Exercises on RSA

1. Python

3. When we translate letters to numbers, UPLOAD becomes 211612150104. This number is not smaller than n. We have to cut it into pieces. We end up with

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

We calculate

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

We send C_1, C_2, then C_3.

5. When we translate letters to numbers, SOLEIL becomes 191512050912. This number is not smaller than n. We have to cut it into pieces. We end up with

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

We add "X" at the end to have to have two segments of the same length.
We calculate

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

We send C_1 then C_2.

7. Using a computer, we find that $n = 7499 \cdot 10427$. So $p = 7499$ and $q = 10427$. With Euclid and Bézout, we can solve for d and t such that $d \cdot e - t(p-1)(q-1) = 1$. We find $d = 45984793$ and $t = 10$.
We calculate

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

The result is SOS.
Moral of the story : n was too small.

9. It is easy to factor numbers of the form $k^2 - 1$. They can be written

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

Therefore $p = k - 1$ and $q = k + 1$. We have all the information we need to decrypt the messages sent to Marie-Louise.

11. It is easy to factor numbers of the form k^2. They can be written

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

Therefore $p = k$ and $q = k$. We have all the information we need to decrypt the messages sent to Jean-Charles.

13. We can find the values of p and q. We know that $pq = n = 2361235232141$. In addition, we know that

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

Therefore, we see that

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

Two equations, two unknowns, all that's left is to solve...

15. Since M is coprime with pq (and p and q are primes), M is not divisible by p or q. Therefore M^{q-1} is not divisible by p and M^{p-1} is not divisible by q. So M^{q-1} is coprime with p and M^{p-1} is coprime with q. By Fermat's little theorem, we find that

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

Thus $x = M^{(p-1)(q-1)}$ is a solution to the system of equations

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

But $x = 1$ is also a solution since

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

By the chinese remainder theorem we know that the solution is unique modulo pq. We conclude that

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