Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso 2021**
Instituto de Matemática y Estadística

PRÁCTICO 10 : 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 Cristiano usando el protocolo Diffie-Hellman. Elegimos juntos $p = 991$ y Cristiano nos avisa (públicamente) que eligió $g = 7$. Cristiano elige al azar (secretamente) un número $n < p$ y nos envia $g^n \equiv 989 \pmod{p}$. Nosotros elegimos al azar $m = 11$ (secretamente). ¿Cual es la clave k común que acordamos con Cristiano? ¿Qué número tenemos que mandarle públicamente a Cristiano para que solo él también pueda hallar la clave?

b. Ahora queremos acordar una clave común con Lionel usando el protocolo Diffie-Hellman. Elegimos un primo p y una raíz primitiva g. Lionel no quiere complicarse con un exponente complicado por miedo a no recordarlo por lo que elige a $p - 1$. Explicarle por qué esto es una mala idea, o sea cómo se puede obtener la clave en este caso.

c. Ahora supongamos que deseamos comunicarnos con Cristiano a través de un sistema Vigenere donde la palabra clave consiste de 3 letras de la siguiente manera:
Tomamos la clave k común acordada con Cristiano en la parte **a**. y la escribimos en base 28:

$$k = L_2 28^2 + L_1 28 + L_0$$

Luego la clave común resulta de sustituir en $L_2 L_1 L_0$ por sus respectivas letras (por ejemplo si $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$ entonces la clave común será `YAC`).

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

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

Ejercicio 2. Cavani desde París y Rolan desde Burdeos quieren acordar tácticas para el partido contra Jamaica; pero los técnicos jamaiquinos contrataron espías para interceptar sus comunicaciones. Así que no tienen más remedio que aprender un poco de criptografía para poder asegurar privacidad.

a. Al principio Cavani 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 $1 < g < p$. Cavani elige en secreto un entero n y Rolan elige un entero m. Cavani calcula $a = ng \pmod{p}$ y le manda a a Rolan; Rolan calcula $b = mg \pmod{p}$ y le manda b a Cavani. Entonces la clave común será $k = ngm \pmod{p}$, la cual Cavani puede calcular haciendo $k = nb \pmod{p}$ y Rolan puede calcular $k = am \pmod{p}$.

i) Si eligen $p = 101$ y $g = 2$. Cavani le manda $a = 19$ y Rolan elige $m = 35$, ¿cuál es la clave común?

ii) Si un observador ve que Cavani manda $a = 19$ y que Rolan 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. Rolan dudando, lee el libro y entendió que hay que usar potencias en vez de multiplicaciones; así que Rolan y Cavani utilizan el método Diffie-Hellman correcto para acordar una clave común. Toman como primo $p = 89$ y $g = 7$. Si Rolan elige el número secreto $m = 86$ y Cavani le envía $b = g^n = 17 \pmod{p}$. ¿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 $E : \mathbb{Z}_{28} \to \mathbb{Z}_{28} /\ E(x) = cx + e \pmod{28}$, 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. Rolan cifra PASALA y se lo manda a Cavani. ¿Qué mensaje recibe Cavani?

d. Supongamos ahora que somos espías y que sabemos que Cavani le envía a Rolan un mensaje cifrado según un criptosistema afín pero desconocemos los valores de c y e de la función de cifrado. Interceptamos el texto: LÑVJ Ñ. Sabemos que el mensaje original (sin cifrar) contiene dos O y nos informan que Cavani siempre usa $e = 9$.

i) Hallar la función de cifrado que usaron Rolan y Cavani.

ii) Descifrar el mensaje interceptado.

Ejercicio 3.

a. Probar que 5 es una raíz primitiva módulo 97.

b. Supongamos que somos espías 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 justo ver que no es fácil descubrir la clave).

c. Supongamos que Diego y Marta quieren utilizar el método Diffie-Helmann 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 $mcd(e_1, e_2) = 1$. 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 $e_2 = 29$.

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?

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

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?

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.

Ejercicio 7.

a. Hallar el menor x que verifica $\begin{cases} x \equiv 10 & \text{mod } 13, \\ x \equiv 91 & \text{mod } 101. \end{cases}$

b. Si E es la función de cifrado con el método RSA con clave (n, e), descibir D la función de descifrado y demostrar que descifra.

c. Si $(n, e) = (1313, 271)$ calcular $E(10)$.

Firma digital: Supongamos que Alice quiere enviar un documento m firmado a Bob, de manera que Bob sepa con seguridad que fue firmado por Alice y no otra persona. Como en RSA, Alice elige dos primos grandes p, 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 Alice es

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

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

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

Ejercicio 8. Alice 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. Alice usa $n = 10379$ como módulo y exponente de cifrado $e = 17$ que son públicos. Bob crea un cuarto documento e intenta falsificar la firma digital de Alice sin éxito. ¿Cuál de los siguientes documentos es la falsificación?

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

Cifrado ElGamal: El procedimiento de cifrado/descifrado ElGamal se refiere a un esquema de cifrado basado en problemas matemáticos de logaritmos discretos.

Supongamos que Alice quiere comunicarse de manera segura con Bob y lo hace de la siguiente manera. Alice 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 $r \equiv g^y \pmod{p}$. Bob calcula $c \equiv h^y m \pmod{p}$, donde m es su mensaje, y envia r y c a Alice.

Para descifrar Alice calcula $m \equiv cr^{-x} \pmod{p}$.

Ejercicio 9.

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

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

c. Si Bob envía un mensaje a Alice usando el método de ElGamal y de alguna manera obtuvimos el valor y que usó Bob ¿cómo se puede usar ese dato para calcular 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 *(ver notas)*.

Póquer mental: Alice y Bob quieren jugar póquer por correo. Alice compra 52 cajas fuertes y en cada una pone una carta distinta y las cierra con candados para los cuales solo ella tiene la llave. Luego se las envía por correo a Bob y Bob elige 5 aleatoriamente y les pone un candado para los cuales solo él tiene llave, y por ultimo le envía esas 5 cajas a Alice. Alice le quita su candado a las cajas recibidas y se las devuelve a Bob, con lo cual Bob puede abrirlas y ver que cartas le han sido repartidas. Bob tiene 47 cajas cerradas por Alice, elige 5 aleatoriamente y se las envía a Alice, quién puede ver sus 5 cartas.

Con esto se termina la primer ronda de reparto de cartas, Bob y Alice tienen 5 cartas cada uno, Alice no tiene cajas fuertes mientras que Bob tiene 42 cajas cerradas por Alice.

Cuando Bob ve sus cartas, decide que quiere descartar 2 de ellas. Las pone en una caja fuerte que cierra con candado y se la envía a Alice. Luego elige al azar dos de las 42 cajas cerradas por Alice, las tranca y se las envía a Alice. Alice quita el candado de las dos últimas que Bob le envió y se las devuelve a Bob, con lo cual Bob puede quitar sus candados y ver sus cartas nuevas.

Si Alice quiere reemplazar 3 cartas, pone las mismas en una caja que cierra con candado y se las envía a Bob, quien elige 3 de las 40 disponibles y se las envia a Alice. Alice ahora puede ver sus 3 cartas nuevas quitando el candado de las cajas que le envió Bob. Por último pueden comparar sus cartas y ver quién ganó.

Una manera de modelar matemáticamente el modelo anterior es el siguiente: Alice y Bob acuerdan un primo p grande. Alice elige un número α secreto coprimo con $p-1$ y calcula α' inverso de α módulo $p-1$, o sea $\alpha\alpha' \equiv 1 \pmod{p-1}$. Bob hace lo mismo y elige β secreto coprimo con $p-1$ y calcula β' con $\beta\beta' \equiv 1 \pmod{p-1}$.

Alice y Bob asignan ahora un número a cada una de las 52 cartas, $n_1, n_2, \ldots, n_{52}$. Alice calcula los numeros c_i

$$c_i \equiv n_i^{\alpha} \pmod{p}.$$

Esto es el equivalente matemático de cerrar con candado las cajas fuertes. Luego de permutarlos de manera aleatoria, se los envía a Bob.

Ahora Bob elige 5 números $c_{i_1}, c_{i_2}, c_{i_3}, c_{i_4}, c_{i_5}$ y los eleva a la potencia β-ésima módulo p (de vuelta, esto es el equivalente matemático de que Bob cierre con candado las 5 cajas fuertes que eligió), y se las envía a Alice,

$$c_{i_1}^{\alpha\beta}, c_{i_2}^{\alpha\beta}, c_{i_3}^{\alpha\beta}, c_{i_4}^{\alpha\beta}, c_{i_5}^{\alpha\beta}.$$

Alice eleva estos números a la potencia α'-ésima módulo p y obtiene los números

$$c_{i_1}^{\beta}, c_{i_2}^{\beta}, c_{i_3}^{\beta}, c_{i_4}^{\beta}, c_{i_5}^{\beta},$$

que se los envía a Bob.

Bob puede entonces obtener los $c_{i_1}, c_{i_2}, c_{i_3}, c_{i_4}, c_{i_5}$ de la siguiente manera

$$c_{i_j} \equiv c_{i_j}^{\beta\beta'} \pmod{p}.$$

Con lo cual Bob obtuvo su primer mano. Y, usando un método similar, Alice puede obtener también sus 5 cartas para comenzar a jugar.

Podemos asignar los números del 1 al 13 a las cartas corazón en orden creciente, del 14 al 26 las picas, del 27 al 39 los diamantes y del 40 al 52 los tréboles.

Ejercicio 11.

a. Si $p = 101$, $\alpha = 43$ y Alice recibe de Bob los números 96, 46, 73, 49 y 51, mientras que la mano de Bob está dada por 18, 13, 23, 9 y 50. ¿Quién gana la mano?

b. Jugar con un compañero por correo electrónico con $p = 223$.

Ejercicios para resolver con ayuda computacional.

Ejercicio 12. Gerrard crea un criptosistema RSA con clave pública:

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

Se han escogido mal los parámetros, hallar la función de descifrado de Gerrard (*Sug:Método de Fermat)*.

Ejercicio 13. 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 14. Supongamos que Bob envía el mismo mensaje m a tres personas distintas. Los textos cifrados son

$$\begin{aligned} c_1 &= 257261 \pmod{303799} \\ c_2 &= 117466 \pmod{289279} \\ c_3 &= 260584 \pmod{410503} \end{aligned}$$

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.