Criptografía y Seguridad - Tarea 2

Rivera González Damián
Tadeo Guillén Diana G

October 29, 2019

Ejercicio 1

Mostrar las siguientes propiedades del símbolo de Jacobi, partiendo de los demostrado en clase del símbolo de Lengendre

Ejercicio 2

a) Muestra que 2 es generados de $\mathbb{Z}^*_{2027}$

b) Mediante el cálculo de índices encontrar $\log_2(13) mod(2027)$, tome como base $B = \{2, 3, 5, 7, 11\}$

   Tenemos la siguiente información: $p = 2027, \alpha = 2, n = 2026, \beta = 13$. Entonces queremos encontrar $\log_2(13) mod(2027)$

   1) Tenemos como base $B = \{-1, 2, 3, 5, 7, 11\}$ (agregamos a -1 ya que n es grande)
   2) Buscamos las relaciones que involucren a los elementos de S

$$\begin{aligned}
2^{596} mod(2027) &= 121 = 11^2 \\
2^{15} mod(2027) &= 336 = 2^4 \cdot 3 \cdot 7 \\
2^{789} mod(2027) &= 135 = 3^3 \cdot 5 \\
2^{1041} mod(2027) &= 154 = 2 \cdot 7 \cdot 11 \\
2^{1040} mod(2027) &= 77 = 7 \cdot 11
\end{aligned}$$

   Con lo se genera un sistema de ecuaciones de 5×5

$$\begin{aligned}
15 &= 4\log_2(2) + \log_2(3) + \log_2(7) mod(2026) \\
789 &= 3\log_2(3) + \log_2(5) mod(2026) \\
1041 &= \log_2(2) + \log_2(7) + \log_2(11) mod(2026) \\
1040 &= \log_2(7) + \log_2(11) mod(2026) \\
586 &= 2\log_2(11) mod(2026)
\end{aligned}$$

   3) Resolviendo el sistema de ecuaciones obtenemos:

$$\begin{aligned}
\log_2(2) &= 1 \\
\log_2(3) &= -731 = 1295 \\
\log_2(5) &= 2982 = 956 \\
\log_2(7) &= 742 \\
\log_2(11) &= 298
\end{aligned}$$

4) Elegimos $k = 30$
Calculamos $\beta \cdot \alpha^k = (13)(2)^{30} mod(2027) = 100 = 2^2 \cdot 5^2$
aplicando $\log_2$ en ambos lados, tenemos:

$$\begin{aligned}
\log_2(13) + 30\log_2(2) &= 2\log_2(2) + 2\log_2(5) mod(2026) \\
\log_2(13) + 30 \cdot 1 &= 2\log_2(2) + 2\log_2(5) mod(2026) \\
\log_2(13) &= 2\log_2(2) + 2\log_2(5) - 30 mod(2026) \\
&= (2(1) + 2(956) - 30) mod(2026) \\
&= 1884 mod 2026 \\
&= 1884
\end{aligned}$$

c) Sea el siguiente mensaje cifrado con Gammal de parámetros públicos $gammal(n = 2027, \alpha = 2, \alpha^k = 13)$, con base a lo previo del ejercicio dos, descifra el mensaje.

Ya que sabemos está cifrado con *gammal*, entonces podemos ver a cada par ordenado (X, Y) como

$$\begin{aligned}
&X = \alpha^b mod(2027) = 2^b mod(2027) \\
&Y = (\alpha^k)^b mod(2027) = (2^{1884})^b \cdot m(mod(2027)) = 13^b \cdot m(mod(2027))
\end{aligned}$$

Esto porque ya conocemos k que cumple $\alpha^k = 13$, que es 1884

Ahora tomamos el primer par $(128, 793)$ y obtenemos los valores para b y m entonces

$$\begin{aligned}
&X = 128 = 2^b mod(2027) \\
&\Rightarrow\ b = 7 \\
&Y = 793 = 13^7 \cdot m(mod(2027)) \\
&\Rightarrow\ m = 4 \\
&\Rightarrow\ (128, 793) = E
\end{aligned}$$

Obtenemos la primer letra del mensaje, E, revisando un alfabeto indexado con 26 letras (sin la Ñ). Ahora tomamos el segundo par $(128, 528)$, como ya conocemos que $b = 7$ entonces basta con revisar quien es Y

$$\begin{aligned}
&Y = 528 = 13^7 \cdot m(mod(2027)) \\
&\Rightarrow\ m = 18 \\
&\Rightarrow\ (128, 528) = S
\end{aligned}$$

Obtenemos la segunda letra del mensaje, S. Y haciendo esto para todos los demás pares obtenemos cada letra para cada par diferente:

$$(128, 793) = E$$
$$(128, 528) = S$$
$$(128, 1233) = T$$
$$(128, 264) = J$$
$$(128, 1850) = R$$
$$(128, 1410) = C$$
$$(128, 1586) = I$$
$$(128, 1762) = O$$
$$(128, 87) = A$$
$$(128, 352) = M$$
$$(128, 1938) = U$$
$$(128, 704) = Y$$
$$(128, 1498) = F$$
$$(128, 1674) = L$$
$$(128, 176) = G$$
$$(128, 1938) = U$$
$$(128, 1145) = Q$$

Con lo cual obtenemos el mensaje descifrado:

"ESTE EJERCICIO ESTA MUY FACIL AL IGUAL QUE LA TAREA"

Ejercicio 3

Mediante el algoritmo de la criba cuadrática descomponer a $n = 87463$

a) Encontrar B y M

Calculamos B y M de la siguiente manera:

$$B = \lfloor (e^{\sqrt{\ln(87463)\cdot\ln(\ln(87463))}})^{\frac{\sqrt{2}}{4}} \rfloor = 6$$

$$M = \lfloor (e^{\sqrt{\ln(87463)\cdot\ln(\ln(87463))}})^{\frac{3\sqrt{2}}{4}} \rfloor = 264$$

b) Dar la base, sugerencia: en la base los enteros no pasa del número 31 Escogemos la base de factorización como

$$S' = \{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$$

de donde tomamos a

$$S = \{-1, 2, 3, 13, 17, 19, 29\}$$

Esto por que cada elemento $p \in S$ debe cumplir que $x^2 \equiv 87463 mod(p)$ esto porque se debe cumplir que $\left(\frac{n}{p}\right) = 1$. Entonces tenemos que

$$\begin{aligned}
x^2 &\equiv (87463) mod(3) \rightarrow 87463^1 \equiv (1) mod(3) \\
x^2 &\equiv (87463) mod(13) \rightarrow 87463^6 \equiv (1) mod(13) \\
x^2 &\equiv (87463) mod(17) \rightarrow 87463^8 \equiv (1) mod(17) \\
x^2 &\equiv (87463) mod(19) \rightarrow 87463^9 \equiv (1) mod(19) \\
x^2 &\equiv (87463) mod(29) \rightarrow 87463^{14} \equiv (1) mod(29)
\end{aligned}$$

Y agregamos a -1 y 2 porque estos siempre son agregados a la base

c) Descomponer n
Generamos a $m = \lfloor \sqrt{87463} \rfloor = 295$ Calculamos la tabla con $t + 1 = 8$ relaciones de x:

i	x	q(x)	Factores de q(x)	a_i	v_i
1	1	153	$3^2 \cdot 17$	296	(0,0,1,0,1,0,0)
2	4	1938	$2 \cdot 3 \cdot 17 \cdot 19$	299	(0,1,1,0,1,1,0)
3	12	6786	$2 \cdot 3^2 \cdot 13 \cdot 29$	307	(0,1,1,1,0,0,1)
4	-17	-10179	$-3^2 \cdot 13 \cdot 29$	278	(1,0,1,1,0,0,1)
5	21	12393	$3^6 \cdot 17$	316	(0,0,1,0,1,0,0)
6	-30	-17238	$-2 \cdot 3 \cdot 13^2 \cdot 17$	265	(1,1,1,1,1,0,0)
7	52	32946	$2 \cdot 3 \cdot 17^2 \cdot 19$	347	(0,1,1,0,1,1,0)
8	-53	-28899	$-3^2 \cdot 13^2 \cdot 19$	242	(1,0,1,1,0,1,0)

Tomamos a

$$T = \{1, 5\}$$

Calculamos a x como

$$x = (a_1 \cdot a_5) mod(87463) = (296 * 316) mod(87463) = 6073$$

Calculamos todos los l_i

$$\begin{aligned}
l_1 &= 0 \\
l_2 &= 0 \\
l_3 &= \frac{2+6}{2} = 4 \\
l_4 &= 0 \\
l_5 &= \frac{1+1}{2} = 1 \\
l_6 &= 0 \\
l_7 &= 0
\end{aligned}$$

Entonces calculamos a y como

$$y = (-1)^0 \cdot (2)^0 \cdot (3)^4 \cdot (13)^0 \cdot (17)^1 \cdot (19)^0 \cdot (29)^0 = 1377$$

Y así, vemos si se cumple que

$$x \not\equiv (y) mod(87463)$$

entonces proseguimos con sacar el $MCD(x - y, n)$ debido a que se cumple que

$$6073 \not\equiv \pm(1377) mod(87463)$$

Entonces calculamos el

$$MCD(x - y, n) = MCD(6073 - 1377, 87463) = 587$$

$$\Rightarrow 87463 = 587 \cdot q$$
$$\Rightarrow q = 149$$

Por lo tanto:

$$n = p \cdot q$$
$$87463 = 587 \cdot 149$$

d) Descrifrar el siguiente mensaje con parámetros públicos (87463, 15157), dar la llave privada d, recuerde el texto se tranforma módulo 26

Ya que tenemos los siguientes valores:

$$\begin{aligned} p &= 857 \\ q &= 149 \\ n &= 87463 \\ e &= 15157 \end{aligned}$$

Podemos obtener los siguientes valores:

$$\begin{aligned} \phi(n) &= (p - 1)(q - 1) = 86728 \\ d &= 50485 \end{aligned}$$

Entonces tomando el primer valor, 21347, tenemos que:

$$\begin{aligned} x_1 &= 21347^{50485} mod(87463) \\ x_1 &= 15 \rightarrow P \end{aligned}$$

Tomando el segundo valor, 41185, tenemos que:

$$\begin{aligned} x_2 &= 41185^{50485} mod(87463) \\ x_2 &= 26 \rightarrow A \end{aligned}$$

Aplicando esto para cada valor cifrado obtenemos la siguiente lista de valores:

$$x_0 = 21347^{50485} mod(87463)$$
$$x_0 = 15 \rightarrow P$$
$$x_1 = 41185^{50485} mod(87463)$$
$$x_1 = 26 \rightarrow A$$
$$x_2 = 31564^{50485} mod(87463)$$
$$x_2 = 17 \rightarrow R$$
$$x_4 = 76237^{50485} mod(87463)$$
$$x_4 = 11 \rightarrow L$$
$$x_5 = 73700^{50485} mod(87463)$$
$$x_5 = 14 \rightarrow O$$
$$x_6 = 53597^{50485} mod(87463)$$
$$x_6 = 18 \rightarrow S$$
$$x_{13} = 14144^{50485} mod(87463)$$
$$x_{13} = 8 \rightarrow I$$
$$x_{14} = 42561^{50485} mod(87463)$$
$$x_{14} = 19 \rightarrow T$$
$$x_{17} = 73593^{50485} mod(87463)$$
$$x_{17} = 3 \rightarrow D$$
$$x_{18} = 14420^{50485} mod(87463)$$
$$x_{18} = 4 \rightarrow E$$
$$x_{22} = 23637^{50485} mod(87463)$$
$$x_{22} = 6 \rightarrow G$$
$$x_{24} = 1^{50485} mod(87463)$$
$$x_{24} = 1 \rightarrow B$$
$$x_{29} = 2136^{50485} mod(87463)$$
$$x_{29} = 2 \rightarrow C$$
$$x_{31} = 22481^{50485} mod(87463)$$
$$x_{31} = 12 \rightarrow M$$
$$x_{39} = 82282^{50485} mod(87463)$$
$$x_{39} = 13 \rightarrow N$$
$$x_{40} = 19930^{50485} mod(87463)$$
$$x_{40} = 20 \rightarrow U$$
$$x_{58} = 67024^{50485} mod(87463)$$
$$x_{58} = 5 \rightarrow F$$

Con lo cual podemos obtener el mensaje decifrado:

"PARA LOS PROPOSITOS DEL ALGEBRA EL CAMPO DE LOS NUMEROS REALES NO ES SUFICIENTE"

Ejercicio 4

Demostrar con álgebra que el problema del logaritmo discreto no depende del generador