

Universidad Nacional  
Autónoma de México

**Equipo**

Calderón Fernández Gabriel  
Cova Pacheco Felipe de Jesús

**Profesor**

Manuel Díaz Díaz

**Materia**

Criptografía y Seguridad

**Tarea**

No. 2

**Fecha de entrega**

Lunes 5 de noviembre de 2018

2. En este ejercicio vas a usar el software de tu preferencia (Se recomienda factor.exe) para atacar dos claves RSA y posteriormente encontrar la clave privada d a partir del conocimiento solamente de la clave pública n y e que se indican, factorizando ese módulo n:

a. Ataque 1

$$n = 297240981923141721738067950563107725849673889821878776340809;$$

$$e = 1999.$$

$$= 449329386292232535250647435097$$

$$\ast 661521349357105339668937661297$$

b. Ataque 2.

$$n = 643590535502220839951864707825089693683144561318250505739519366732215705459;$$

$$e = 101$$

$$= 11348055580883272011090856053175361113$$

$$\ast 56713727820156410577229101238628035243$$

c. ¿De qué tamaño en bits son las claves atacadas y los valores de  $p$  y  $q$  encontrados?

•) En la clave del inciso a), obtuvimos que el tamaño en bits es igual a 198 bits y el tamaño de los factores es de 99 bits para el primero y 100 bits para el segundo factor

•) Para la clave del inciso b), tenemos que el tamaño en bits es 249 bits y asimismo, el tamaño de los factores son 124 bits y 126 bits para el primero y segundo, respectivamente.

Nota: Cabe mencionar que se nos facilitó el cálculo de esto, usando un método muy útil, llamado `bitLength()` de la clase `BigInteger`.

d. ¿Cuánto tiempo has tardado en factorizar los dos módulos?

Describir las características de hardware del equipo en la cual fueron ejecutados estos ataques.

•) Para el primer inciso, tardó 2.82 segundos

•) Para el segundo inciso, tardó 2 minutos con 41.6 segundos

∴) Equipo:

-Procesador 2.6GHz Intel Core i7

-8 GB RAM

-Sistema operativo macOS Mojave

e. En cada caso, genera la clave RSA con el software de tu preferencia (Se recomienda Expocrip) para encontrar la clave privada

•) Clave privada del inciso a):

121334498811870117305565955360600977739333491210  
799759229642543

•) Clave privada del inciso b):

26125952431278271720818270317652155879424152370896676  
9794051245116404946765

4. Supongamos que  $n = 4633$

a. Para  $x = 68, 69$  y  $96$  calcula  $x^2 \bmod n$ .

$$68 \times 68 = 4624 \bmod 4633 = 4624$$

$$69 \times 69 = 4761 \bmod 4633 = 128$$

$$96 \times 96 = 9216 \bmod 4633 = 4583$$

b. Factoriza los residuos obtenidos en el paso anterior en la base:  $\{-1, 2, 3, 5\}$ .

Tomemos en cuenta que  $4624 = -9 \bmod 4633$

y que  $4583 = -50 \bmod 4633$ ,

entonces para  $x = 68$ , tenemos que:

$$x^2 = -9 = -1 \times 3 \times 3 \bmod 4633,$$

para  $x = 69$ , tenemos:

$$x^2 = 128 = 2^7 \bmod 4633$$

para  $x = 96$ , tenemos que  $x^2 = -50 = -1 \times 2 \times 5 \times 5 \bmod 4633$

y ya lo factorizamos en término de la base dada.

c. Usa las tres factorizaciones en el paso anterior para generar una congruencia de la forma  $y^2 \equiv x^2 \bmod n$  y factoriza  $n$ .

Tenemos que  $(68 \times 69 \times 96)^2 = -1^2 \times 2^8 \times 3^2 \times 5^2 \bmod 4633$ ,

enseguida nos damos cuenta que del lado derecho, todo tiene exponentes pares, entonces se cumple que  $-1^2 \times 2^8 \times 3^2 \times 5^2 = (-1 \times 2^4 \times 3 \times 5)^2 = -240$ . Por lo tanto tenemos que  $(68 \times 69 \times 96)^2 = (-240)^2 \bmod 4633$

Además ...

Además,  $63 \times 69 \times 96 = 1031 \pmod{4633}$ ,  
entonces tenemos  $1031^2 = (-240)^2 \pmod{4633}$

Por lo tanto aquí notamos que el algoritmo de la Criba Cuadrática funciona, porque busca números  $x, y$  tales que  
 $x^2 = y^2 \pmod{n}$ , pero  $x! = y \pmod{n}$  y  $x! = y \pmod{n}$   
entonces 1031 y -240 cumplen esas dos cosas.

Entonces un factor de 4633 es  $\text{Med}(1031 - (-240), 4633) = 41$

5. Encontrar un factor no trivial de  $N=87463$  utilizando el algoritmo de la criba cuadrática.

Calculamos los parámetros  $M$  y  $B$  para determinar el tamaño del intervalo de criba y de la base de factores.

$$B = \left\lfloor \left( e^{\sqrt{\ln(N) \ln(\ln(N))}} \right)^{\frac{\sqrt{2}}{4}} \right\rfloor = 6$$

$$M = \left\lfloor \left( e^{\sqrt{\ln(N) \ln(\ln(N))}} \right)^{\frac{3\sqrt{2}}{4}} \right\rfloor = 264$$

$\Rightarrow$  El intervalo de criba es  $[264, 264]$ .

Para la base de factores, debemos de encontrar 5 números primos que cumplen  $\left(\frac{N}{p}\right) = +1$ .

P	3	5	7	11	13	17	19	23	29
$\left(\frac{N}{P}\right)$	1	-1	-1	-1	1	1	1	-1	1

$\Rightarrow$  Nuestra base de factores es:  $F = \{-1, 2, 3, 13, 17, 19, 29\}$

Calculamos los valores  $sp_1$  y  $sp_2$  para cada elemento  $p$  de  $F$  con la ecuación

$$sp_1 = x_1 - \lfloor \sqrt{N} \rfloor \pmod{p} \quad y \quad sp_2 = x_2 - \lfloor \sqrt{N} \rfloor \pmod{p}.$$

P	2	3	13	17	19	29
x	1	1, 2	5, 8	7, 10	5, 14	12, 17
$Sp_1, Sp_2$	0	0, 1	9, 12	1, 4	4, 14	7, 12

Los valores  $Sp_1$  y  $Sp_2$  nos indican para cada factor primo en  $F$  en qué momento empieza la progresión aritmética.

Se hará una tabla con el proceso de criba para un pequeño intervalo de  $[M, M]$ , en este caso  $[0, 12]$ . Notamos que  $\lfloor \sqrt{N} \rfloor = 295$ .

$i$	$i + \lfloor \sqrt{N} \rfloor$	$d(ai)$	-1	2	3	13	17	19	29	$d(ai)$ Final
0	295	438	X	X	X					73
1	296	153			X		X			1
2	297	746		X						373
3	298	1341			X					149
4	299	1938		X	X		X	X		1
5	300	2537								2537
6	301	3138		X	X					523
7	302	3741			X				X	43
8	303	4346		X						2173
9	304	4953			X	X				127
10	305	5562		X	X					103
11	306	6173								6173
12	307	6786		X	X	X			X	1

Encontramos tres elementos que tienen la propiedad de ser  $\beta$ -lisos, es decir, factorizan completamente en nuestra base de factores  $F$ . Se debe de realizar a estos tres números  $\beta$ -lisos el proceso de obtención del vector de exponentes módulo 2.

$d(ai)$	Factorización	Vector de exponentes	Vector de exponentes (módulo 2)
153	$3^2 \cdot 17$	$[0, 0, 2, 0, 1, 0, 0]$	$[0, 0, 0, 0, 1, 0, 0]$
1938	$2 \cdot 3 \cdot 17 \cdot 19$	$[0, 1, 1, 0, 1, 1, 0]$	$[0, 1, 1, 0, 1, 1, 0]$
6786	$2 \cdot 3^2 \cdot 13 \cdot 29$	$[0, 1, 2, 1, 0, 0, 1]$	$[0, 1, 0, 1, 0, 0, 1]$

Una vez acabado el proceso de criba, debemos tener al menos  $B+1$  números que factoríen la base de factores.

Ahora construimos una matriz  $A$ , donde las columnas son los vectores de los exponentes módulo 2.

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \cdot \bar{v} = \bar{0}$$

Buscamos una posible solución para el sistema anterior

$$\bar{v} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \Rightarrow \text{la solución involucra los cuatro primeros columnas, es decir, que el producto de los cuatro números } d(a_i) = (i+N)^2 - N \text{ asociados}$$

es un cuadrado

$$\Rightarrow x^2 = (265 \cdot 278 \cdot 296 \cdot 307)^2 = 44816869024979257600$$

Ahora si tomamos

$$y^2 = (265^2 - N)(278^2 - N)(296^2 - N)(307^2 - N) = 182178565001329$$

Tenemos dos números cuadrados que cumplen

$$x^2 \equiv y^2 \pmod{N}$$

ya que

$$44816869024979257600 \equiv 10093 \pmod{N}$$

$$182178565001319 \equiv 10093 \pmod{N}$$

pero

$$x \not\equiv y \pmod{N}$$

donde tenemos

$$6694540240 \equiv 34757 \pmod{n}$$

$$13497354 \equiv 28052 \pmod{N}$$

Ahora solo queremos comprobar si  $x$  e  $y$  proporcionan un factor no trivial de  $N$ . Para ello calculamos

$$\text{mcd}(x+y, N) = \text{mcd}(6708037594, N) = 587$$

$$\text{mcd}(x-y, N) = \text{mcd}(6681642886, N) = 149$$

∴ Podemos decir que  $\underline{\underline{N=587 \cdot 149}}$

7: El entero  $p=458009$  es primo y  $\alpha=2$  tiene orden 57251 en  $\mathbb{Z}_p^*$ . Use el algoritmo Rho de Pollard para calcular el Logaritmo Discreto en  $\mathbb{Z}_p^*$  de  $B=56851$  en base  $\alpha$ . Tome el valor inicial  $x_0=1$  y defina la partición  $\{S_1, S_2, S_3\}$  como el ejemplo visto en clase. Encuentre el entero más pequeño  $i$  s.t.  $x_i \equiv x_{2i} \pmod{p}$  y calcule el log. discreto buscado. Elija 10 iteraciones y muestre los resultados.

i	$x_i$	$a_i$	$b_i$	$x_{2i}$	$a_{2i}$	$b_{2i}$
1	56851	0	1	324697	0	2
2	324697	0	2	424840	1	3
3	212420	0	3	232522	2	8
4	424840	1	3	295215	4	18
5	390243	1	4	212527	16	72
6	232522	2	8			
7	52464	2	9			
8	295215	4	18			
9	111669	8	36			
10	212527	16	72			

Tenemos que  $x_{676} = x_{898} = 180178$ . Calculamos  $r = b_{676}^{-1} b_{898}$  mod 57251 = 31778,  $r^{-1} = 48652$

$$\begin{aligned} \log_2(56851) &= 48652(34505 - 7765) \text{ mod } 57251 \\ &= 40007 \end{aligned}$$