Cryptosystème RSA - Karim Zayana et Paul Dorbec, Tangente Education

```
> p := nextprime(10^10); q := nextprime(p); n := p·q; phi := (p − 1)·(q − 1);
```

$$p := 10000000019$$
$$q := 10000000033$$
$$n := 100000000520000000627$$
$$\phi := 100000000500000000576 \quad (1)$$

```
>
```

Choix de e, calcul de d,

```
> d := nextprime(10^19); igcdex(d, phi,'e','v'); e := e mod phi;
```

$$d := 10000000000000000051$$
$$1$$
$$e := 82199951011149359995 \quad (2)$$

```
>
```

Vérification, oubli de p, q, phi

```
> e·d mod phi
```

$$1 \quad (3)$$

```
> p :='p'; q :='q'; phi :='phi';
```

$$p := p$$
$$q := q$$
$$\phi := \phi \quad (4)$$

```
> mssgAlphanumeriqueClair := "IloveU"; l := length(%);
```

$$mssgAlphanumeriqueClair := \text{"IloveU"}$$
$$l := 6 \quad (5)$$

> Padding (conversion du texte en une séquence de codes ascii)

```
>
> mssgNumeriqueClair := convert(mssgAlphanumeriqueClair, bytes);
```

$$mssgNumeriqueClair := [73, 108, 111, 118, 101, 85] \quad (6)$$

```
>
>
> mssgNumeriqueClair := sum(mssgNumeriqueClair[k]·10^(3·(k − 1)), k = 1 ..l);
```

$$mssgNumeriqueClair := 85101118111108073 \quad (7)$$

```
>
> mssgNumeriqueChiffré := Power(mssgNumeriqueClair, d) mod n
```

$$mssgNumeriqueChiffré := 4053868297883620455 \quad (8)$$

```
>
> mssgNumeriqueDéchiffré := mssgNumeriqueChiffré &^ e mod n
```

$$mssgNumeriqueDéchiffré := 85101118111108073 \quad (9)$$

```
>
> convert(mssgNumeriqueDéchiffré, base, 1000);
```

$$[73, 108, 111, 118, 101, 85] \quad (10)$$

```
> convert(%, bytes);
```

$$\text{"IloveU"} \quad (11)$$

```
> ifactor(n);
```

$$(10000000019)(10000000033) \quad \textbf{(12)}$$

```
> ifactor(10^100 + 16)
>
```