Criptografía Pública: RSA

1. Calcula $3^{301} \, mod \, 11$, utilizando el teorema pequeño de Fermat.
2. Calcula $5^{596} \, mod \, 1234$.
3. Calcula el inverso de 7 en Z_{27}, utilizando el teorema de Euler generalizado.
4. Resuelve el sistema de congruencias siguiente:

$$\begin{aligned} x &\equiv 2 \, mod \, 3 \\ x &\equiv 2 \, mod \, 5 \\ x &\equiv 2 \, mod \, 7 \end{aligned}$$

5. Resuelve el sistema de congruencias siguiente:

$$\begin{aligned} x &\equiv 5 \, mod \, 3 \\ x &\equiv 3 \, mod \, 5 \\ x &\equiv 10 \, mod \, 7 \end{aligned}$$

6. Resuelve el sistema de congruencias siguiente:

$$\begin{aligned} x &\equiv 34 \, mod \, 46 \\ x &\equiv 31 \, mod \, 51 \\ x &\equiv 10 \, mod \, 55 \end{aligned}$$

7. Demuestra el teorema del resto chino.
8. Descifra el mensaje 10 enviado a un usuario de clave RSA $n = 35$ y $e = 5$.
9. En un sistema RSA se ha decidido que $p = 11$, $q = 29$ y $e = 3$. Da el valor de d y el cifrado de 100.
10. En un sistema RSA se ha decidido que $p = 17$, $q = 11$ y $e = 7$. Da el valor de d y el cifrado de $M = 88$. Comprueba que descifrado con el exponente d se recupera M.

11. Conociendo n y $\Phi(n)$, indica cómo se pueden obtener los primos p y q, tales que $n = pq$. Aplica esto a $n = 4386607$ y $\Phi = 4382136$.

12. Demuestra que el RSA es multiplicativo, es decir, $E_e(m_1)E_e(m_2)\, mod\, n = E_e(m_1 m_2)$.

13. Un usuario tiene como clave pública $(3599, 31)$. ¿Cuál es su clave privada?

14. Se quiere montar un RSA con parámetros $p = 17$ y $q = 19$. ¿Cuál de los parámetros $e = 33$ y $e = 35$ es correcto? ¿Cuáles son las claves públicas y privadas?

15. Presenta un algoritmo para la potenciación modular mediante cuadrados sucesivos. Comprueba con un ejemplo que funciona correctamente.

16. Presenta un algoritmo que calcule el inverso de un número en Z_m a través del algoritmo generalizado de Euler. Comprueba su efectividad y complejidad en relación al algoritmo extendido de Euclides.

17. Explica detalladamente en qué consiste la función de cifrado y descifrado del RSA y cuál es su base matemática.

18. Demuestra el teorema pequeño de Fermat.

19. Demuestra el teorema generalizado de Euler.

20. Demuestra la inyectividad en el algoritmo de encriptación de RSA.

21. Demuestra que si p es primo las únicas soluciones de la congruencia $x^2 \equiv 1\, mod\, p$ son las raíces triviales $x = \pm 1\, mod\, p$.

22. Demuestra que si p y q son números primos y si tuviéramos una solución x_0 no trivial de la congruencia $x^2 \equiv 1\, mod\, n$ (con $n = pq$), entonces se cumple obligatoriamente que

    a) mcd(n, $x_0 + 1$)=p ó q, ó

    b) mcd(n, $x_0 - 1$)=p ó q.

23. Escribe un pseudocódigo óptimo para el algoritmo de Miller-Rabin.

24. Da la evolución del algoritmo de Miller-Rabin sobre $p = 561$ y $a = 7$.

25. Estima cuál es la probabilidad de que mediante el algoritmo de Miller-Rabin, un número de longitud n bits responda m veces que sea primo, siendo éste en realidad compuesto.

26. Un usuario ha descubierto que su clave privada ha sido comprometida. En vez de generar un nuevo par de primos p, q y su módulo decide seguir con el módulo anterior y calcular un nuevo e y d. ¿Cómo se puede atacar?

27. Escribe un pseudocódigo óptimo para el algoritmo de las Vegas.

28. Supongamos que tenemos un RSA cuyo $n = 187$ ($p = 17,\ q = 11$), el exponente de cifrado es $e = 7$. Cifra y descifra el mensaje $M = 88$.

29. Supongamos que tenemos un RSA cuyo $n = 77$, el exponente de cifrado es $e = 7$ y, de algún modo, se ha averiguado que el exponente de descifrado es $d = 43$.

    a) Calcula razonadamente p y q (no es válido utilizar el hecho de que $7 \times 11 = 77$). Utiliza la potenciación modular a través de cuadrados sucesivos, usando $3\, mod\, 77 = 3$, $3^2\, mod\, 77 = 9$, $9^2\, mod\, 77 = 4$, $4^2\, mod\, 77 = 16$, $16^2\, mod\, 77 = 25$, $25^2\, mod\, 77 = 9$, $9^2\, mod\, 77 = 4$ y $4^2\, mod\, 77 = 16$.

    b) Explica qué tipo de algoritmo has utilizado y presenta su pseudocódigo.

    c) Explica razonada y explícitamente cuál es la base matemática del algoritmo que debes usar para calcular los dos factores primos.

    d) Una vez que has averiguado p y q, razona por qué es correcto que el exponente de descifrado sea $d = 43$.

30. Generación de número primos (Miller-Rabin).

    a) Explica razonada y detalladamente la evolución del algoritmo *Miller-Rabin* para el número $p = 221$, aplicándolo a dos valores distintos de la base $a = 5,\ 21$. *Nota: Utiliza la potenciación modular a través de cuadrados sucesivos, mostrando su evolución detallada.*

    b) ¿Qué muestran los resultados anteriores para las diferentes bases $a = 5$ y $a = 21$ respecto a la pregunta que el algoritmo de *Miller-Rabin* pretende resolver? Explica tu respuesta.

31. Supongamos que tenemos un RSA $n = 35$ y no sabemos los dos factores de $n = pq$. Se conoce que el exponente de cifrado es $e = 5$, y de alguna manera se ha averiguado que el exponente de descifrado es $d = 5$. Calcula a través del algoritmo tipo las vegas p y q.

32. Supongamos que A manda un mensaje M a B_1, B_2 y B_3, cuyas llaves públicas (e, n) son respectivamente: $(3, 46)$, $(3, 51)$, $(3, 55)$. Se han interceptado los mensajes cifrados que llegaron a B_1, B_2 y B_3, siendo estos respectivamente: 34, 31 y 10. ¿Cuál es el mensaje M que envío A a B_1, B_2 y B_3?

33. Escribe un pseudocódigo para codificar previamente el mensaje que se quiere enviar a través de un RSA de módulo n. Escribe también un pseudocódigo para decodificar el mensaje recibido que se envió a través de un RSA de módulo n.