Códigos y Criptografía (GIINF)

Practica Cifrado Mochila

ALBERTO LUQUE RIVAS

1. ¿Cuáles de las siguientes secuencias numéricas representan mochilas supercrecientes?

(a){5,10,8,3}
(b){5,10,12,40}
(c){5,10,16,40.2}
(d){5,10,16,40} , ya que sus numeros consecutivos son mayores a la suma de todos los anteriores, y son enteros positivos.

2. Dada la mochila supercreciente {2,3,6,12,25}, comprobar si el problema de la mochila tiene solución para los siguientes valores, y en caso afirmativo hallar los x_i's correspondientes:

(a) 1, no tiene solucion.
(**b) 15, si tiene solucion:**
(0,1,0,1,0), conseguido en 4 iteraciones.
(c) 24, no tiene solucion.
(d) 27, si tiene solucion:
(1,0,0,0,1), conseguido en 5 iteraciones.

(e) 50, no tiene solucion.

3. Dada la mochila{3,1,15,2,4}, cifra el mensaje: 'HOLA'

Primero debemos de pasar a codigo ASCI y luego a binario el mensaje a cifrar.

H = 01001000
O = 01001111
L = 01001100
A = 01000001111

El **n** de la mochila es de 5, debemos de coger de 5 en 5 elementos todos los bits del mensaje a cifrar.

Segundo representamos la cadena de 5 bits en la mochila

01001 = {3,1,15,2,4} = 5
00001 = {3,1,15,2,4} = 4
00111 = {3,1,15,2,4} = 21
10100 = {3,1,15,2,4} = 18
11000 = {3,1,15,2,4} = 4
10000 = {3,1,15,2,4} = 3
01111 = {3,1,15,2,4} = 22

El mensaje cifrado es **(5 4 21 18 4 3 22)**

4. Dada la mochila supercreciente {2,3,6,12,25}, descifra el criptograma (3 31 12 6 14 39 17 39).

Debemos de aplicar lo del ejercicio 3 pero al reves empezaríamos por el paso 2.

3 = {2,3,6,12,25} = 01000
31 = {2,3,6,12,25} = 00101
12 = {2,3,6,12,25} = 00010
6 = {2,3,6,12,25} = 00100
14 = {2,3,6,12,25} = 10010
39 = {2,3,6,12,25} = 10011
17 = {2,3,6,12,25} = 11010
39 = {2,3,6,12,25} = 10011

Agrupamos en cadenas de 8 bits:

0100000101000100010010010100111101010011

El mensaje cifrado es : **ADIOS**

5. Dada la mochila{2,3,7,13}, ¿tienen los siguientes números factores comunes con alguno de sus elementos?

(a) 8 , tiene factor común con el 2.

(b) 5 , no tiene factor comunes y ademas es primo.

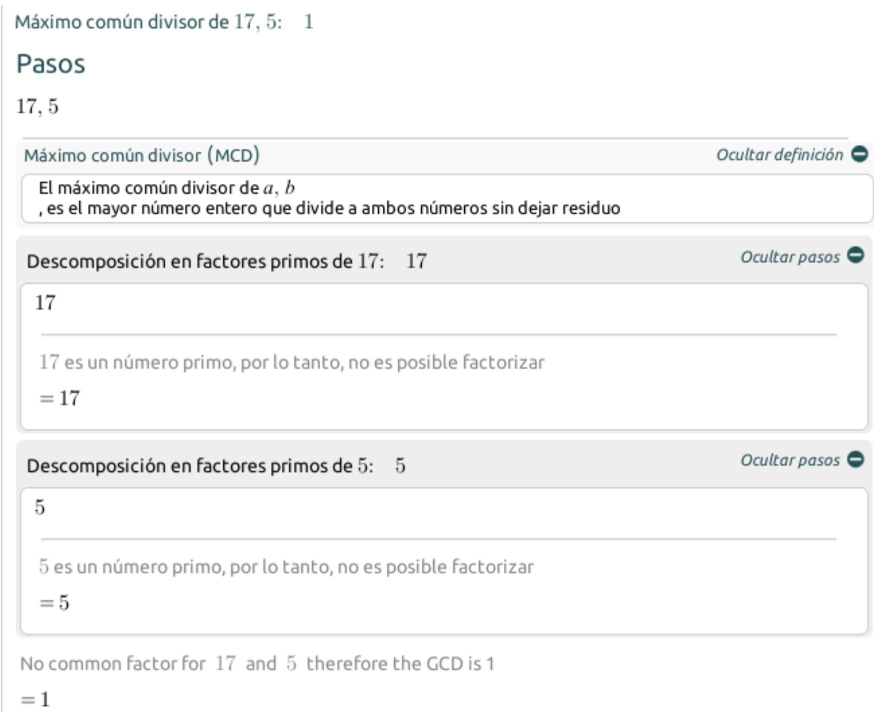
(c) 12, tiene factores comunes con 2 y 3.

6. ¿Es la mochila {1,2,4,8} supercreciente? Si es así, ¿es el valor m= 17 adecuado como módulo para el criptosistema de la mochila con trampa?, ¿y el elemento multiplicativo w= 5 es también adecuado? En caso afirmativo generar a partir de estos valores una clave pública y una clave privada válidas para dicho criptosistema.

La mochila si es supercreciente, cumple los requisitos para ello, es positiva de carácter numérico entero y cada valor nuevo es superior a la suma de todos los anteriores.

El modulo es adecuado pues 17 es mayor a la suma de todos los elementos de la mochila.

Si el elemento multiplicativo es 5 se calcula el **mcd** de 17 y 5, **mcd(17,5)** = 1 , si el **mcd** es 1 es adecuado. Por ser M.C.D.(m,w) = 1, existe el inverso modular de **w** y se puede revertir el proceso.



La clave privada para nuestro problema constaría de 3 elementos, **mochila**, modulo **m** y factor multiplicativo **w**:

mochila = **{1,2,4,8}**
m = **17 , se cumple que m > 2a_n en todos los casos.**
w = **5**

Para la clave publica cogemos el factor multiplicativo **w** multiplicamos cada elemento de la mochila por **w** y aplicando el modulo **m**.

mochila * w = **{5,10,3,6}**

7. Utilizar la clave pública del ejercicio 6 para cifrar el mensaje 'M O C H I L A'

Primero debemos de pasar a codigo ASCI y luego a binario el mensaje a cifrar.

M = 0100 1101
O = 0100 1111
C = 0100 0011
H = 0100 1000
I = 0100 1001
L = 0100 1100
A = 0100 0001

El **n** de la mochila es de 4, debemos de coger de 4 en 4 elementos todos los bits del mensaje a cifrar.

Ahora ciframos:

0100 = {5,**10**,3,6} = 10
1101 = {**5**,**10**,3,**6**} = 21
0100 = {5,**10**,3,6} = 10
1111 = {**5**,**10**,**3**,**6**} = 24
0100 = {5,**10**,3,6} = 10
0011 = {5,10,**3**,**6**} = 9
0100 = {5,**10**,3,6} = 10
1000 = {**5**,10,3,6} = 5

0100 = {5,**10**,3,6} = 10
1001 = {**5**,10,3,**6**} = 11
0100 = {5,**10**,3,6} = 10
1100 = {**5**,**10**,3,6} = 15
0100 = {5,**10**,3,6} = 10
0001 = {5,10,3,**6**} = 6

Mensaje cifrado = **(10 21 10 24 10 9 10 5 10 11 10 15 10 6)**

8. Mediante la clave privada del ejercicio 6, descifrar el criptograma 16 10 16 3 10 6 10 21 16 0 10 6.

Primero debemos de sacar el inverso de **w** en modulo **m**

$5^{-1} \bmod 27 = 7$

Multiplicamos el inverso por cada componente del criptograma en modulo 27:

(10 2 10 4 2 8 2 11 10 0 2 8)

Aplicamos:

10 = {1,**2**,4,**8**} = 0101
2 = {1,**2**,4,8} = 0100
10 = {1,**2**,4,**8**} = 0101
4 = {1,2,**4**,8} = 0010
2 = {1,**2**,4,8} = 0100
8 = {1,2,4,**8**} = 0001
2 = {1,**2**,4,8} = 0100
11 = {**1**,**2**,4,**8**} = 1101
10 = {1,**2**,4,**8**} = 0101
0 = {1,2,4,8} = 0000
2 = {1,**2**,4,8} = 0100
8 = {1,2,4,**8**} = 0001

Agrupamos en cadenas de 8 bits:

010101000101001001000001010011010101000001000001

El mensaje cifrado es : **TRAMPA**

9. Conocida la clave pública de un criptosistema de mochila con trampa{5,10,3}, y el módulo m= 21, aplicar el criptoanálisis de Shamir y Zippel para obtener la clave privada, es decir,la mochila supercreciente.

Averiguar W y Mochila

Cogemos para candidato a **a1** el valor mas chico de la mochila con trampa y que tenga inverso en modulo 21.

En este caso es el 5 que es **b1** donde su inversa en modulo 21 es 17.

Hayamos el valor de **q** que se calcula como q = 5*17 mod 21 , q = 1 mod 21.

Calculamos los múltiplos Como n= 3, hallamos{q,2q,...,2^{3+1}q} modulo 21.

El menor de los múltiplos es 1 nuestro candidato a **a1 es 1.**

El factor de multiplicación sería w=$b_1 a^{-1}_1$mod m , w= 5*1 , w=5 mod 21.

a_2 = 17 * 10 mod 21 = **2**
a_3 = 17 * 3 mod 21 = **9**

La clave privada seria **(1,2,9)**