Exercices sur RSA

1. Python

3. Quand on traduit les lettres en chiffres, UPLOAD devient 211612150104. Ce nombre n'est pas plus petit que n. On doit donc le couper en morceaux. On a

$$M_1 = 2116$$
$$M_2 = 1215$$
$$M_3 = 0104$$

On calcule

$$C_1 \equiv M_1^e \equiv 2116^{17} \equiv 1581 \pmod{3233}$$
$$C_2 \equiv M_2^e \equiv 1215^{17} \equiv 574 \pmod{3233}$$
$$C_3 \equiv M_3^e \equiv 104^{17} \equiv 2170 \pmod{3233}.$$

On envoie C_1, C_2 puis C_3.

5. Quand on traduit les lettres en chiffres, SOLEIL devient 191512050912. Ce nombre n'est pas plus petit que n. On doit donc le couper en morceaux. On a

$$M_1 = 19151205$$
$$M_2 = 09122424$$

On a décidé d'ajouter des « X » à la fin pour avoir deux morceaux de la même taille. On calcule

$$C_1 \equiv M_1^e \equiv 19151205^{13} \equiv 9244707 \pmod{77075627}$$
$$C_2 \equiv M_2^e \equiv 9122424^{13} \equiv 44378501 \pmod{77075627}$$

On envoie C_1 puis C_2.

7. À l'aide d'un ordinateur, on trouve que $n = 7499 \cdot 10427$. Donc $p = 7499$ et $q = 10427$. À l'aide d'Euclide et de Bézout, on trouve d et t tels que $d \cdot e - t(p-1)(q-1) = 1$. On trouve $d = 45984793$ et $t = 10$.

On calcule

$$50140492^{45984793} \equiv 19151927 \pmod{78192073}$$

On obtient SOS.

Morale de l'histoire : n était trop petit.

9. Il est facile de factoriser les nombres de la forme $k^2 - 1$. En effet,

$$n = k^2 - 1 = (k-1)(k+1).$$

Donc $p = k - 1$ et $q = k + 1$. On a toute l'information nécessaire pour décrypter les messages envoyés à Marie-Louise.

11. Il est facile de factoriser les nombres de la forme k^2. En effet,

$$n = k^2 = k \cdot k.$$

Donc $p = k$ et $q = k$. On a toute l'information nécessaire pour décrypter les messages envoyés à Jean-Charles.

13. On peut trouver les valeurs de p et de q. En effet, on sait que $pq = n = 2361235232141$. De plus, on sait que

$$\begin{aligned}(p-1)(q-1) &= 2361232122300\\ pq - p - q + 1 &= 2361232122300\\ n - p - q + 1 &= 2361232122300\\ 2361235232141 - p - q + 1 &= 2361232122300\\ p + q &= 3109842.\end{aligned}$$

On a donc

$$\begin{aligned}pq &= 2361235232141\\ p + q &= 3109842.\end{aligned}$$

Deux équations, deux variable, il s'agit de résoudre...

15. Comme M est copremier avec pq (et que p et q sont des nombres premiers), M n'est pas divisible par p ni par q. Donc M^{q-1} n'est pas divisible par p et M^{p-1} n'est pas divisible par q. Donc M^{q-1} est copremier avec p et M^{p-1} est copremier avec q. Par le petit théorème de Fermat, on trouve donc

$$\begin{aligned}M^{(p-1)(q-1)} &\equiv \left(M^{q-1}\right)^{p-1} \equiv 1 \pmod{p}\\ M^{(p-1)(q-1)} &\equiv \left(M^{p-1}\right)^{q-1} \equiv 1 \pmod{q}.\end{aligned}$$

Donc $x = M^{(p-1)(q-1)}$ est une solution au système

$$\begin{aligned}x &\equiv 1 \pmod{p}\\ x &\equiv 1 \pmod{q}.\end{aligned}$$

Mais $x = 1$ est aussi une solution à ce système puisque

$$\begin{aligned}1 &\equiv 1 \pmod{p}\\ 1 &\equiv 1 \pmod{q}.\end{aligned}$$

Le théorème du reste chinois nous dit que la solution à ce système est unique modulo pq. On a donc

$$M^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$