PRÁCTICA

Módulos 2 y 3: Criptografía de clave privada y criptografía de clave pública

Objetivos

Utilizar los principales conceptos que aparecen en los **módulos 2 y 3** de *Criptografía de clave privada* y Criptografía *de clave pública* para la transmisión de información confidencialmente. Se trata de utilizar los conocimientos adquiridos en los módulos correspondientes de la asignatura.

Formato y fecha de entrega

Redacción de un informe. Creación de un informe en formato pdf con todas las explicaciones de cada uno de los apartados de la práctica. No se trata de copiar ni de reproducir los conceptos explicados en el material escrito de la asignatura. Si se utilizan fuentes externas hay que referenciarlas.

El formato de entrega:

1) fichero PDF con el informe especificado anteriormente +
2) cualquier otro tipo de fichero adicional que hayáis creado para hacer la práctica (si es necesario).

Fecha límite: **7 de abril de 2019**

Buzón de entrega: **buzón para entregar prácticas (Registro EC núm. 2)**

Archivos para entregar: Informe en formato pdf. En caso de que se tenga que entregar más de un fichero estos se tendrán que enviar comprimidos.

Herramientas

- Miniaplicación RSA contenida en el material web de la asignatura o
- http://aurea.es/demos/criptografia/pag/calculadoraRSA.html o

en http://materials.cv.uoc.edu/continguts/PID_00199760/index.html dentro del punto *1.2.1 Método* del Módulo 3.

Criterios de evaluación

- Realización de los objetivos marcados.
- Claridad a la exposición del informe.

Recordad detallar en el informe todo lo que hacéis y adjuntad las imágenes que consideráis oportunas. Justificad todo lo que comentáis o explicadlo, aunque sea de manera breve.

Propiedad intelectual

A menudo es inevitable, al producir una obra multimedia, hacer uso de recursos creados por terceras personas. Es por lo tanto comprensible hacerlo en el marco de una práctica de los estudios del Grado Multimedia, siempre y esto se documente claramente y no suponga plagio en la práctica.

Por lo tanto, al presentar una práctica que haga uso de recursos ajenos, se tiene que presentar junto con ella un documento en que se detallen todos ellos, especificando el nombre de cada recurso, su autor, el lugar donde se obtuvo y su estatus legal: si la obra está protegida por el copyright o se acoge a alguna otra licencia de uso (Creative Commons, licencia GNU, GPL ...). El estudiante tendrá que asegurarse que la licencia que sea no impide específicamente suyo uso en el marco de la práctica. En caso de no encontrar la información correspondiente tendrá que asumir que la obra está protegida por el copyright.

Se tendrán que adjuntar además los ficheros originales cuando las obras utilizadas sean digitales, y su código fuente si corresponde.

Otro punto a considerar es que cualquier práctica que haga uso de recursos protegidos por el copyright no podrá en ningún caso publicarse en Mosaico, la revista del Graduado en Multimedia a la UOC, a no ser que los propietarios de los derechos intelectuales den su autorización explícita.

Plagio

Salvo que se especifique de manera diferente en el enunciado, las pruebas de evaluación continua y prácticas se tienen que hacer de forma individual. En caso de detectar actividades plagiadas, todas ellas serán calificadas con una nota de D.

MÓDULO 2. CRIPTOGRAFÍA DE CLAVE PRIVADA

Es muy sabido que la criptografía, desde la antigüedad clásica, ha servido, a lo largo de la historia, para esconder deseos inconfesables, intrigas, asesinatos, revanchas,… y ha sido una fuente inagotable para resolver las más bajas necesidades humanas de ambición y poder.

En esta parte de la práctica nos adentraremos en una historia de ficción ambientada en un contexto misterioso con aspectos del cual tendréis que adivinar con las pistas que os daremos a continuación.

1. Sabemos que esta novela, sucede sobre un río, que atraviesa de largo un país el nombre del cual está encriptado por el método de César, pero no recordamos la clave secreta.

El mensaje encriptado c es:
JLCUY

Encontrad el mensaje m original y la clave secreta k teniendo en cuenta que detrás las 27 letras del abecedario (incluyendo la ñ) añadimos un carácter espacio (_). **(0,5 puntos)**
SOLUCIÓN:
$k = 5$
EGYPT

2. En esta misma novela, una joven adinerada, el nombre de la cual está encriptado por el método de Vernam marcará la trama de la historia. La clave privada utilizada es:

k = 11101011 00100111 00010010 10111010 01111011 00111010
01110010 00010111 11100110 00101111 10011110 01110000

Y el mensaje recibido es:
c = 10100111 01101110 01011100 11110100 00111110 01101110
00101101 01010011 10101001 01110110 11010010 00110101

a) Así pues, ¿cuál es el mensaje original *m*? **(0.75 puntos)**

SOLUCIÓN

Según el código ASCII $m = c - k$:

c = 10100111 01101110 01011100 11110100 00111110 01101110

k = 11101011 00100111 00010010 10111010 01111011 00111010

_____

m = 01001100 01001001 01001110 01001110 01000101 01010100

L Y N N E T

00101101 01010011 10101001 01110110 11010010 00110101

01110010 00010111 11100110 00101111 10011110 01110000

_____

01011111 01000100 01001111 01011001 01001100 01000101

_ D O Y L E

m = LINNET_DOYLE

b) ¿Qué le sucede a este personaje? Averiguadlo. **(0.25 puntos)**

SOLUCIÓN

Aparecerá asesinada en su camarote del barco mientras hace un viaje por el río Nilo.

3. Cabe decir que, en esta novela, se produce un delito. En el siguiente texto encriptado podréis encontrar las claves principales:

%#86 8(ñ (+(7€ $0 t8$#6 +7#t$3#1 7 €6(37#6ñ t8(t 9862 7 86(€ñ t8(t $26 8(ñ /662 0$52ñ 72 €$#(376 $tt6€/$5€26># 8(2ñ/(< t86 ñ(* $0 t86 #6(€)81 @()=563726 #(t (t t86 #(&6 t(/36 (# t86* ñ7ñ1 9862 #86 €6(37#6ñ t8(t t86€6 9(# <$72< t$ /6 (#6(€)8 #86 #37++6ñ 7t 72t$ t86 $t86€ <7€3># 8(2ñ/(<1 3(t6€ #86 962t t$ €$#(376>#)(/72 (2ñ <$t 7t /(){ (0t6€ 8(}72< ñ7#t€()t6ñ 86€ (tt62t7$2 97t8 ( )$&+(€7#$2 $0 37+#t7){#1 (# /$t8 #86 (2ñ 86€)(/72 8(ñ /662 #6(€)86ñ *6#t6€ñ(* 7t 9(#2>t t8$5<8t 26)6##(€* t$ ñ$ 7t (<(721% &€#1 (336€t$2 #(7ñ∞ %*$5 9(2t6ñ 86€ t$ t({6 t8(t 9(* $5t£% %*6#1 /5t #86 9$53ñ 2$t t({6 7t (3$261 t8(t 7# 98* #7&$2 Ñ$*36 8(# ñ76ñ (2 6(#76€ ñ6(t8 t8(2 86 ñ6#6€}6ñ1% &€#1 (336€t$2 #87}6€6ñ1

De este texto sabemos que las frecuencias de aparición más altas de los caracteres en el código inicial del mensaje *m*, en el cual está encriptado el siguiente mensaje *c*, son:

DE MÁS A MENOS FRECUENTE

1. e
2. a
3. t
4. h

A partir del sistema del ataque estadístico encontrad la desencriptación del texto anterior (que no distingue mayúsculas y minúsculas y sí distingue letras acentuadas en caso de que haya). Los espacios entre palabras no están codificados. **(1,5 puntos)**

SOLUCIÓN

Este es un fragmento final de la novela *Death on the Nile* donde se dan algunas de las pistas sobre el asesinato producido:

"She had a pair of those pistols. I realised that when I heard that one had been found in Rosalie Otterbourne's handbag the day of the search. Jacqueline sat at the same table as they did. When she realised that there was going to be a search she slipped it into the other girl's handbag. Later she went to Rosalie's cabin and got it back after having distracted her attention with a comparison of lipsticks. As both she and her cabin had been searched yesterday it wasn't thought necessary to do it again." Mrs. Allerton said: "You wanted her to take that way out?" "Yes. But she would not take it alone. That is why Simon Doyle has died an easier death than he deserved." Mrs. Allerton shivered.

FUENTE:

https://ngwcreaderscorner.webs.com/Death%20on%20the%20Nile.pdf

MENSAJE *m*	MENSAJE ENCRIPTADO *c*	FRECUENCIA del carácter en el mensaje *m*
"	%	6
.	1	12
t	4	60
l	3	18
w	9	10

f	0	5
n	2	33
b	/	12
u	5	8
y	*	10
i	7	36
o	$	34
d	ñ	30
p	+	6
a	(	62
c	)	11
r	€	30
q	=	1
e	6	71
g	<	9
h	8	44
s	#	43
m	&	5
j	@	1
k	{	4
`	>	t
?	£	1
:	∞	1
v	}	3

4. Tenéis que saber que esta novela tiene una famoso personaje belga el nombre del cual ha sido encriptado con una clave privada para una encriptación de Vigenère formada por longitud del bloque igual a 3 caracteres y claves $k_1 = 4$, $k_2 = 2$ y $k_3 = 3$ que os pedimos que encontréis.

Teniendo presente:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**_**	
15	16	17	18	19	20	21	22	23	24	25	26	27	

Y sabiendo que el mensaje encriptado *c* es:

c = LGUGWOIUCTQLVQW

Encontrad el mensaje m original. **(0,5 puntos)**

SOLUCIÓN

m = HERCULES_POIROT

5. Como última pista, diremos que el nombre de la novelista ha sido **encriptado** según el método de clave privada basado en las transposiciones utilizando una longitud de bloque de 5 caracteres y la permutación:

$$1 \to 4$$
$$2 \to 1$$
$$3 \to 2$$
$$t \to 5$$
$$5 \to 3$$

El mensaje encriptado *c* es:

GAHAT_CRAHSTEII

Encontrad el mensaje m original. **(1 punto)**

SOLUCIÓN

m = AGATHA_CHRISTIE

6. Con toda esta información, averiguad cuál es la novela a la que nos hemos referido durante toda esta parte de la práctica. **(0,5 puntos)**

SOLUCIÓN

Como habréis podido deducir, la novela a la cual hacíamos referencia es *Death on the Nile*, de Agatha Christie.

Como curiosidad, aquí tenéis una teoría matemática para encontrar quién es el asesino en las novelas de Agatha Christie.

MÓDULO 3. CRIPTOGRAFIA DE CLAVE PÚBLICA

1. Christian quiere enviar un mensaje $m = NIL$ a Ágata a través de un canal no seguro. Para eso, deciden acordar que el algoritmo criptográfico a utilizar será el RSA. Para pasarlo a código numérico, utilizaremos el siguiente alfabeto:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**_**	
15	16	17	18	19	20	21	22	23	24	25	26	00	

a) Si sabemos que Ágata escoge la siguiente pareja de números primos: $p_{Ágata} = 173$, $q_{Ágata} = 313$, según el teorema de Euler, podría enviar Christian este mensaje a Ágata ? **(0,5 puntos)**

SOLUCIÓN

Las condiciones para el método RSA son:

1) p i q tienen que ser números primos

2) $e \cdot d \equiv 1 \, mod \, (p-1)(q-1)$

3) m no divisible ni por p ni por q (por el teorema de Euler).

En este caso $m = 140912$ no es divisible ni por p $\frac{m}{p} = \frac{140912}{173} = 814{,}52$ ni por q: $\frac{m}{q} = \frac{140912}{313} = 450{,}19$, por tanto Christian sí puede enviar el mensaje m a Àgata por el método RSA.

b) Podemos decir que la opción $e_{Ágata} = 181$ se puede considerar una clave pública? **(0,75 puntos)**

SOLUCIÓN

Hace falta primero encontrar

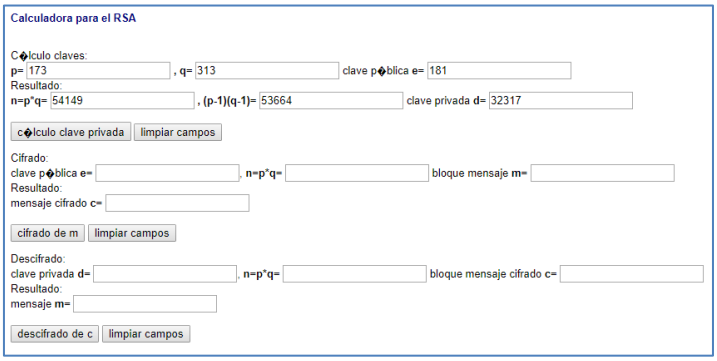
$$n_{Ágata} = p \cdot q = 173 \cdot 313 = 54149$$

$$(p-1) \cdot (q-1) = (173-1) \cdot (313-1) = 172 \cdot 312 = 53664$$

La clave pública e tiene que cumplir que es un número coprimo con $(p-1) \cdot (q-1)$ y por tanto no puede ser factor común del resultado $(p-1) \cdot (q-1)$. Es decir, no tienen ningún factor primero en común o, dicho de otra manera, sólo tienen 1 como divisor común.

Si observamos $181 = 1 \cdot 181$ es un número primo y $53664 = 2^5 \cdot 3 \cdot 13 \cdot 43$. Por tanto, e puede ser una clave pública puesto que 181 y 53664 no tienen ningún factor primero en común, o dicho de otra manera, sólo tienen 1 como divisor común.

Si lo comprobamos con la calculadora RSA:
http://aurea.es/demos/criptografia/pag/calculadoraRSA.html



c) ¿Y si $e_{Ágata} = 301$? ¿Se puede considerar una clave pública? **(0,75 puntos)**

SOLUCIÓN

$$n_{Ágata} = p \cdot q = 173 \cdot 313 = 54149$$

$$(p-1) \cdot (q-1) = (173-1) \cdot (313-1) = 172 \cdot 312 = 53664$$

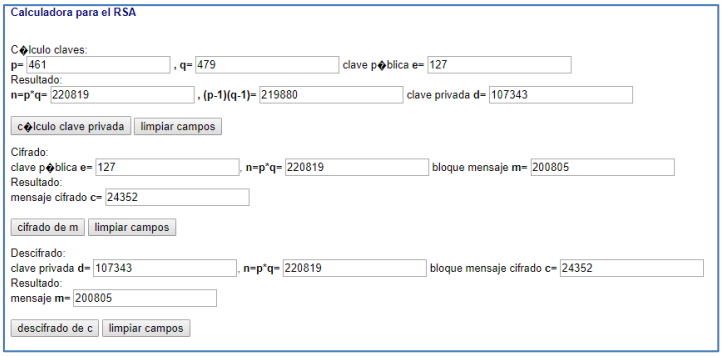
Como hemos dicho antes, la clave pública e tiene que cumplir que es un número coprimo y por tanto no puede ser factor común del resultado $(p-1) \cdot (q-1)$. Es decir, no tienen ningún factor primero en común, o dicho de otra manera, sólo tienen 1 como divisor común.
Si observamos $301 = 7 \cdot 43$ y $53664 = 2^5 \cdot 3 \cdot 13 \cdot 43$ vemos que e no puede ser una clave pública, puesto que 301 y 53664 tienen 43 como factor primero en común.

Si lo comprobamos con la calculadora RSA:
http://aurea.es/demos/criptografia/pag/calculadoraRSA.html

d) Seguidamente, Ágata con $q_{Ágata} = 461$ decide dar a conocer su clave pública $n_{Ágata} = 220819$, $e_{Ágata} = 127$ para que le enviemos mensajes cifrados con RSA. Si Christian le quiere enviar el mensaje $m = THE$, ¿qué mensaje codificado recibirá Ágata? ¿Qué clave privada usará la Ágata para descifrarlo? **(0,5 puntos)**

SOLUCIÓN

En este caso $n_{Ágata} = 220819$ implica que $p_{Ágata} = \frac{220819}{q_{Ágata}} = 479$, $m = 200805$ y si usamos la calculadora RSA vemos que para estos valores:



http://aurea.es/demos/criptografia/pag/calculadoraRSA.html

Y por tanto el valor del mensaje codificado que obtenemos es $c = 24352$ con la clave privada $d_{Ágata} = 107343$.

2. Anna ($p_{Ana} = 157$ $q_{Ana} = 167, e_{Ana} = 197$) conoce la clave pública de María ($p_{Maria} = 229$ $q_{María\,=251}, e_{María\,=263}$) y le quiere enviar un mensaje de forma que se asegure la máxima autenticidad y confidencialidad posible.

El mensaje que Ana quiere enviar a María es SLMO. Para pasarlo a código numérico, utilizaremos el siguiente alfabeto:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**_**	
15	16	17	18	19	20	21	22	23	24	25	26	00	

Se pide:

a) Encontrad el mensaje a encriptar *m*. **(0,5 puntos)**

SOLUCIÓN

En primer lugar, hace falta encontrar el mensaje m. Según el código numérico:

S	L	M	O
19	12	13	15

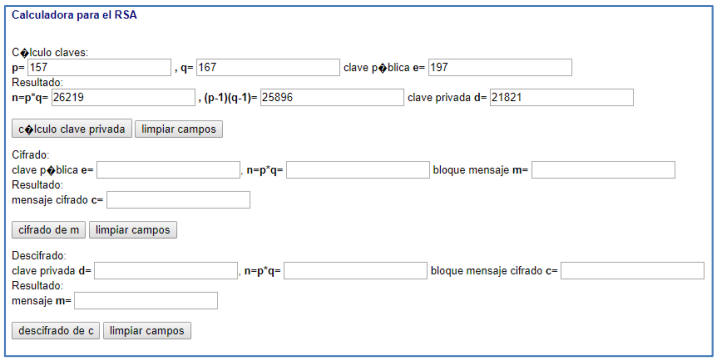
Por tanto el mensaje a encriptar será $m = 19121315$.

b) Encontrad las claves privadas de Ana y María. **(0,5 puntos)**

SOLUCIÓN

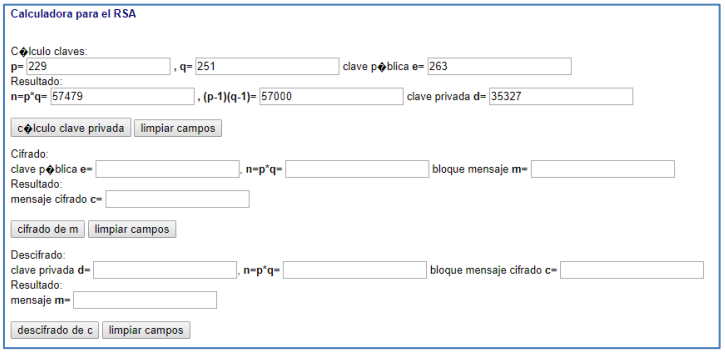
Calculamos la clave privada d con la clave pública e y la p la q que que ya conocía-mos y después desencriptamos el mensaje.

ANA



MARÍA

http://aurea.es/demos/criptografia/pag/calculadoraRSA.html



Así pues $d_{Ana} = 21821$ y d $d_{María} = 35327$.

c) Ana quiere enviar ahora el mensaje codificado SLMO de la manera que asegure la máxima autenticidad y confidencialidad posible. Encontrad el mensaje enviado a María separando el mensaje en bloques inferiores a n. **(1,5 puntos)**

SOLUCIÓN

Para buscar máxima AUTENTICIDAD, usaremos el método de la de firma digital. Para buscar CONFIDENCIALIDAD, a continuación, usaremos el método RSA de la forma habitual.

AUTENTICIDAD.

Procedimiento correcto, separando el mensaje m en bloques inferiores a $n_{Ana} = 26219$:

- Separación en bloques de una cifra menos de las que tiene el módulo con que se trabaja, en este caso bloques de 4 cifras: $m = 1912\,1315$, y si es necesario se llena con ceros (delante) para que nos salga un número entero de bloques. En este caso no será necesario.
- Calculamos la firma digital del mensaje m con la clave privada de Ana:
  s = $D_{d\ Ana}$ (m) = $D_{(d=21821,\ n=26219)}$ (1912)= 185
  s = $D_{d\ Ana}$ (m) = $D_{(d=21821,\ n=26219)}$ (1315)= 22483
  s = 18522483

CONFIDENCIALIDAD.

- Enviar encriptado a María con su clave pública:
  Es necesario separar en bloques de una cifra menos de las que tiene el módulo con que se trabaja $n_{María} = 57479$, en este caso bloques de 4 cifras, y si es necesario se llena con ceros (delante) para que nos salga un número entero de bloques:
  s = 18522483
  c = $E_{e\ María}$ (s) = $E_{(e=263,\ n=57479)}$ (1852) = 35425
  c = $E_{e\ María}$ (s) = $E_{(e=263,\ n=57479)}$ (2483) = 32421
  Resultado c = 3542532421
  $D \rightarrow$ uso del applet de desencriptació
  $E \rightarrow$ uso del applet de encriptació

  Nota: Si habéis hecho:
  c = $E_{e\ María}$ (s) = $E_{(e=263,\ n=57479)}$ (185) = 43453
  c = $E_{e\ María}$ (s) = $E_{(e=263,\ n=57479)}$ (22483) = 7631
  Resultado c = 434537631