Segunda tarea

Profesor: Manuel Díaz Díaz
Ayudante:Gerardo Rubén López Hernández
Alumnos: César Eduardo Jardines Mendoza,
Emiliano Galeana Araujo

19 de mayo de 2020

1. Mediante el algoritmo de `Rho-Pollard` descomponer el número `n = 557437`, expresando claramente el proceso.[1].

i	x_i	y_i	MCD(| x_i - y_i |,mod)
0	5	26	1
1	26	458330	1
2	677	108979	1
3	458330	31871	1
4	157510	408810	1
5	108979	200153	1
6	227157	96572	1
7	31871	45835	1
8	110428	130880	1
9	408810	176439	1
10	429131	481892	1
11	200153	225945	1
12	455968	226069	389

Cuadro 1: Proceso de descomposición con `Rho-Pollard`

2. Sea $\mathbb{Z}_{10007}$ y $\mathbb{S} = \{2, 3, 5, 7\}$, calcular el índice de $\beta = 9451$ en $\alpha = 5$.

   a) Mostrar que $\alpha = 5$ es raíz primitiva de $\mathbb{Z}^*_{10007}$.

   b) $\rho_1 = 4063, \rho_2 = 5136$ y $\rho_0 = 9865$, úselos para calcular los logaritmos de 2, 3 y 7 base 5, ¿Por qué no es necesario calcular el logaritmo de 5 base α?

   c) Dados los cálculos anteriores obtener el índice de $\beta = 9451$ en α módulo 10007.

   Con 10007 que es primo y $\text{Ind}_5 5 = 1$.
   Con lo que $\varphi(10007) = 10006$.

   Ahora si 5 es raíz primitiva de $\mathbb{Z}^*_{10007}$ hay que ver que:
   $\text{ord}_{10007} 5 = \varphi(10007) = 10006$ Lo que es equivalente a demostrar que

$$5^{10006} \equiv 1 (\text{mod} 10007)$$

[1]Con el uso de un programa en python hicimos este ejercicio

Ahora podemos ver que $10006 = 2 \times 5003$, si pasa esto entonces basta ver que ninguna de estas es raíz primitiva, por lo que 5 es raíz primitiva.

Con el caso de $x = 4063$

$$5^x = 5^{4063} \bmod 10007 = 42 = 2 \times 3 \times 7$$

Con lo que podemos dar la congruencia siguiendo las respectivas propiedades de los índices

$$1)\, \mathrm{Ind}_5 2 + \mathrm{Ind}_5 3 + \mathrm{Ind}_5 7 \equiv 4063 \,(\mathrm{mod}\, 10006)$$

De manera similar

$$5^{5136} \bmod 10007 = 54 = 3^3 \times 2$$

Y a su vez

$$5^{9865} \bmod 10007 = 189 = 7 \times 3^3$$

que para cada una de estas ρ_i propuestas.

Obtendríamos las siguientes dos congruencias

$$2)\, 3\mathrm{Ind}_5 3 + \mathrm{Ind}_5 7 \equiv 9865 (\mathrm{mod}\, 10006)$$

$$3)\, \mathrm{Ind}_5 2 + 3\mathrm{Ind}_5 3 \equiv 5136 (\mathrm{mod}\, 10006)$$

Con lo que obtenemos las siguientes soluciones:

$$\log_5 2 = 6578$$

$$\log_5 3 = 6190$$

$$\log_5 7 = 1301$$

Ahora tendremos que calcular $\mathrm{Ind}_5\, 9451$.
Podemos ver que nos conviente encontrar un exponente n tal que, aplicando las propiedades de los índices, nos de un x tal que:

$$5^n \times 9451 \bmod 10007 = x$$

Entonces:

$$\mathrm{Ind}_5(5^n \times 9451 \bmod 10006) = \mathrm{Ind}_5 x$$

Y con eso decimos que:

$$n \times \mathrm{Ind}_5 5 + \mathrm{Ind}_5\, 9451 = \mathrm{Ind}_5 x \Longrightarrow n + \mathrm{Ind}_5\, 9451 = \mathrm{Ind}_5 x$$

$$\Longrightarrow \mathrm{Ind}_5\, 9451 = \mathrm{Ind}_5 x - n \,(\mathrm{mod} 10006)$$

y $x = 2^\alpha 3^\beta 5^\gamma 7^\delta$ esto quiere decir, que la descomposición en primos sea en factores de $\mathbb{S}$, y con esto,

$$\mathrm{Ind}_5 x = \sum_{\substack{p \in \{2,3,5,7\} \\ k \in \{\alpha,\beta,\gamma,\delta\}}} k \mathrm{Ind}_5\, p$$

Después de varios intentos, el exponente $n = 7736$ fuinciona por lo que de esta manera calculamos

$$5^n \times 9451 \bmod 10006 = 5^{7737} \times 9451 \bmod 10006 = 8400$$

Ahora, vemos que la descomposición de $8400 = 2^4 3^1 5^2 7^1$ que de igual forma, son los elementos que teniamos en $\mathbb{S}$. De aquí, aplicando de nuevo propiedades de los índices obtenemos que

$$\begin{aligned}\mathrm{Ind}_5 9451 &= (4\,\mathrm{Ind}_5 2 + \mathrm{Ind}_5 3 + 2\,\mathrm{Ind}_5 5 + \mathrm{Ind}_5 7 - n) \bmod 10006 \\ &= (4 \times 6578 + 6190 + 2 + 1301 - 7736) = 6057\end{aligned}$$

Con lo obtendríamos $\mathrm{Ind}_5\, 9451 = 6057$.

3. Descifrar el siguiente mensaje en `RSA` con parámetros (2257, 7) con las siguientes condiciones.

   3I) Aplicar el algoritmo de criba cuadrática para descomponer a 2257.

   a) Usar la siguiente base $\mathbb{S} = \{-1, 2, 3, 17\}$.

   b) Dar $\mathbb{M}, \mathbb{B}$ y decir para qué sirven.
   Sea n = 2257, descompondremos a n con el algoritmo de la criba cuadrática:

   - Calculamos a $\mathbb{M}\left[(e^{\sqrt{In(n)In(In(n))}^{\frac{3\sqrt{2}}{4}}})\right] = 67$.
   - Calculamos a $\mathbb{B}\left[(e^{\sqrt{In(n)In(In(n))}^{\frac{\sqrt{2}}{4}}})\right] = 4$.

     $\mathbb{M}, \mathbb{B}$ Nos sirven (respectivamente) para saber el rango de búsqueda y el número mínimo de elementos que se puedan factorizar usando elementos de nuesrta base.
   - Se calcula a $m = \sqrt{n} = 47$.
   - Se forma $q(x) = (x + m)^2 - n = (x + 47)^2 - 2257$.
     En la siguiente tabla podemos observar todos los valores que se pueden factorizar en nuestro rango (-67,67).[2]

[2]Se hizo mediante un programa, en caso de requerirlo, nos lo pueden pedir.

i	x	$b_i = q(x)$	$b_i = \prod_{k=1}^{4} P_i$	a_i	w_i	v_i
1	-56	-2176	$(-1^1)(2^7)(3^0)(17^1)$	-9	(1, 7, 0, 1)	(1, 1, 0, 1)
2	-55	-2193	$(-1^1)(2^0)(3^1)(17^1)$	-8	(1, 0, 1, 1)	(1, 0, 1, 1)
3	-47	-2257	$(-1^1)(2^0)(3^0)(17^0)$	0	(1, 0, 0, 0)	(1, 0, 0, 0)
4	-39	-2193	$(-1^1)(2^0)(3^1)(17^1)$	8	(1, 0, 1, 1)	(1, 0, 1, 1)
5	-38	-2176	$(-1^1)(2^7)(3^0)(17^1)$	9	(1, 7, 0, 1)	(1, 1, 0, 1)
6	-24	-1728	$(-1^1)(2^6)(3^3)(17^0)$	23	(1, 6, 3, 0)	(1, 0, 1, 0)
7	-23	-1681	$(-1^1)(2^0)(3^0)(17^0)$	24	(1, 0, 0, 0)	(1, 0, 0, 0)
8	-22	-1632	$(-1^1)(2^5)(3^1)(17^1)$	25	(1, 5, 1, 1)	(1, 1, 1, 1)
9	-21	-1581	$(-1^1)(2^0)(3^1)(17^1)$	26	(1, 0, 1, 1)	(1, 0, 1, 1)
10	-17	-1357	$(-1^1)(2^0)(3^0)(17^0)$	30	(1, 0, 0, 0)	(1, 0, 0, 0)
11	-16	-1296	$(-1^1)(2^4)(3^4)(17^0)$	31	(1, 4, 4, 0)	(1, 0, 0, 0)
12	-11	-961	$(-1^1)(2^0)(3^0)(17^0)$	36	(1, 0, 0, 0)	(1, 0, 0, 0)
13	-6	-576	$(-1)(2^6)(3^2)(17^0)$	41	(1,6,2,0)	(1,0,0,0)
14	-4	-408	$(-1)(2^3)(3^1)(17^1)$	43	(1,3,1,1)	(1,1,1,1)
15	0	-48	$(-1)(2^4)(3^1)(17^0)$	47	(1,4,1,0)	(1,0,1,0)
16	2	144	$(-1^0)(2^4)(3^2)(17^0)$	49	(0,4,2,0)	(0,0,0,0)
17	3	243	$(-1^0)(2^0)(3^5)(17^0)$	50	(0,0,5,0)	(0,0,1,0)
18	8	768	$(-1^0)(2^8)(3^1)(17^0)$	39	(0,8,1,0)	(0,0,1,0)
19	12	1224	$(-1^0)(2^3)(3^2)(17^1)$	59	(0, 3, 2, 1)	(0, 1, 0, 1)
20	15	1587	$(-1^0)(2^0)(3^1)(17^0)$	62	(0, 0, 1, 0)	(0, 0, 1, 0)
21	26	3072	$(-1^0)(2^{10})3^1)(17^0)$	73	(0, 10, 1, 0)	(0, 0, 1, 0)
22	29	3519	$(-1^0)(2^0)(3^2)(17^1)$	76	(0, 0, 2, 1)	(0, 0, 0, 1)
23	30	3672	$(-1^0)(2^3)(3^3)(17^1)$	77	(0, 3, 3, 1)	(0, 1, 1, 1)
24	31	3827	$(-1^0)(2^0)(3^0)(17^0)$	78	(0, 0, 0, 0)	(0, 0, 0, 0)
25	38	4968	$(-1^0)(2^3)(3^3)(17^0)$	85	(0, 3, 3, 0)	(0, 1, 1, 0)
26	47	6579	$(-1^0)(2^0)(3^2)(17^1)$	94	(0, 0, 2, 1)	(0, 0, 0, 1)
27	52	7544	$(-1^0)(2^3)(3^0)(17^0)$	99	(0, 3, 0, 0)	(0, 1, 0, 0)
28	53	7743	$(-1^0)(2^0)(3^1)(17^0)$	100	(0, 0, 1, 0)	(0, 0, 1, 0)
29	61	9407	$(-1^0)(2^0)(3^0)(17^0)$	108	(0, 0, 0, 0)	(0, 0, 0, 0)

c) Expresar el proceso claramente por el cual se obtienen x y y, con los cuales se puede descomponer 2257.

- Se tiene que T = $\{v_{16}\}$ pues su suma coordenada a coordenada es congruente con cero módulo dos.
- Se tiene que W = $\{\alpha_{16}\}$ = (0,4,2,0); $L_1 = 0, L_2 = 2, L_3 = 1, L_4 = 0$
  - x = (a_{16} mod 2257) = 49
  - y = $(-1^0)(2^2)(3^1)(17^0)$ = -12 mod 2257 = 2245

d) Dar los valores para los cuales se obtienen x e y tales que $(x - y, 2257)$ es un factor no trivial de 2257.

- Ahora 49 $\not\equiv \pm$ 2245 (mod 2257). Así calculamos mcd ($x - y$, n) = mcd (-2196,2257) = 61
- Así, los dos factores no triviales de n = 2257 son 61 (por lo anterior) y 37 por $(\frac{2257}{61})$

3II) Descifrar el mensaje mediante el siguiente proceso:

a) Dar las llaves pública y privada de `RSA` y su proceso de como se obtienen de manera resumida pero clara.
Buscaremos a dos primos p y q tales que p $\neq$ q, tomaremos a p = 37 y a q = 61, entonces con esto se obtiene que:

$$n = p * q$$

$$\theta = (p-1) * (q-1)$$

lo que tendríamos que:

$$n = 37 * 61 = 2257$$

$$\theta = (p-1) * (q-1) = 2160$$

Con esto nos referimos a que:

$$(p-1) = 36 y (q-1) = 60$$

Ahora solo nos falta buscar un número que no tenga multiplos en comun con θ, este numeró deberá de estar entre $1 < e < \theta$ tal que MCD(θ,e)=1, entonces con esto obtenemos que:

$$e = 7$$

$$MCD(2160, 7) = 1$$

Despues de esto se calculará el exponente privado de RSA (dado por d = inv(e,θ)).

$$d = inv(7, 2160) = 1543$$

con lo que nuestras llaves quedarían de esta forma:
Llave pública: (e,n) = (7,2257)
Llave privada: (d,n) = (1543,2257)

b) Descifrar el mensaje. 585 1660 585 2011 431 322 431 322 274 585 322 431 585 1660 68 322 1660 1933 1132 128 1995 322 2218 322 128 399 585 1660 128 399 322 585 2011 1933 1132 1411 2011 585 1660 128 399 233 233 322 2218 585 274 319 2011 585 1660 128 399 233 233 319 1660 319 2011 399 68 1660 399 1387 399 128 322 274 322 2218 399 2187 319 2011 399 68 1660 399 1387 399 128 322 585 1660 585 2011 431 585 128 322 2011 319 1418 1132 585 2011 322 233 585 128 319 1660 233 319 1 322 2011 399 128 319 1411 322 284 585 274 322 1660 1418 1132 585 585 2011 431 319 585 2011 431 322 1933 1132 1411 2187 399 284 585 274 431 399 2187 319

Sugerencia el polinomio $q(x)$ no sobre pasa $x = \pm 27$.

Ya con nuestras llaves y dandole un número a cada letra del abecedarió:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Usando nuestras llaves y usando nuestra llave de desifrado, el proceso de decifrado es:

$$585^{1543} mod 2257 = 4$$

$$1660^{1543} mod 2257 = 13$$

$$585^{1543} mod 2257 = 4$$
$$2011^{1543} mod 2257 = 18$$
$$\vdots$$
$$\vdots$$

Seguimos con el proceso hasta terminar con el texto cifrado. [3] Después de agregar espacios donde tienen que ir, tenemos el siquiente texto:

`En esta tarea tengan mucha paciencia es muy sencilla pero sencillo no significa rapido significa en este caso que sale con lo basico ya veran que esto esta muy divertido.`

[3] Usamos un programa para automatizar los cambios de números con los módulos y reemplazar las palabras.