Ejercicio Tema 3

Ana Buendía Ruiz-Azuaga

May 7, 2022

1 Ejercicio Tema 3

Este ejercicio es individualizado. Cada uno parte del númerode su DNI, supongamos por ejemplo 12340987. Dividimos dicho número en dos bloques,1234 y 0987. Si alguno de ellos es menor que 1000,rotamos las cifras a la izquierda hasta obtener un número mayor o igual que 1000, en nuestro caso 9870 (si alguien tuviese como un bloque el 0000, que coja un número mayor que 1000 cualquiera a su elección.Sean p y q los primeros primos mayores o iguales que los bloques anteriores. Concretamente, en el ejemplo p=1237 y q=9871. Sea n=pq y e el menor primo mayor o igual que 11 que es primo relativo con $\varphi(n)$. Sea $d = e^{-1} \mod \varphi(n)$

Tomamos mi dni, que es 77770080, y por lo tanto lo dividimos en dos bloques, 7777 y 0080. Como 0080 es menor que 1000, rotamos las cifras dos veces, obteniendo 8000.

Por tanto, consideramos p y q los siguientes primos a estos números, resultando $p = 7789$ y $q = 8009$.

Definimos ahora $n = pq = 62382101$, teniendo así que $\varphi(n) = 62366304$, y como e tomamos el menor primo mayor o igual que 11 que es primo relativo con $\varphi(n)$. Luego tenemos que $e = 17$.

Finalmente, calculamos el inverso de e módulo $\varphi(n)$, resultando así $d = 29348849$.

1.1 Apartado 1

Cifra el mensaje m=0xCAFE.

Para cifrar el mensaje, siendo $m = 0xCAFE$ calculamos (en mi caso en sagemath) $c = m^e \mod n$, obteniendo por tanto $c = 0x3494740$.

1.2 Apartado 2

Descifra el criptograma anterior.

Para descifrar el mensaje, calculamos $m = c^d \mod n$, de donde resulta $m = 0xCAFE$, que era el mensaje original.

1.3 Apartado 3

Intenta factorizar n mediante el método P-1 de Pollard. Para ello llega, como máximo a b=8.

Para factorizar, vamos a ir probando para los distintos valores de $b = 1, \cdots, 8$. Comenzamos probando con $m = 2$. Para hacer esto se ha usado el siguiente código:

```
m = 2
for b in range(1,9):
    print(b)
    pot = power_mod(m,factorial(b),n)
    print(n.gcd(pot-1))
```

Podemos ver que el máximo común divisor siempre es 1, por lo que repetimos el proceso para el siguiente valor de m, que es $m = 3$. Para automatizar este proceso, se ha implementado otro código también sagemath:

```
for m in range(1,1000):
    for b in range(1,9):
        pot = power_mod(m,factorial(b),n)
        mcd = n.gcd(pot-1)
        if(mcd != 1):
            print("MCD DISTINTO DE 1")
            print(m)
            print(b)
            print(mcd)
            break
```

Al ejecutar este código, nos fijamos en la salida. La primera solución es el propio n, por lo que no nos sirve, pero el siguiente resultado sí. La salida resultante es:

```
MCD DISTINTO DE 1
1
1
62382101
MCD DISTINTO DE 1
233
3
7789
```

de donde obtenemos que con $m = 233$ y $b = 3$, su máximo común divisor es 7789, luego uno de los factores de n es 7789. Y, calculando $n/7789 = 8009$ obtenemos el otro factor.

1.4 Apartado 4

Intenta factorizar n a partir de $\varphi(n)$.

Sabemos que $\varphi(n) = 62366304$, luego consideramos $(x-p)(x-q) = x^2-(p+q)x+n$, como $\varphi(n) = n+1-(p+q)$ tenemos $(x-p)(x-q) = x^2+(\varphi(n)-n-1)x+n$, luego p y q son las raices de este polinomio.

Calculamos por tanto las raíces del polinomio como se muestra:

```
x = var('x')
solve(x^2-(n+1-phi)*x+n, x)
```

Por tanto, se obtienen como raíces del polinomio 7789 y 8009, que serían p y q.

1.5 Apartado 5

Intenta factorizar n a partir de e y d.

Consideramos $k = ed - 1 = 498930432$ y $a \in \{2, 3, 5, 7, 11, 13, 17, 19\}$.

Como $a^k = a^{498930432} \equiv 1 \mod n$ para $a = 2, 3, 5, 7, 11, 13, 17, 19$ tomamos $k = k/2 = 249465216$.

Como $a^k = a^{249465216} \equiv 1 \mod n$ para $a = 2, 3, 5, 7, 11, 13, 17, 19$ tomamos $k = k/2 = 124732608$.

Como $a^k = a^{124732608} \equiv 1 \mod n$ para $a = 2, 3, 5, 7, 11, 13, 17, 19$ tomamos $k = k/2 = 62366304$.

Como $a^k = a^{62366304} \equiv 1 \mod n$ para $a = 2, 3, 5, 7, 11, 13, 17, 19$ tomamos $k = k/2 = 31183152$.

Como $a^k = a^{31183152} \equiv 1 \mod n$ para $a = 2, 3, 5, 7, 11, 13, 17, 19$ tomamos $k = k/2 = 15591576$.

Como $a^k = a^{15591576} \equiv 1 \mod n$ para $a = 2, 3, 5, 7, 11, 13, 17, 19$ tomamos $k = k/2 = 7795788$.

Como $3^{7795788} \mod n \equiv 11909382$ calculamos $(n, 3^{7795788} - 1) = 7789$ y $\frac{n}{7789} = 8009$ son los factores que buscamos.