

PRÁCTICO 12: CRIPTOGRAFÍA

En los ejercicios que siguen, vamos a utilizar la siguiente numeración de los **28** símbolos:

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

**Sistemas de clave privada**

**Ejercicio 1.**

- a. Deseamos acordar una clave común con Romina usando el protocolo **Diffie-Hellman**. Elegimos el primo  $p = 991$ , y  $g = 7$  como raíz primitiva módulo  $p$ ; ambas de forma pública. Romina elige al azar, y en secreto, un número  $n < p$ , y nos envía públicamente  $g^n \equiv 989 \pmod{p}$ . Nosotros elegimos al azar  $m = 11$  (secretamente).
- ¿Cuál es la clave  $k$  común que acordamos con Romina?
  - ¿Qué número tenemos que mandarle públicamente a Romina para que solamente ella pueda calcular la clave fácilmente?
- b. Supongamos que deseamos comunicarnos con Romina a través de un **sistema Vigenere**, utilizando una palabra clave de 3 letras. Para esto tomamos la clave  $k$  común acordada con Romina en la parte anterior, y la escribimos en base 28:

$$k = L_2 28^2 + L_1 28 + L_0, \quad 0 \leq L_i < 28.$$

A partir de esto definimos la clave común como:  $L_2 L_1 L_0$ . Por ejemplo, si fuese  $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$ , la clave común sería YAC.

- Cifrar los siguientes mensajes: SIMULADOR, Y\_WALTER.
- Descifrar los siguientes mensajes enviados por Romina: GZFAKPVP, NJÑJXDPX.

**Ejercicio 2.** Queremos acordar una clave común con Rodrigo usando el protocolo **Diffie-Hellman**. Elegimos un primo  $p$  y una raíz primitiva  $g$  módulo  $p$ . Rodrigo no quiere un exponente complicado por miedo a no recordarlo, por lo que elige a  $p - 1$ . Explicarle por qué esto es una mala idea.

**Ejercicio 3.** Ofelia desde Colonia y Lucía desde Artigas quieren intercambiar un mensaje de forma privada. Así que no tienen más remedio que aprender un poco de criptografía.

- a. Al principio Ofelia no entendió bien el método de Diffie-Hellman y propone el siguiente método para fijar una clave común: eligen (públicamente) un primo  $p$  y un entero  $1 < g < p$ . A su vez, Ofelia elige en secreto un entero  $n$  y Lucía elige un entero  $m$ . Ofelia calcula  $a = ng \pmod{p}$  y le manda  $a$  a Lucía. Lucía calcula  $b = mg \pmod{p}$  y le manda  $b$  a Ofelia. La clave común será:  $k = ngm \pmod{p}$ ; la cual Ofelia puede calcular haciendo  $k = nb \pmod{p}$ , y Lucía haciendo  $k = am \pmod{p}$ .
- Eligen  $p = 101$  y  $g = 2$ . Ofelia le manda  $a = 19$  y Lucía elige  $m = 35$ , ¿cuál es la clave común?

- ii) Un observador ve que Ofelia manda  $a = 19$ , y que Lucía manda  $b = 35$ . ¿Puede obtener la clave? En caso afirmativo, hallarla.
  - iii) Describir un método para encontrar la clave en general, conociendo  $p$ ,  $g$ ,  $a$  y  $b$ .
- b. Lucía lee el libro y entiende que hay que usar potencias en vez de multiplicaciones; así que Lucía y Ofelia utilizan el método **Diffie-Hellman** correcto para acordar una clave común. Toman como primo  $p = 89$  y  $g = 7$ . Lucía elige el número secreto  $m = 86$  y Ofelia le envía  $b = g^n \equiv 17 \pmod{p}$ . ¿Cuál es la clave secreta  $K$  que acuerdan?
- c. Sea  $K$  la clave secreta acordada en la parte anterior. Se utiliza luego un **criptosistema afín**, con función de encriptado  $E : \mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$ , tal que  $E(x) = cx + e \pmod{28}$ , sabiendo  $K = c \cdot 28 + e$ , con  $0 \leq c < 28$  y  $0 \leq e < 28$ . Para cifrar un texto se cifra letra a letra usando la función de cifrado. Lucía cifra PASALA y se lo manda a Ofelia. ¿Qué mensaje recibe Ofelia?
- d. Supongamos ahora que somos espías y sabemos que Ofelia le envía a Lucía un mensaje cifrado según un **criptosistema afín**, pero desconocemos los valores de  $c$  y  $e$  de la función de cifrado. Interceptamos el siguiente texto: LÑVJ Ñ. Sabemos que el mensaje original (sin cifrar) contiene dos O y nos informan que Ofelia siempre usa  $e = 9$ .
- i) Hallar la función de cifrado que usaron Lucía y Ofelia.
  - ii) Descifrar el mensaje interceptado.

#### Ejercicio 4.

- a. Probar que 5 es una raíz primitiva módulo 97.
- b. Supongamos que interceptamos la conversación entre Alicia y Bob cuando ambos están utilizando el protocolo **Diffie-Hellman** para acordar una clave común. Alicia y Bob acuerdan  $p = 97$  para el módulo y  $g = 5$  como generador. Alicia le envía a Bob 3 y Bob le envía a Alicia 7. ¿Cuál es la clave  $k$  común que acuerdan Alicia y Bob? (la idea es ver que no es fácil descubrir la clave).
- c. Supongamos que Diego y Marta quieren utilizar el método **Diffie-Hellman** de intercambio de clave, usando el primo  $p = 97$  y la raíz primitiva  $g = 29$ . Diego le envía a Marta el número  $x = 85$ . Marta luego le envía a Diego el número  $y = 3$ . Recordando que 5 es una raíz primitiva módulo 97, y teniendo como datos los siguientes logaritmos discretos  $\log_5 29 = 13$  y  $\log_5 85 = 90$ , hallar la clave común.

## Sistemas de clave pública

#### Ejercicio 5. (Parcial 2, Semestre 1, 2021)

- a. Hallar el menor  $x \in \mathbb{Z}^+$  que verifica  $\begin{cases} x \equiv 10 \pmod{13} \\ x \equiv 91 \pmod{101} \end{cases}$ .
- b. Sea  $E$  la función de cifrado **RSA** con clave  $(n, e)$ . Describir la función de descifrado  $D$ , y probar que descifra.
- c. Si  $(n, e) = (1313, 271)$ , cifrar la letra  $K$ . Sugerencia: usar TCR con  $1313 = 101 \times 13$ .

#### Ejercicio 6. Sea $n = pq$ , con $p$ y $q$ primos.

- a. Describir un método para factorizar  $n$  si se conocen los valores de  $n$  y  $\varphi(n)$ .
- b. Factorizar  $n = 187$  sabiendo que  $\varphi(187) = 160$ .

**Ejercicio 7.** Supongamos que  $n$  es un número muy difícil de factorizar. Bernardo utiliza un **criptosistema RSA** con clave  $(n, e_1)$ , al mismo tiempo que Bruno utiliza la clave  $(n, e_2)$ , con  $\text{mcd}(e_1, e_2) = 1$ . Adriana les envía el mismo texto  $x$  a ambos, calculando  $y_1 = x^{e_1}$  (mód  $n$ ) e  $y_2 = x^{e_2}$  (mód  $n$ ) (envía  $y_1$  a Bernardo e  $y_2$  a Bruno). Alguien que intercepta los mensajes realiza los siguientes cálculos:

$$\text{hallar } c_1, c_2 \in \mathbb{Z}^+ / c_1 e_1 + c_2 e_2 = 1, \text{ y luego calcular } x_1 \equiv y_1^{c_1} y_2^{c_2} \pmod{n}.$$

Notar que estos cálculos se pueden realizar de forma eficiente (por ejemplo mediante Euclides extendido y exponenciación rápida).

- Probar que  $x_1$  es el texto  $x$ . Por lo tanto, si bien el criptosistema es seguro, el mensaje puede ser descifrado en este caso.
- Descifrar el mensaje si  $y_1 = 9983$  e  $y_2 = 4026$ , sabiendo que  $n = 16123$ ,  $e_1 = 27$  y  $e_2 = 29$ .

**Ejercicio 8.** Sean  $n = 606409$  y  $e = 1111$ . Factorizar  $n$  mediante el **método de Fermat**. Este método consiste en lo siguiente: vamos calculando  $n + s^2$ , con  $s = 0, 1, 2, \dots$ , hasta obtener un cuadrado perfecto. Una vez que lo conseguimos, se obtiene:  $n + s^2 = t^2 \Rightarrow n = t^2 - s^2 = (t - s)(t + s)$ . Este método es eficiente para factorizar números que poseen divisores cercanos a  $\sqrt{n}$ .

## Ejercicios adicionales

**Ejercicio 9.** Se considera el siguiente método de intercambio de clave: dado un grupo  $G$ , Alicia y Bob eligen un elemento  $g \in G$ . Alicia elige en secreto un entero  $m$  y le manda a Bob  $x = g^m \in G$ . Luego Bob elige en secreto un elemento  $k \in G$  que será la clave, un entero  $n$  y le manda a Alicia el par  $(g^n, kx^n)$ .

- ¿Puede Alicia descubrir la clave?
- Sea  $G = GL(2, \mathbb{R})$  y  $g \in G$  una matriz diagonalizable, con valores propios positivos. ¿Puede un observador descubrir la clave?
- Sea  $G = GL(2, \mathbb{R})$  y  $g \in G$ , con  $\det(g) \neq \pm 1$ . ¿Puede un observador descubrir la clave? Sugerencia: discutir según la forma de Jordan de la matriz  $g$ .
- Sea  $G = U(97)$  y  $g = 5$ . Si Alicia elige  $m = 4$ , ¿qué elemento le manda a Bob? Si luego Alicia recibe  $(74, 44)$ , hallar la clave.

**Ejercicio 10. Firma digital.** Supongamos que Alicia quiere enviar un documento  $m$  firmado a Bob, de manera que Bob sepa con seguridad que fue firmado por Alicia y no otra persona. Como en RSA, Alicia elige dos primos grandes  $p$  y  $q$ , para obtener  $n = pq$ , y  $e$  coprimo con  $\varphi(n)$ . Luego calcula  $d$  tal que  $ed \equiv 1 \pmod{\varphi(n)}$ . Publica  $n$  y  $e$  y guarda  $p$ ,  $q$  y  $d$ . La firma digital de Alicia, asociada al mensaje  $m$ , es:

$$s = m^d \pmod{n},$$

y puede enviar  $(m, s)$  a Bob. Ahora Bob puede verificar que el documento fue firmado por Alicia elevando  $s$  a la potencia  $e$ -ésima y compararlo con  $m$ :

$$s^e = (m^d)^e = m^{ed} \equiv m \pmod{n}.$$

Supongamos que Alicia envía tres documentos a Bob con su firma digital de la forma  $(m, s)$ , donde  $m$  es el documento y  $s$  la firma digital del mismo. Alicia usa  $n = 10379$  como módulo, y exponente de cifrado  $e = 17$ ; siendo ambos valores públicos. Bob crea un cuarto documento e intenta falsificar la firma digital de Alicia sin éxito. ¿Cuál de los siguientes documentos es la falsificación?

$$(209, 8690), \quad (1059, 5909), \quad (921, 636), \quad (347, 5120).$$