14. El siguiente mensaje fue cifrado usando RSA.

    32020, 47286, 177452, 80202, 185908, 32020, 47286, 215221, 196322, 17038, 176712, 0, 80202, 185908, 67201, 176712, 47286, 0,1, 28557, 32020, 80202, 0, 47286, 28557, 32020,176712, 177452, 32020.

    Los parámetros públicos son (N, e) = (256961, 53). Factoriza N utilizando el algoritmo $\rho - 1$ Pollard para encontrar un factor no trivial y así calcular N = pq, finalmente descifra el mensaje.

15 . En este ejercicio vas usar el software de tu preferencia (se recomienda factor.exe) para atacar dos claves RSA y posteriormente encontrar la clave privada d a partir del conocimiento solamente de la clave pública n y e que se indican, factorizando ese módulo n:

    a. Ataque 1:
       n=297240981923141721738067950563107725849673889821878776340809;
       e= 1999.

    b. Ataque 2:
       n=643590535502220839951864707825089693683144561318250505739519366732215705459;
       e = 101.

    c. ¿De qué tamaño en bits son las claves atacadas y los valores de p y q encontrados?

    d. ¿Cuánto tiempo has tardado en factorizar los dos módulos? Describir las carac terísticas de hardware del equipo en la cual fueron ejecutados estos ataques.
    e. En cada caso, genera la clave RSA con el software de tu preferencia (se recomienda ExpoCrip) para encontrar la clave privada.

18. Aplicar el test de primalidad de Solovay-Strassen a:
n = 661521349351105000008725817463 y concluir si es primo o compuesto.

20. Supongamos que n = 4633

a. Para x = 68, 69 y 96 calcula x^2 mod n.

b. Factoriza los residuos obtenidos en el paso anterior en la base: {−1, 2, 3, 5}.

c. Usa las tres factorizaciones en el paso anterior para generar una congruencia de la forma $y^2 \equiv x^2$ mod n y factoriza n.