Práctico 10: Criptografía

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

Cifrado Cesar: ① Escribir el alfabeto

② Elegimos una clave k entre 0 y 27

③ Escribimos el texto a cifrar en una fila, y sustituimos cada letra por el nº correspondiente.

④ Sumamos a cada nº k y reducimos mod 28.

Variante: Vigenère. ① Escribir el alfabeto español como antes

② Elegir una palabra clave.

③ Escribimos el texto en una fila y la palabra clave (repetida) en la de abajo

HOLA-COMO-ESTAS

SOLSOLSOLSOL...

④ Sumamos $Z = 7+19$ el nº correspondiente a las dos letras de cada columna.

Diffie-Hellman: Ana y Bruno van a acordar una clave común. El canal puede ser interceptado.

① Entre los dos eligen p primo y g una raíz primitiva módulo p.

② Ana elige un entero n (privado) y envía g^n a Bruno. $(1 < n < p)$

③ Bruno elige m (privado) y envía g^m a Ana.

④ La clave es $k \equiv g^{n \cdot m} \equiv (g^n)^m \equiv (g^m)^n \pmod p$

⇝ Ana y Bruno pueden calcular la clave de forma sencilla, el resto no.

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 envía $g^n \equiv 989 \pmod p$. 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?

La clave es $989^{11} \pmod{991}$ esto es $(-2)^{11} \pmod{991}$

$(-2) \cdot (-2)^{10} \pmod{991}$

$(-2) \cdot (1024) \pmod{991}$

$(-2)(33) = -66 \pmod{991}$

$= 925 \pmod{991}$ ←

Tenemos que enviarle $7^{11} \pmod{991}$ (Cuentas...)

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.

$g^{p-1} \equiv 1 \pmod{p} \Rightarrow$ la clave es $(g^{p-1})^m \equiv 1 \pmod{p}$.

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:

925

$$k = L_2 28^2 + L_1 28 + L_0 = 1 + 28 \cdot 33 = 1 + 28 \cdot (28+5) = 1 + 5 \cdot 28 + 1 \cdot 28^2.$$

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.

La clave es: B F B

(i)

S	I	M	U	L	A	D	O	R
B	F	B	B	F	B	B	F	B
T	N	N	V	P	B	E	T	S

(ii)

G	Z	F	A	K	P	V	P
B	F	B	B	F	B	B	F
F	U	E	—	F	O	U	L

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

Conocemos n y $\varphi(n)$

Queremos calcular: p, q tales que $p \cdot q = n$.

$\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$

$\Rightarrow \boxed{(p+q) = n + 1 - \varphi(n)}$

$n/p = q$ ⇝ Sustituimos q por n/p

$\Rightarrow (p+q) = p + n/p$ y por otra parte

$(p+q) = n+1-\varphi(n)$

$\Rightarrow$ Multiplicando $\cdot p$: $p^2 + n = np + p - \varphi(n)p$

Hallar p es resolver $p^2 - (n+1-\varphi(n))p + n = 0$.

Exp. Rápida: Queremos calcular $x^e \pmod n$

$\Rightarrow$ Escribimos e en base 2: $e = 2^0 \cdot e_0 + 2^1 \cdot e_1 + \ldots + 2^k e_k$

$$x^e = x^{2^0 \cdot e_0 + 2^1 e_1 + \ldots 2^k e_k}$$
$$= x^{2^0 (e_0)} \cdot x^{2^1 e_1} \cdot \ldots \cdot x^{2^k e_k}$$

Basta calcular x^{2^i} para $0 \le i < k$

i	$x^{2^i} (n)$	$x=2$
0	$x\ (n)$	$2\ (n)$
1	$x^2\ (n)$	$4\ (n)$
2	$x^4\ (n)$	$16\ (n)$
3	$x^8 (n)$	$256\ (n)$
4	$x^{16} (n)$	$256^2\ (n)$

La fila i-ésima se calcula elevando al cuadrado la anterior y reduciendo mód n

Al final multiplicamos x^{2^i} cuando $e_i = 1$.