Ejercicios

Salvo indicación contraria, utilizar el alfabeto de 26 letras.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

1. Semana 1

1.1. Criptografía cásica

1. Utilizar el cifrado de César para

   a) cifrar “ASTERIX”,

   b) descifrar “REHOLA”.

2. Descifrar el mensaje “VEYFCLNS” obtenido por un cifrado de Vigenère con la clave “CAKE”.

3. Utilizar un cifrado de Vigenère encadenado con la clave inicial “PAN” para

   a) cifrar “VIGENERE”,

   b) descifrar “RISIIVW”.

4. Utilizar el alfabeto de 37 caracteres formado por las 26 letras anteriores, las 10 cifras decimales 0, 1, ... 9 y el espacio en blanco

A	B	...	Z	0	1	2	3	4	5	6	7	8	9	“ ”
0	1	...	25	26	27	28	29	30	31	32	33	34	35	36

   para cifrar el mensaje

   MI TELEFONO ES 600123456

   siguiendo un cifrado encadenado de Vigenère, con la clave CERO.

   Supongamos que hemos equivocado el número de teléfono y que el número correcto es 609123456. Cifrar de nuevo el mensaje con el mismo método. Comparar los bloques de mensaje obtenidos en última posición, en uno y otro caso.

   Nota: Se observa que si cambia un dato del mensaje, el último bloque cambia. El último bloque cifrado de un cifrado encadenado puede utilizarse como *código de autenticación de mensaje* (se denomina MAC o “message authentication code”). Así, si junto al mensaje enviamos el último bloque cifrado, el receptor puede saber si el mensaje recibido es correcto o no. Basta con que lo vuelva a cifrar y observe si el último bloque coincide con el recibido aparte.

1.2. Seguridad criptográfica

1. Precisar los cuatro servicios criptográficos principales.
2. Explicar qué se entiende por seguridad incondicional de un criptosistema.
3. Explicar en qué consiste un ataque de texto en claro.

1.3. Conversión de mensajes. Aritmética modular

1. Dividir el mensaje "CESAR" en bigramas y transformarlo en números enteros. Después transformar dichos números enteros en bits.

   Nota: Como $26^2 - 1 = 675$ necesita 10 bits para ser representado en base 2 ($9 \leq \log_2 675 < 10$), se pide representar cada entero con 10 bits.

2. Encontar los mensajes tales que los equivalentes numéricos y binarios de los bigramas en los que han sido divididos son:

   $$(117, 214, 312)$$

   $$0001000010010010110001111001101000011010$$

3. Calcular

   $$10 + 13 \mod 15, \quad 10 + (-13) \mod 15,$$
   $$15 \cdot 10 \mod 26, \quad (-15) \cdot 10 \mod 26.$$

4. Sabemos que $(\mathbb{Z}_5, +, \cdot)$ es un anillo. ¿Es $(\mathbb{Z}_5, \cdot, +)$ un anillo?

5. Siguendo paso a paso el algoritmo de cálculo de potencias modulares, hallar $19^{12} \mod 7$.

   Nota:

   a) Justificar que $19^{12} \equiv 5^{12} \mod 7$.

   b) Comprobar que $19^{12} \not\equiv 5^{12 \mod 7} \mod 7$.

6. Hallar: a) $38^{75} \mod 103$; b) $2^{32} \mod 16$.

1.4. Cifrado afín I. Divisibilidad. Números primos

1. Utilizar un cifrado afín con clave $a = 5, b = 10$ para cifrar "CESAR".
2. Se define la función de cifrado *translación* como:

   $$\begin{array}{rccc} f: & \mathcal{M} & \longrightarrow & \mathcal{C} \\ & M & \mapsto & C \equiv M + b \mod N \end{array}$$

   donde M es el equivalente numérico de cada letra, N es el número de letras del alfabeto y b es un número entero, $0 \leq b \leq N - 1$.

   La clave de cifrado es: b.

a) Obtener la función de descifrado.

b) Utilizando la clave $b = 15$,

1) cifrar "OBELIX",
2) descifrar "PHITGXM".

c) Interceptamos el criptograma "ELIX". Obtener la clave y descifrar el mensaje sabiendo que la última letra del mensaje en claro es "A".

3. Siguiendo paso a paso el algoritmo de Euclides calcular $d = \text{mcd}(a, b)$. Retrocediendo en el cálculo anterior, encontrar números enteros u y v tales que $d = au + bv$.

a) $a = 3$, $b = 26$.

b) $a = 22$, $b = 28$.

c) $a = 15$, $b = 28$.

4. Calcular $d = \text{mcd}(a, b)$ con el algoritmo de Euclides. Encontrar números enteros u y v tales que $d = au + bv$.

a) $a = 21$, $b = 15$.

b) $a = -21$, $b = 15$.

c) $a = 21$, $b = -15$.

d) $a = -21$, $b = -15$.