Criptografía y Seguridad - Tarea 2

Rivera González Damián
Tadeo Guillén Diana G

October 28, 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

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

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

$$15 = 4\log_2(2) + \log_2(3) + \log_2(7) mod(2026)$$
$$789 = 3\log_2(3) + \log_2(5) mod(2026)$$
$$1041 = \log_2(2) + \log_2(7) + \log_2(11) mod(2026)$$
$$1040 = \log_2(7) + \log_2(11) mod(2026)$$
$$586 = 2\log_2(11) mod(2026)$$

3) Resolviendo el sistema de ecuaciones obtenemos:

$$\log_2(2) = 1$$
$$\log_2(3) = -731 = 1295$$
$$\log_2(5) = 2982 = 956$$
$$\log_2(7) = 742$$
$$\log_2(11) = 298$$

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

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

c) Descomponer n

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

Ejercicio 4

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