Criptografía: Aspectos Teóricos y Prácticos — Práctico 4

1. Sean $N = 143041\,, k = 247$. Escribir una rutina en `SAGE` que, partiendo de $b = 1$ y luego poniendo $b \leftarrow b + 1$, halle un valor de $b \in \mathbb{Z}$ tal que $k \cdot N + b^2$ sea un cuadrado perfecto en $\mathbb{Z}$. A partir del valor de b hallado, hallar un factor no trivial de N.

2. Sea $N = 52907$. Utilizando los datos provistos abajo, hallar a y b tales que $a^2 \equiv b^2 \mod N$, y luego calcular $\gcd(N, a - b)$ para hallar un factor no trivial de N.

   - $399^2 \equiv 480 \mod N, \qquad 480 = 2^5 \cdot 3 \cdot 5.$
   - $763^2 \equiv 192 \mod N, \qquad 192 = 2^6 \cdot 3.$
   - $773^2 \equiv 15552 \mod N, \quad 15552 = 2^6 \cdot 3^5.$
   - $976^2 \equiv 250 \mod N, \qquad 250 = 2 \cdot 5^3.$

3. Escribir un algoritmo en `SAGE` que, dados un número $B > 0$ y un número $n \in \mathbb{N}$, utilizando la criba de Eratóstenes, decida si n es B-liso, y que en caso afirmativo devuelva la factorización de n; por ejemplo, en formato de una lista L cuyos componentes sean los pares (p, e_p) con p primo y $e_p \in \mathbb{Z}_{\geq 0}$ tales que $n = \prod_p p^{e_p}$.

4. Sean $p = 19079$ y $g = 17$.

   a) Hallar tres valores de $k \in \mathbb{N}$ tales que $g^k \mod p$ sea 5-liso.

   b) Utilizando los cálculos del ítem anterior (o más, si hiciera falta), álgebra lineal sobre cuerpos finitos y el Teorema Chino del Resto, calcular los logaritmos discretos $\log_g(2), \log_g(3)$ y $\log_g(5)$. Notar que $p - 1 = 2 \cdot 9539$, y 9539 es primo.

   c) Hallar $m \in \mathbb{N}$ tal que $19 \cdot g^m \mod p$ sea 5-liso.

   d) Utilizando los logaritmos discretos obtenidos en *b*) y el m hallado en *c*), calcule el logaritmo discreto $\log_g(19)$. Verfique que el valor hallado es correcto.

   Nota: En los ítems *a*) y *c*) se puede utilizar el algoritmo desarrollado en el ejercicio anterior.

5. Utilizando el critopsistema de clave pública Goldwasser-Micali, (des)encriptar los siguientes mensajes.

   a) La clave pública de Beto está dada por $N = 1842338473$ y $a = 1532411781$. Alicia encripta tres bits y le envía a Beto los mensajes cifrados

   $$1794677960, \quad 525734818, \quad \text{y} \quad 420526487.$$

   Desencriptar los mensajes de Alicia utilizando la factorización $N = 32411 \cdot 56843$.

   b) La clave pública de Beto está dada por $N = 781044643$ y $a = 568980706$. Encriptar los bits, $1, 1$ y 0 usando, respectivamente, los valores aleatorios

   $$r = 705130839, \quad r = 631364468, \quad \text{y} \quad r = 67651321.$$