Segunda entrega de ejercicios resueltos

(Criptografia)

Ulkei Szabolcs

D210871

(17)

$p = 47$
$q = 89$
$\Rightarrow n = 4183$

$\phi(n) = (p-1)(q-1) = 4048$

$e = 5$; $2 < e < \phi(n)$ ✓

$\phi(n) = 2^4 \cdot 11 \cdot 23$
$c = 5^1$
$\Rightarrow \text{mcd}(e, \phi(n)) = 1$

el inverso de $5 \bmod 4048 = 2429 = d$

$26^0 = 1$
$26^1 = 26$
$26^2 = 676$
$26^3 = 17,576$
$\Rightarrow$ Cada mensaje puede contener 2 letras

L → 11
U → 20
N → 13
A → 0

LU → $m_1 = 11 \cdot 26 + 20 = 306$
NA → $m_2 = 13 \cdot 26 + 0 = 338$

Finalmente:

$c_1 = m_1^e \bmod n = 2140$

$c_2 = m_2^e \bmod n = 2038$

$\Rightarrow$ envia en base 26:

$c_1 = 3 \cdot 26^2 + 4 \cdot 26^1 + 8 = DEI$

$c_2 = 3 \cdot 26^2 + 0 \cdot 26 + 10 = DAK$

$\Rightarrow$ DEI DAK

Descifrar:

$d = 2429$

$m_1 = c_1^d \bmod n = 306 = 11 \cdot 26 + 20 = LU$

$m_2 = c_2^d \bmod n = 338 = 13 \cdot 26 + 0 = NA$

$\Rightarrow m = m_1, m_2 = LU NA$

(18)

$$(p+q)^2 = p^2 + 2pq + q^2$$

$$(p-q)^2 = p^2 - 2pq + q^2$$

$$\frac{}{4pq} -$$

$$1 \Rightarrow (p+q)^2 - (p-q)^2 = 4pq = 4n$$

Entonces si puedo encontrar dos primos cuya suma cuadrado menos el diferencia cuadrado está igual con $4n$, puedo saber la clave secreta.

En caso en cual p y q son enormes esto puede ser calculando muy facil, simplemente con pruebas

Por que p y q son cercanos $\Rightarrow$
$(p-q)^2$ esta muy pequeña comparado
con el numeros primos

$\Rightarrow (p+q)^2 \approx 4pq$

↑ Asi voy a simbolizar que
son cercanos

$\Rightarrow p^2+q^2+2pq \approx 4pq \Rightarrow p^2+q^2 \approx 2pq$

Ahora tambien usando ⭐ el prop
que $p \approx q$ puedo decir que $2p^2 \approx 2pq$

$\Rightarrow p^2 \approx pq = n$

Así tenemos de calcular $\sqrt{n}$
En caso nosotros $\sqrt{n} \approx 88895$

Esto significa que p y q son también primos cerca de 88958, y como $n = pq$, todo que tenemos de hacer está encontrar una pareja cual satisfecha esta condición.

$n / 88959 \in \mathbb{N}$

$n / 88931 \in \mathbb{N}$

$n / 88961 \in \mathbb{N}$

$n / 88919 \in \mathbb{N}$

$n / 88967 \in \mathbb{N}$

$n / 88917 = 8893001 \in \mathbb{N} \Rightarrow p \; y \; q$ son encontrados.

19.)

$p = 4513$ < primera primo siguiente del 4508

$\alpha = 9$

$v = 1234$

$a = 13$

$\alpha^v = 9^{1234} \bmod 4513 = 1296$

$(\alpha^{va}) = 9^{1234 \cdot 13} \bmod 4513 = 1710$

$M = 2317 \Rightarrow m \cdot \alpha^{bv} \bmod 4513 = \overset{641}{\cancel{4169}}$

El mensaje enviado será $(1296, \overset{641}{\cancel{4169}})$

Recibiendo A va a calcular $(\alpha^v)^a =$

$= (1296)^{13} \bmod 4513 = 4449$ y obtiene el

mensaje $M = 641 \cdot (4449)^{-1} \bmod 4513 =$

$= 641 \cdot 2327 \bmod 4513 = 2317 = M$

(20)

$q = 4583$ (primo) | $a, b = ?$

$g = 3116$ (generador) | $X, Y, G = ?$

Con el generador y numero primo A y B pueden elijir un numero aleatorio. Sean $a = 4$ y $b = 7$

Con estos datos cada participante será capaz de calcular X respectivamente Y

$X = g^a \bmod q = 94\,273\,535\,815\,936 \bmod 4583$

$= 926$ ← esto lo sabe A y mandará para B

$Y = g^b \bmod q = 2299$ ← lo sabe B y mandará

Ahora A tiene: q, g, x, Y

B tiene: q, g, x, Y

A calcula $G = Y^a \bmod q = 2299^4 \bmod q =$

$= 1159$

B calcula $G = X^b \bmod q = 826^7 \bmod q =$

$= 1159$

$\Rightarrow$ Entonces tambien participantes tienen el numero $G = 1159$, sin de transmitar esto. Pueden usar para cifrar y descifrar mensajes.

22)

$p = 23$.

$y^2 = x^3 + 13x + (-7)$ que es del forma

$y^2 = x^3 + ax + b$ entonces si $\Delta \neq 0$

luego está bien definida.

$\Delta \equiv 4a^3 + 27b^2 = 4 + 27 \cdot 49 \neq 0$

x, y	$x^3 + 13x - 7 \bmod 23$	y^2
0	$-7 \bmod 23 = 16$	0
1	7	1
2	4	4
3	13	9
4	17	16
5	22	2
6	11	13
7	13	3
8	11	18
9	11	12
10	19	8
11	18	6
12	14	6
13	13	18
14	21	12
15	21	18
16	19	3
17	21	13
18	10	2
19	15	16
20	19	9
21	5	4
22	2	1

Los puntos de la curva dada son:

$\{O, (0,4), (0,19), (2,2), (2,21),$
$(3,6), (3,17), (7,6), (7,17),$
$(11,8), (13,6), (13,17), (22,5)$
$(22,18), (11,15)\}$

Por lo que en efecto $\#E = 14$