Exercises on RSA

1. Implement (with your favorite language) Euclid, Bézout and the algorithm to test if a number is prime (the one that tests numbers up to $\sqrt{n}$).
2. Implement RSA.
3. Encrypt the message UPLOAD using RSA with $n = 3233$ et $e = 17$.
4. Encrypt the message PATATE using RSA with $n = 356519$ et $e = 11$.
5. Encrypt the message SOLEIL using RSA with $n = 77075627$ et $e = 13$.
6. In RSA, is it possible to have $e = 2$?
7. You intercept the following message : 50140492. It was encrypted using RSA item with values $n = 78192073$ and $e = 17$. Decrypt this message.
8. Send messages encrypted using RSA to a colleague. Try to guess their p and q. Ask them to do the same.
9. Marie-Louise publicly announces her n and e values to allow others to send her messages using RSA encryption. Upon closer inspection, you notice that $n = k^2 - 1$ for some integer k. Explain how to decrypt all the messages received by Marie-Louise.
10. Herménégilde publicly announces his n and e values to allow others to send him messages using RSA encryption. Upon closer inspection, you notice that $n = 4^k - 1$ for some integer k. Explain how to decrypt all the messages received by Herménégilde.
11. Jean-Charles publicly announces his n and e values to allow others to send him messages using RSA encryption. Upon closer inspection, you notice that $n = k^2$ for some integer k. Explain how to decrypt all the messages received by Jean-Charles.
12. Wilfrid's public values are $n = 2356828614859$ and $e = 43$. You hire a spy who finds out that $(p-1)(q-1) = 2356825501800$. What are the values of p and q ? What are the values of d and t ?
13. Virginie's public values are $n = 2361235232141$ et $e = 17$. You hire a spy who finds out that $(p-1)(q-1) = 2361232122300$. What are the values of p and q ? What are the values of d and t ?
14. You intercept the following message

    $$C = 91976306632746298303233033242907631$$

    which was encrypted using RSA. The numbers used are

    $$n = 300052220105410832294480576890956 73 \qquad \text{and} \qquad e = 13.$$

    Find the values of p, q, d, t, as well as the decrypted message in number form and in letter form.
15. In the explanation of RSA encryption, we used the following result.

Result : Let $p, q \in \mathbb{Z}$ be primes and $M \in \mathbb{Z}$ a positive integer coprime with pq. Then $M^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

To prove this result, we wrote : "we can apply the chinese remainder theorem". Explain exactly, and in detail, how the chinese remainder theorem is used to prove this.

16. Prove the following result.

Result : Let $p, q, r \in \mathbb{Z}$ be three primes and $M \in \mathbb{Z}$ a positive integer coprime with pqr. Then $M^{(p-1)(q-1)(r-1)} \equiv 1 \pmod{pqr}$.