Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Segundo semestre 2023**
Instituto de Matemática y Estadística

PRÁCTICO 11: 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

Ejercicio 1.

a. Supongamos que deseamos acordar una clave común con Romina usando el protocolo **Diffie-Hellman**. Elegimos juntos $p = 991$ y Romina nos avisa (públicamente) que eligió $g = 7$. Romina elige al azar (secretamente) un número $n < p$ y nos envia $g^n \equiv 989 \pmod{p}$. 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 hallar la clave?

b. Ahora queremos acordar una clave común con Rodrigo usando el protocolo **Diffie-Hellman**. Elegimos un primo p y una raíz primitiva g. 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.

c. 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 **a**, 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`.

i) Cifrar los siguientes mensajes: `SIMULADOR`, `HACHAZO`.

ii) Descifrar los siguientes mensajes enviados por Romina: `GZFAKPVP`, `NJÑJXDPX`.

Ejercicio 2. 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 $k = am \pmod{p}$.

i) 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 $E : \mathbb{Z}_{28} \to \mathbb{Z}_{28}$, 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 3.

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 envia 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 $g = 29$. Diego le envia 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.

Ejercicio 4. Sea $n = pq$, con p y q primos. Describir un método para factorizar n si se conoce $\varphi(n)$.

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 $\operatorname{mcd}(e_1, e_2) = 1$. 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:

$$c_1, c_2 \in \mathbb{Z}^+ \quad / \quad c_1 e_1 + c_2 e_2 \equiv 1 \pmod{\varphi(n)}, \quad x_1 \equiv y_1^{c_1}(y_2^{c_2}) \pmod{n}.$$

a. 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.

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

Ejercicio 6. 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).

a. ¿Puede Alicia descubrir la clave?

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

c. Sea $G = GL(2, \mathbb{R})$ y $g \in G$ un elemento con $\det(g) \neq \pm 1$. ¿Puede un observador descubrir la clave?

d. 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 7.

a. Hallar el menor x 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 $(n, e) = (1313, 271)$, calcular $E(10)$.

Ejercicio 8. 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 es:

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

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:

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

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?

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

Ejercicio 9. Cifrado ElGamal. Es un esquema de cifrado basado en problemas de logaritmos discretos. Si Alicia y Bob quieren comunicarse de manera segura mediante ElGamal, lo hacen de la siguiente manera:

- Alicia elige un primo p y una raíz primitiva módulo p. Luego elige x, con $2 \leq x \leq p - 2$, y calcula $h \equiv g^x \pmod{p}$. Los datos p, h y g son públicos y x no.
- Ahora Bob elige y con $2 \leq y \leq p - 2$ y calcula $r \equiv g^y \pmod{p}$. Además calcula $c \equiv h^y m \pmod{p}$, donde m es su mensaje, y envia r y c a Alicia.
- Para descifrar, Alicia calcula $m \equiv c r^{-x} \pmod{p}$.

a. Explicar por qué funciona el descifrado en el cifrado de ElGamal descripto anteriormente.

b. Alicia elige los siguientes números: $p = 46454609$, $g = 3$ y $h = 7902328$. Bob elige $y = 1142987$, y su mensaje es $m = 7601846$. ¿Cuáles serán los datos r y c que Alicia recibe de Bob?

c. Supongamos que Bob envía un mensaje a Alicia usando el método de ElGamal, y de alguna manera obtenemos el valor y que usó Bob ¿cómo se puede usar ese dato para calcular el mensaje m?

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. El método de Fermat para factorizar n consiste en lo siguiente: vamos calculando $n + s^2$, con $s = 0, 1, 2, \ldots$, 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 para resolver con ayuda computacional

Ejercicio 11. Diego crea un **criptosistema RSA** con la siguiente clave pública:

$$(n, e) = (92852447, 22413211).$$

Los parámetros elegidos no son buenos. Hallar la función de descifrado de Diego (Sug: Método de Fermat).

Ejercicio 12. El primo 12347 tiene raíz primitiva 2. Supongamos que sabemos que $2^x \equiv 8938 \pmod{12347}$ y $2^y \equiv 9620 \pmod{12347}$, pero no sabemos x ni y. ¿Es $2^{xy} \equiv 7538 \pmod{12347}$? ¿Es $2^{xy} \equiv 7557 \pmod{12347}$?

Ejercicio 13. Bob envía el mismo mensaje m a tres personas distintas. Los textos cifrados son:

$$c_1 = 257261 \pmod{303799}, \quad c_2 = 117466 \pmod{289279}, \quad c_3 = 260584 \pmod{410503};$$

con respectivos módulos de **RSA**:

$$n_1 = 303799, \; n_2 = 289279, \; n_3 = 410503.$$

El exponente de cifrado de cada persona es $e = 3$, por lo que $m^3 \equiv c_i \pmod{n_i}$.

a. Hallar x tal que $0 \leq x < n_1 n_2 n_3$ y

$$x \equiv c_1 \pmod{n_1}, \; x \equiv c_2 \pmod{n_2}, \; x \equiv c_3 \pmod{n_3}.$$

b. Mostrar que $0 \leq m^3 < n_1 n_2 n_3$.

c. Mostrar que x es igual a m^3.

d. Encontrar el mensaje m.

Esto muestra la desventaja de usar exponentes de cifrado pequeños.