22/06

Práctico 10: Criptografía.

Ejercicio 6. Se considera el siguiente método de intercambio de clave: dado un grupo G, Alice y Bob eligen un elemento $g \in G$. Alice elige en secreto un entero m y le manda a Bob el elemento $x = g^m \in G$. Luego Bob elige en secreto un elemento $k \in G$ que será la clave, un entero n y le manda a Alice el par (g^n, kx^n).

a. ¿Puede Alice descubrir la clave? Sí

b. Si $G = GL(2, \mathbb{R})$ y $g \in G$ es una matriz diagonalizable, ¿Puede un observador descubrir la clave? Sí

c. Si $G = GL(2, \mathbb{R})$ y $g \in G$ es cualquier elemento con determinante distinto de ± 1. ¿Puede un observador descubrir la clave? Sí

d. Si $G = U(97)$ y $g = 5$. Si Alice elige $m = 4$, ¿qué elemento le manda a Bob? Si luego Alice recibe $(74, 44)$, hallar la clave.

(a) Es público: g, $x = g^m$, g^n, kx^n

$kx^n = kg^{mn}$ y Alice conoce m y g^n

$\Rightarrow$ puede calcular $\boxed{k = kg^{mn} \cdot (g^n)^{-m}}$

(b) · Es público: $g \in G$, $x = g^m$, g^n, kx^n.

· Queremos poder hallar k, para esto basta tener m, n o g^{mn}.

· Ahora $G = GL_2(\mathbb{R})$ y g es diagonalizable: $\boxed{g = PA^mP^{-1}}$ A diagonal.

· Tenemos también: $g^n = PA^nP^{-1}$, $g^m = PA^mP^{-1}$, $kg^{nm} = kPA^{nm}P^{-1}$ $\quad (g^n)^m)^{-1}$

Multiplicar por $(g^n)^{-1} \cdot (g^m)^{-1} = g^{-n} \cdot g^{-m} = g^{-(n+m)}$ ✗ No funciona:

Si conseguimos m: $k = kg^{nm} \cdot ((g^n)^m)^{-1}$

$g = A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ Público.

$n = 3$ Privado $\rightsquigarrow$ $g^n = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$ Público

$m = 4$ Privado

$g^m = \begin{pmatrix} 1 & 0 \\ 0 & 16 \end{pmatrix}$ Público.

Tenemos $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ y $\begin{pmatrix} 1 & 0 \\ 0 & 16 \end{pmatrix}$ y queremos hallar m.

↳ Sugerencia: Hallar m tal que $2^m = 16$, en este caso $m=4$.

En general, podemos calcular m tq si $g = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix}$ $g^n = \begin{pmatrix} h_1 & 0 \\ 0 & h_n \end{pmatrix}$

$\Rightarrow g_1^m = h_1 \quad g_2^m = h_2$.

Luego de hallar m calculamos el inverso de $(g^n)^m$.

(c) $g \in GL_2(\mathbb{R})$ con $\det \cdot d \neq \pm 1$.

Esta vez la matriz puede no ser diagonalizable.

Queremos hallar m, n ; g^{-mn} como antes

Ej: $g = \begin{pmatrix} 3 & 4 \\ 7 & 1 \end{pmatrix}$ $\det -25$.

- Calculamos el det $d = -25$
- $\frac{1}{5}\begin{pmatrix} 3 & 4 \\ 7 & 1 \end{pmatrix}$ tiene det 1.
- Sabemos que $g = 5 \left(\frac{1}{5}\begin{pmatrix} 3 & 4 \\ 7 & 1 \end{pmatrix}\right)$
- g^m es: 5^m (algo de det. 1)

Este m es el que queremos.

$\det(A^m) = \det(A)^m$.

tenemos el det. de g y el de g^m.

Hallamos m igual que antes.

Solo funciona si det es distinto de cero o 1.

Ejercicio 10. Sean $n = 606409$ y $e = 1111$.

a. Utilizando el esquema de cifrado en bloques ECB para RSA con (n, e), cifrar el siguiente texto

"MATERIA ENLOQUECIDA DE AZAR".

b. Factorizar n mediante el método de Fermat *(ver notas)*.

- Partimos de un texto y una clave pública de cifrado RSA (n,e). (Tenemos la función de cifrado $E(x) = x^e \ (n)$).
- Elegimos K tal que $28^K < n < 28^{K+1}$. (Para $n = 606409$ $K = 3$)

$K=1 : 28 < n < 28^2$
$K=2 \ 28^2 < n < 28^3$
$K=3 \ 28^3 < n$
$28^4 \not< n$

- Ahora dividimos el texto en bloques de tamaño K.

MAT	ERI	A-E	. . .	
b_1	b_2	b_3		

(1)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

- Le llamamos $\bar{x}$ al número que le corresponde a la letra x.

$b_1 = a_1 a_2 a_3 \mapsto a_1 \cdot 28^2 + a_2 \cdot 28 + a_3$.

En este caso $b_1 \mapsto c_1 = 12 \cdot 28^2 + 0 \cdot 28 + 20 = 9428$

9428	c_2	c_3	

(2)

- Ahora aplicamos cada c_i con la función E.

$E(c_1)$	$E(c_2)$	$E(c_3)$	

(3)

En el ejemplo: $E(c_1) = E(9428) = 9428^{1111} \ (606409)$.

Si lo queremos hacer a mano: exp rápida.

→ Pasamos 1111 a base 2: $1024 + 64 + 16 + 4 + 2 + 1$

$= 2^{10} + 2^6 + 2^4 + 2^2 + 2^1 + 1$.

i	$9428^{2^i} \ (n)$
0	9428
1	...
⋮	
10	

· El último paso es escribir $E(c_i)$ en base 28: y sustituir cada letra.

$E(c_i) = c_k \cdot 28^k + \dots + c_1 \cdot 28 + c_0$

no es obvio que los coef c_{k+n} $n \geq 1$ son cero.

Ej: Si $E(c_i) = +1 \cdot 28^3 + 2 \cdot 28^2 + 3 \cdot 28 + 4$.

BCDE	

Ejercicio 5.

Supongamos que n es un número muy díficil de factorizar. Bernardo utiliza un criptosistema RSA con clave (n, e_1), al mismo tiempo que Bruno utiliza la clave (n, e_2), con $mcd(e_1, e_2) = 1$. Adriana les envía el mismo texto x a ambos, calculando $y_1 = x^{e_1} \pmod n$ e $y_2 = x^{e_2} \pmod n$ (envía y_1 a Bernardo e y_2 a Bruno). Alguien que intercepta los mensajes realiza los siguientes cálculos:
1. c_1 y c_2 positivos tales que $c_1 e_1 + c_2 e_2 \equiv 1 \pmod{\varphi(n)}$. 2. $x_1 = y_1^{c_1}(y_2^{c_2}) \pmod n$.

a. Probar que x_1 calculado en el paso 2 es el texto x. Por lo tanto, si bien el criptosistema es seguro, el mensaje puede ser descifrado en este caso.

b. Descifrar el mensaje si $y_1 = 9983$ e $y_2 = 4026$, sabiendo que $n = 16123, e_1 = 27$ y $e_2 = 29$.

Idea: (a) Supongamos que tenemos c_1 y c_2 como en 1. Tenemos que ver que $x_1 = y_1^{c_1}(y_2)^{c_2} \equiv x \pmod n$.

· Sustituimos y_1 y y_2: $y_1 = x^{e_1} \pmod n$ y $y_2 = x^{e_2} \pmod n \Rightarrow x_1 = x^{e_1 c_1 + e_2 c_2} \pmod n$

· Como $c_1 e_1 + c_2 e_2 \equiv 1 \pmod{\varphi(n)}$ podemos escribir: $c_1 e_1 + c_2 e_2 = 1 + \varphi(n) \cdot k$ para algún $k \in \mathbb{Z}$.

· Nos queda: $x_1 = x^{1+\varphi(n)k} \pmod n$ y ahora podemos dividir en casos:

Si $mcd(x, n) = 1 \rightsquigarrow$ por Euler $x_1 \equiv x \pmod n$

Si $mcd(x, n) > 1$ hay tres posibilidades: (1) $p \mid x$ y $q \nmid x$

(2) $p \nmid x$ y $q \mid x$

(3) $pq \mid x$

En el caso (3) $x \equiv 0 \pmod n$ y x_1 también.

En el caso (1) $\begin{cases} x_1 \equiv 0 \equiv x \pmod p \\ x_1 \equiv x \pmod q \end{cases} \rightsquigarrow$ Por teo. Chino $x_1 \equiv x \pmod{pq}$

Para (b) hallemos enteros c_1 y c_2 tq $\boxed{c_1 e_1 + c_2 e_2 = 1}$ pero no necesariamente positivos. Si y_1 y y_2 son invertibles no tendremos problemas.

Observar que no vamos a hallar $\varphi(n)$.