Exercices sur RSA

1. Implémenter (avec votre langage préféré) Euclide, Bézout et l'algorithme pour tester si un nombre est premier (celui qui teste les nombres jusqu'à $\sqrt{n}$).
2. Implementer RSA.
3. Cryptez le message UPLOAD à l'aide du système RSA avec $n = 3233$ et $e = 17$.
4. Cryptez le message PATATE à l'aide du système RSA avec $n = 356519$ et $e = 11$.
5. Cryptez le message SOLEIL à l'aide du système RSA avec $n = 77075627$ et $e = 13$.
6. Dans le système RSA, est-ce possible d'avoir $e = 2$?
7. Vous interceptez le message suivant : 50140492. Il a été crypté suivant le sytème RSA avec les valeurs $n = 78192073$ et $e = 17$. Décryptez ce message.
8. Envoyez des messages à l'aide de RSA avec un collègue. Essayez de deviner son p et son q. Demandez-lui de faire de même.
9. Marie-Louise annonce publiquement ses valeurs de n et de e pour lui envoyer des messages à l'aide de la méthode RSA. En regardant attentivement, vous réalisez que $n = k^2 - 1$ pour un entier k. Expliquer comment décrypter tous les messages reçus par Marie-Louise.
10. Herménégilde annonce publiquement ses valeurs de n et de e pour lui envoyer des messages à l'aide de la méthode RSA. En regardant attentivement, vous réalisez que $n = 4^k - 1$ pour un entier k. Expliquer comment décrypter tous les messages reçus par Herménégilde.
11. Jean-Charles annonce publiquement ses valeurs de n et de e pour lui envoyer des messages à l'aide de la méthode RSA. En regardant attentivement, vous réalisez que $n = k^2$ pour un entier k. Expliquer comment décrypter tous les messages reçus par Jean-Charles.
12. Les valeurs publiques de Wilfrid sont $n = 2356828614859$ et $e = 43$. Vous engagez un espion qui réussit à découvrir que $(p-1)(q-1) = 2356825501800$. Quelles sont les valeurs de p et q ? Quelles sont les valeurs de d et t ?
13. Les valeurs publiques de Virginie sont $n = 2361235232141$ et $e = 17$. Vous engagez un espion qui réussit à découvrir que $(p-1)(q-1) = 2361232122300$. Quelles sont les valeurs de p et q ? Quelles sont les valeurs de d et t ?
14. Vous interceptez le message suivant

    $$C = 91976306632746298303233033242907631$$

    qui a été crypté avec la méthode RSA. Les nombres utilisés sont

    $$n = 3000522201054108322944805768909567 3 \qquad \text{et} \qquad e = 13.$$

    Trouvez les valeurs de p, q, d, t, le message décrypté en nombres et le message décrypté en lettres.

15. Dans l'explication de RSA, on a utilisé le résultat suivant.

    Résultat : Soit $p, q \in \mathbb{Z}$ deux nombres premiers et $M \in \mathbb{Z}$ un nombre positif copremier avec pq. Alors $M^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

    Pour démontrer ce résultat, on a écrit : « on peut appliquer le théorème du reste chinois ». Expliquez exactement, et avec tous les détails, comment le théorème du reste chinois est utilisé pour démontrer ce résultat.

16. Démontrer le résultat suivant.

    Résultat : Soit $p, q, r \in \mathbb{Z}$ trois nombres premiers et $M \in \mathbb{Z}$ un nombre positif copremier avec pqr. Alors $M^{(p-1)(q-1)(r-1)} \equiv 1 \pmod{pqr}$.