# Ejercicios Tema 5 y 6

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Justo Peralta López

**Teoría de Códigos y Criptografía**

**Grado Ingeniería Informática** Curso **2018/19**

# Tema 5

## 1. Cifra el texto “Este es mi primer ejercicio de Criptografía Utilizando el cifrador de Cesar con un desplazamiento de 7 caracteres. Descifra el texto encriptado obtenido para comprobar el resultado.

Este es mi primer ejercicio de Criptografía

LZAL LZ TP WYPTLY LQLYJPJPV KL JYPWAVNYHMíH

El alfabeto de referencia es: ABCDEFGHIJKLMNOPQRSTUVWXYZ.

## 2. Descifra el siguiente texto sabiendo que ha sido encriptado utilizando un cifrador de tipo Cesar: “Sld cpdfpwez nzccpnelxpyep pdep pupcntntz op nctaezrclqtl jafpopd nzyetyflc nzy wl cpwlntzy op aczmwpxld” Obtén la clave secreta utilizada.

La semilla es : 11

El resultado es: HAS RESUELTO CORRECTAMENTE ESTE EJERCICIO DE CRIPTOGRAFIA Y PUEDES CONTINUAR CON LA RELACION DE PROBLEMAS

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Justo Peralta López

**Teoría de Códigos y Criptografía**

**Grado Ingeniería Informática** Curso **2018/19**

# Tema 6

## 4. Calcula Φ(113) , Φ(143) y Φ(128) .

Φ(113) = 113 - 1 = 112 -> según el lema 2.2.1.2  (113 es primo)

Φ(143) = Φ(11) Φ(13) ->según el lema 2.2.1.1  10 * 12 =120

Φ(128)= Φ(2^7) = 2^7 - 2^6 = 64 para todo p primo y k > 1 -> según el lema 2.2.1.3

## 5. Calcula un número primo aleatorio de 10 cifras.

Utilizamos la fórmula 2^p - 1.

Al pedirnos un número de 10 cifras sería, 2^31 - 1 = 2147483647

## 6. Sean n = 13 · 17 y e = 7 la clave pública de un criptosistema RSA. Calcula la correspondiente clave privada.

n=221; p=13; q=17; e=7

La clave pública es (221,7).

Podemos obtener Φ(221) = 12 * 16 = 192

7 * d = 1mod(192) → d = 55

La clave privada es (211,55)

## 7. Encripta el mensaje m = 8 utilizando el criptosistema RSA del ejercicio 6.

m=8

clave pública (211,55)

0<m<=220

e=8^7(mod 211)-> e=83

## 8. Descifra el mensaje c = 8 utilizando el criptosistema RSA del ejercicio 6.

e=8

clave privada (211,55)

m=8^55(mod 211) -> m=83

## 9. Sabiendo que una fuente envía a 3 destinatarios distintos con claves públicas RSA(1003 , 3) , (1219 , 3) y (1363 , 3) respectivamente el mismo mensaje m y hemos interceptado los tres cifrados respectivos c1 = 191, c2 = 972 y c3 = 834, encuentra el mensaje m sin factorizar los módulos de cada una de las claves públicas de los usuarios.

X = 191 (mod 1003)

X = 972 (mod 1219)

X = 834 (mod 1363)

mismo mensaje m

X= 834 + 1363K -> 834 + 1363K = 972 (mod 1219)

1363K = 138 (mod 1219)

144K = 138 (mod 1219) -> K= 966 (mod 1219)

K = 966 + 1219M

X = (966 + 1219M) 1363 + 834 = 1317492 + 1661497M

1317492 + 1661497M = 191 (mod 1003)

553 + 529M = 191 (mod 1003)

529M = 641 (mod 1003)

M = 771 + 1003T

X = 1281014187 + 1666481491T -> m debe ser un entero positivo menor que 1666481491=n1n2n3 nos quedamos con T=0

X = M ^ 3

M = raíz_cubo(1281014187) = 1086

## 10. Sean (1363 , 3) y (1363 , 5) las claves publicas dos usuarios ́ u 1 y u 2 del criptosistema RSA. Supongamos que el mismo mensaje m ha sido enviado a ambos usuarios, resultado c 1 = 1185 y c 2 = 1039 respectivamente. Calcula m sin factorizar el número 1363.

Ataque con módulo común no1, obtenemos lo siguiente:

3S + 5T = 1

S = 2

T = -1

m = m^(e1S * e2T) (mod n) → m^(e1S) * m^(e2T) (mod n) → C1^S * C2^T (mos n)

m = 1185^(2) * 1039^(-1) (mod 1363)

m = 1351,5158 (mod 1363)

m = 11,48

m ≈ 11

## 12. Comprueba que 3 es un generador de Z ∗ 43. Sea ( p = 43, g = 3, g a = 37) la clave pública de un criptosistema ElGamal.

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Justo Peralta López

**Teoría de Códigos y Criptografía**

**Grado Ingeniería Informática** Curso **2018/19**

$q = 2p + 1 = 87$

Si $g^2 \neq 1 \pmod{p}$ y $(g^a)^q \neq 1$ Es generador.

$37^2 \equiv 43\ 1$  falso.

$37^{87} \equiv 43\ 1$ es falso, por lo que el número es generador.

a) Encripta el mensaje $m = 8$

$K = 2$ número generado al azar $0 \geq K \leq p - 2$

$h = g^K = 3^2 = 9 \pmod{43}$

$d = m*(g^a)^K = 8* (37)^2 \pmod{43}$

$c = ( 9 , 30 )$

b ) Sabiendo que $a = 7$ es la clave secreta, descifra el resultado del apartado anterior.

$a = 7$

$m = h^{(p-1-a)} * d$

$m = (9^{35}) * 30 \pmod{43}$

$m = 8$

## 13. Sean n los parámetros público de un criptosistema ElGamal cuya clave pública es( p = 43, g = 3, g a = 32). Encripta, usando como parámetro privado aleatorio k = 5 el mensaje m = 6 . Sabiendo que el mensaje cifrado c 0 = (28 , 39) se ha obtenido

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Justo Peralta López

**Teoría de Códigos y Criptografía**

**Grado Ingeniería Informática** Curso **2018/19**

**usando el mismo criptosistema y el mismo parámetro privado k = 5, descifra el mensaje original cuyo encriptado es c` .**

ENCRIPTADO

h = g^k = 3^5 = 243 (mod 43) = 28

d = m* (g^a)^k = 6 * 32^5 = 201326592 (mod 43) = 33

c=(28,33)

DECODIFICADO

k = 5

c` = ( 28 , 39 )

$$\frac{d}{d} = \frac{m}{m`} \rightarrow \frac{33}{39} = \frac{6}{m`}$$

33m`=234(mod 43)

m`=11

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Justo Peralta López

**Teoría de Códigos y Criptografía**

**Grado Ingeniería Informática** Curso **2018/19**

Miguel Santiago Cervilla

Firmado digitalmente por Miguel Santiago Cervilla
Fecha: 2019.01.13 21:19:14 +01'00'

**Alumno:** Miguel Santiago Cervilla

**Profesor:** Justo Peralta López

**Teoría de Códigos y Criptografía**

**Grado Ingeniería Informática** Curso **2018/19**