in binary 29 is 11101 ), we deduce that

$$
\begin{aligned}
82^{29} & \equiv(82)^{16}(82)^{8}(82)^{4}(82)^{1} \quad(\bmod 91) \\
& \equiv(9)(81)(9)(82) \quad(\bmod 91) \\
& \equiv 10 \quad(\bmod 91)
\end{aligned}
$$

We conclude that $82^{29} \bmod 91=10$.

We choose $e=5$.

