

UNIVERSIDADE DA CORUÑA  
Facultade de Informática

## PPSD, Práctica 3: Protección de datos II

Losada Sánchez, Alicia  
`alicia.losada.sanchez@udc.es`

Muñiz Rodríguez, Nicolás  
`nicolas.muniz@udc.es`

Rivas Moar, Iago  
`iago.rivas@udc.es`

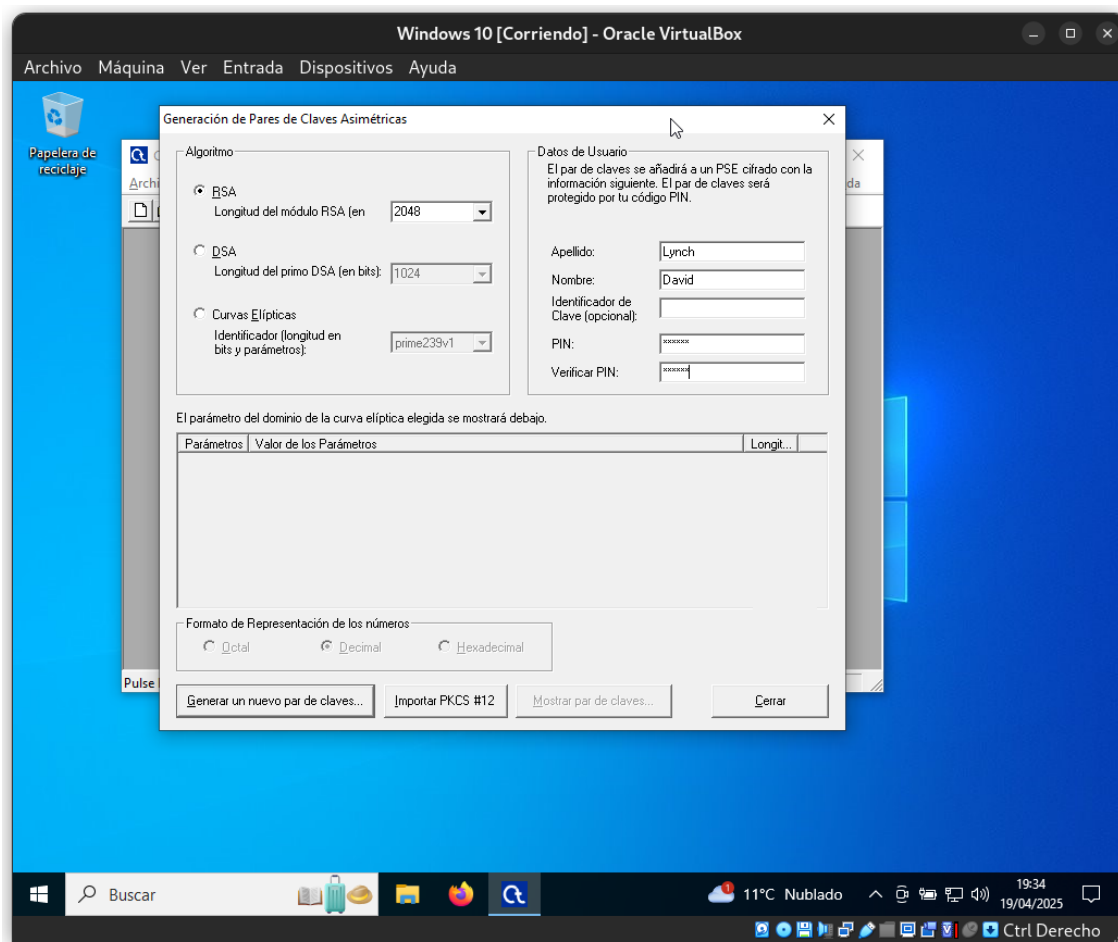
23 de abril de 2025

# Índice

<b>1. Criptografía moderna</b>	<b>3</b>
1.1. Ejercicio 1 . . . . .	3
1.2. Ejercicio 2 . . . . .	14
1.3. Ejercicio 3 . . . . .	14
<b>2. Certificados digitales</b>	<b>14</b>
2.1. Ejercicio 4 . . . . .	14
2.1.1. Certificados web . . . . .	14
2.1.2. Análisis con openssl . . . . .	19
2.2. Ejercicio 5 . . . . .	20
<b>3. PGP y S/MIME</b>	<b>20</b>
3.1. Ejercicio 6 . . . . .	20
3.2. Ejercicio 7 . . . . .	20
3.3. Ejercicio 8 . . . . .	20
3.4. Ejercicio 9 . . . . .	20
3.5. Ejercicio 10 . . . . .	20
3.6. Ejercicio 11 . . . . .	20
<b>4. Privacidad</b>	<b>20</b>
4.1. Ejercicio 12 . . . . .	20
4.2. Ejercicio 13 . . . . .	20
4.3. Ejercicio 14 . . . . .	20
4.4. Ejercicio 15 . . . . .	20
4.5. Ejercicio 16 . . . . .	20
4.6. Ejercicio 17 . . . . .	20

# 1. Criptografía moderna

## 1.1. Ejercicio 1



**Figura 1:** Generación del perfil del par de claves RSA

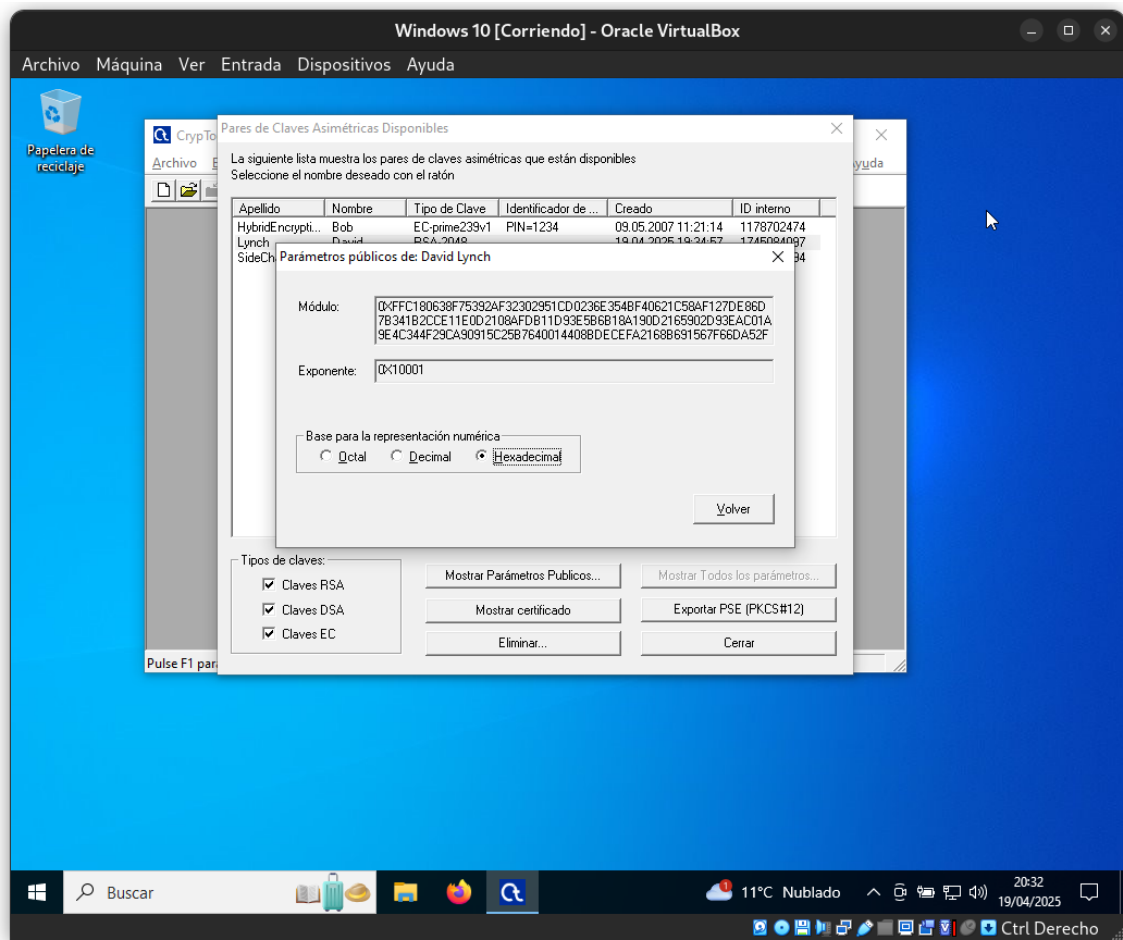


Figura 2: Parámetros públicos de la clave ( $n$ ,  $e$ )

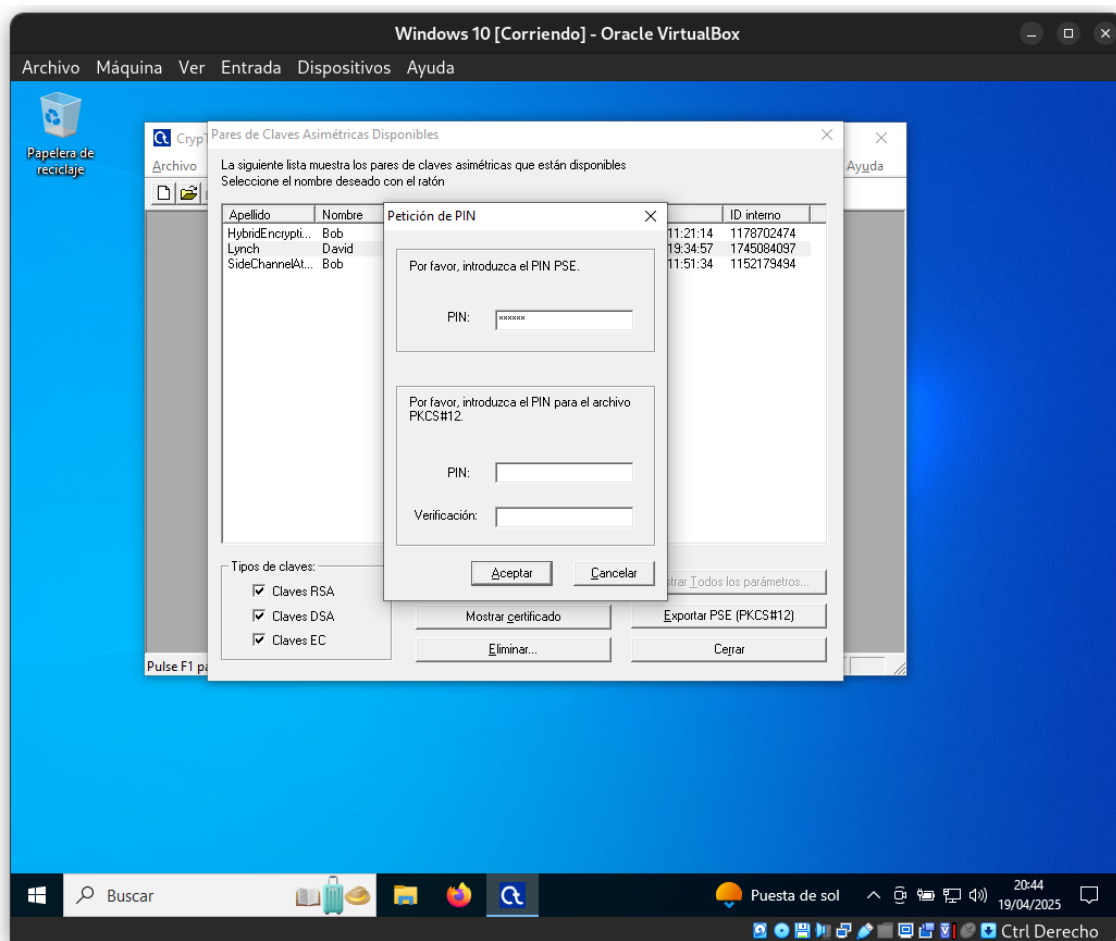


Figura 3: Pantalla del PIN de usuario

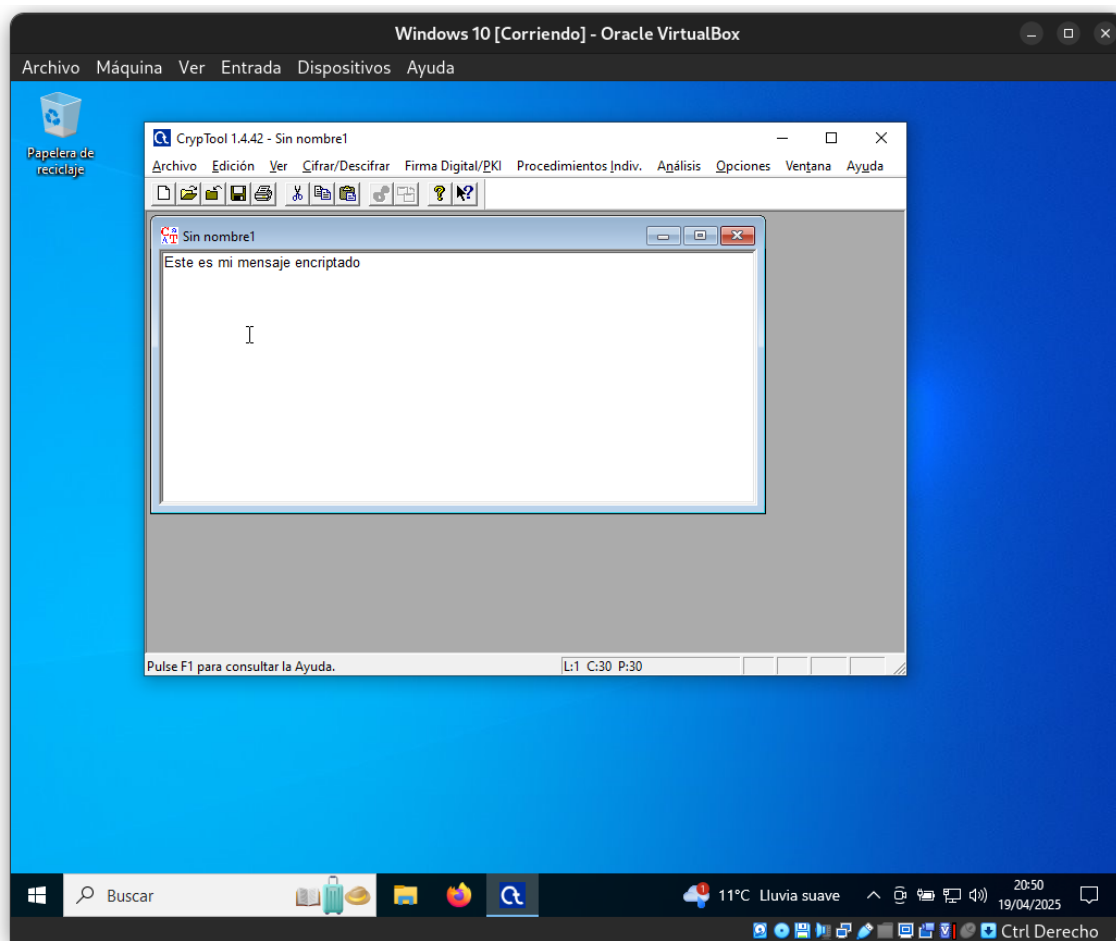
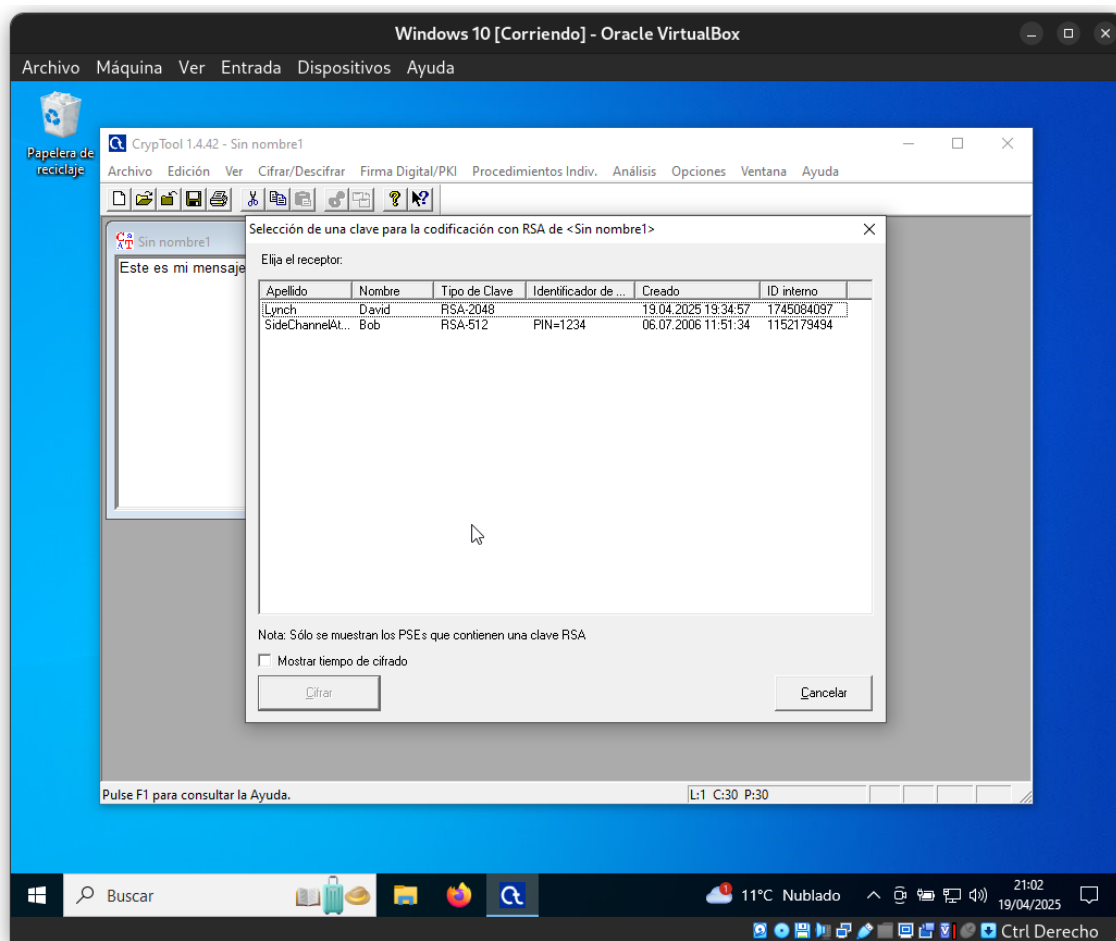


Figura 4: Texto de ejemplo para encriptar



**Figura 5:** Generación del perfil del par de claves RSA

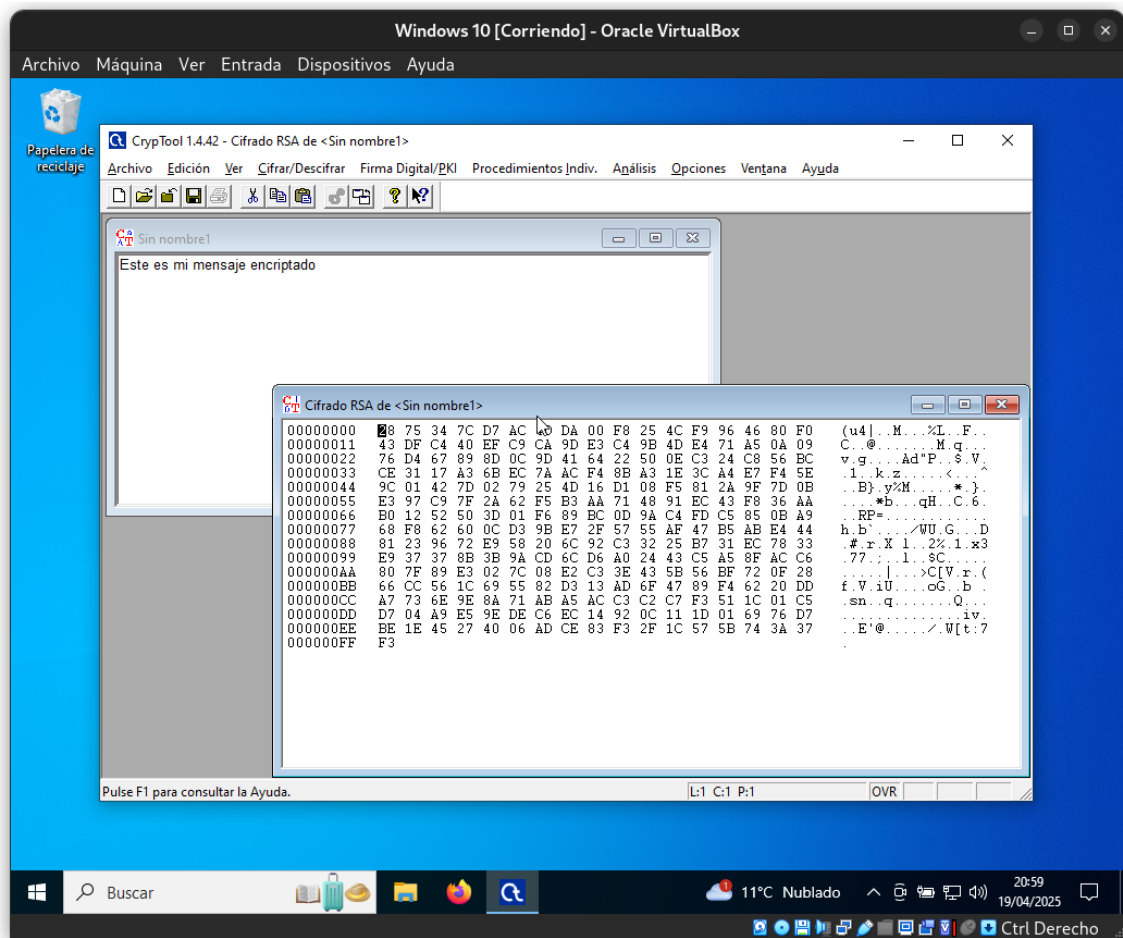


Figura 6: Generación del perfil del par de claves RSA



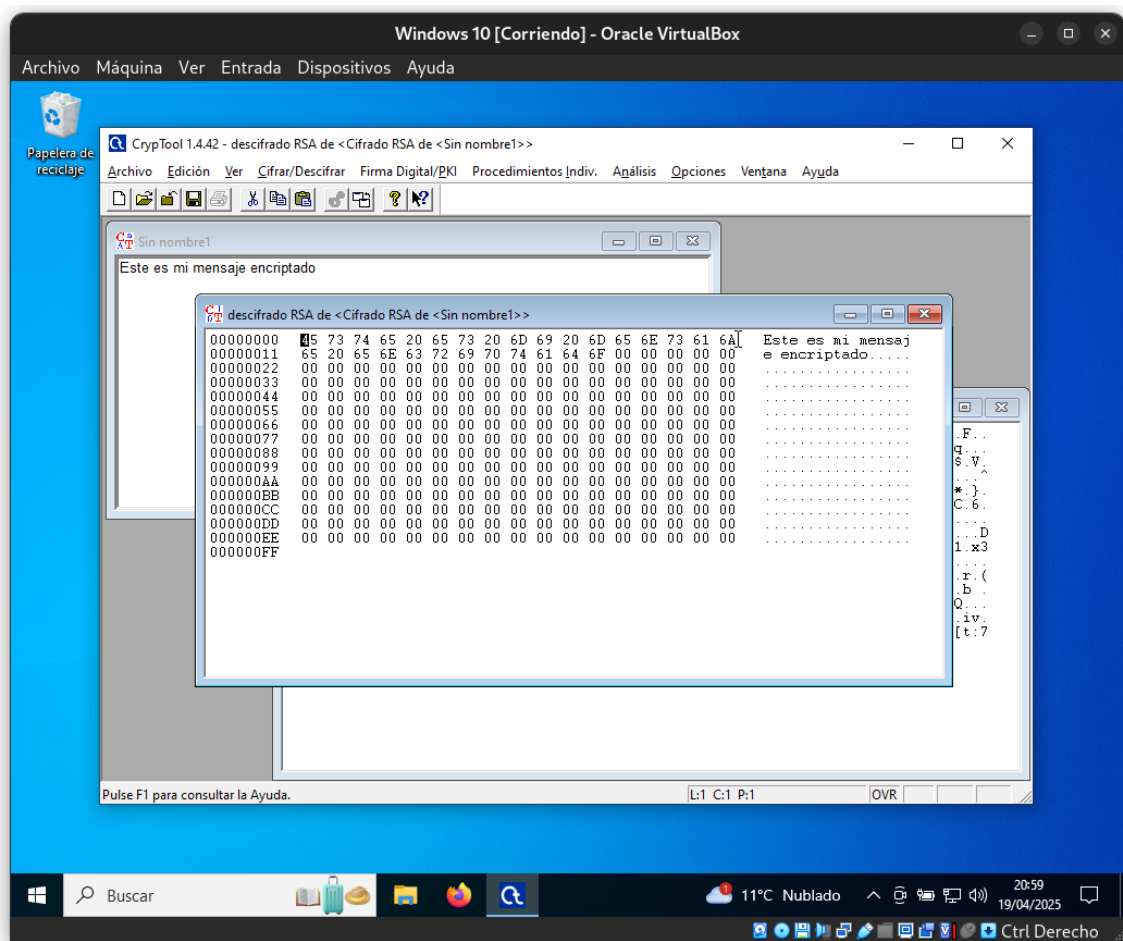


Figura 7: Generación del perfil del par de claves RSA

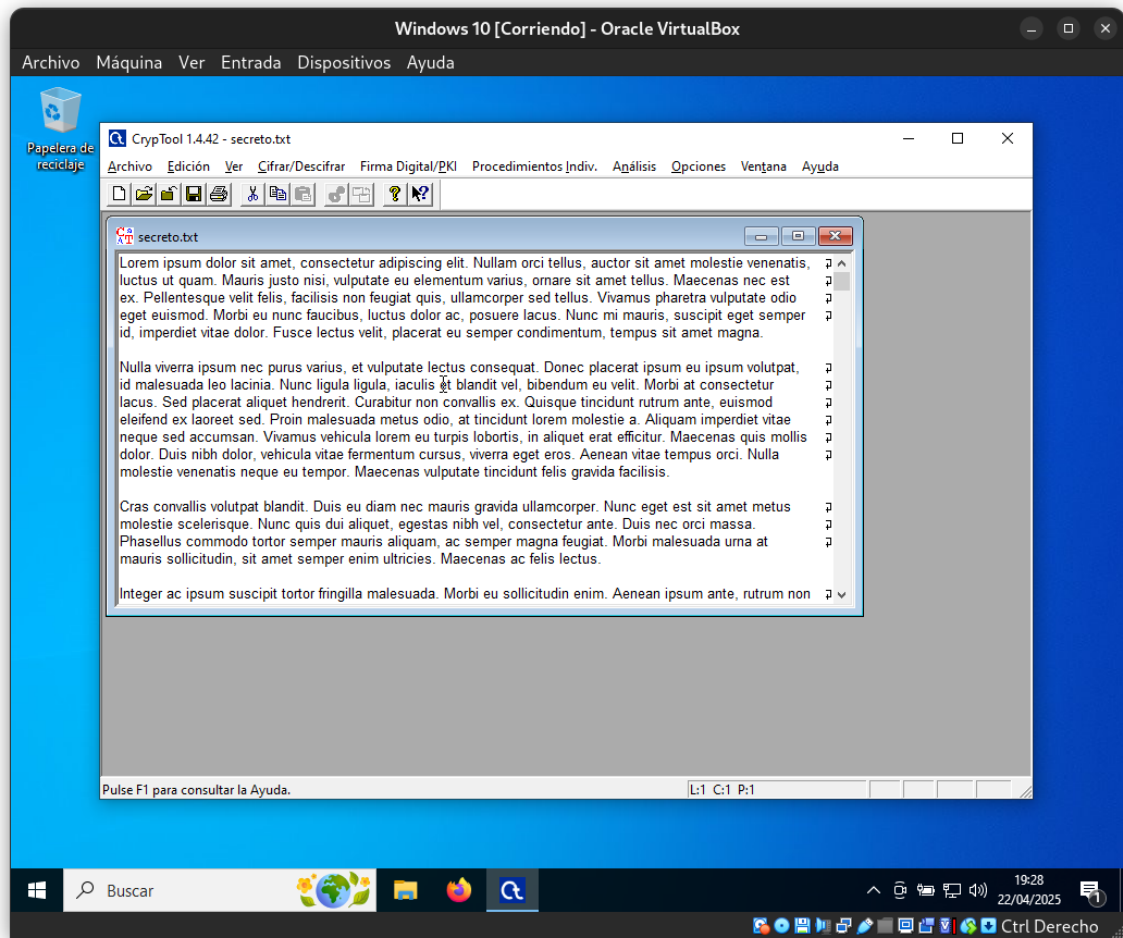


Figura 8: Generación del perfil del par de claves RSA

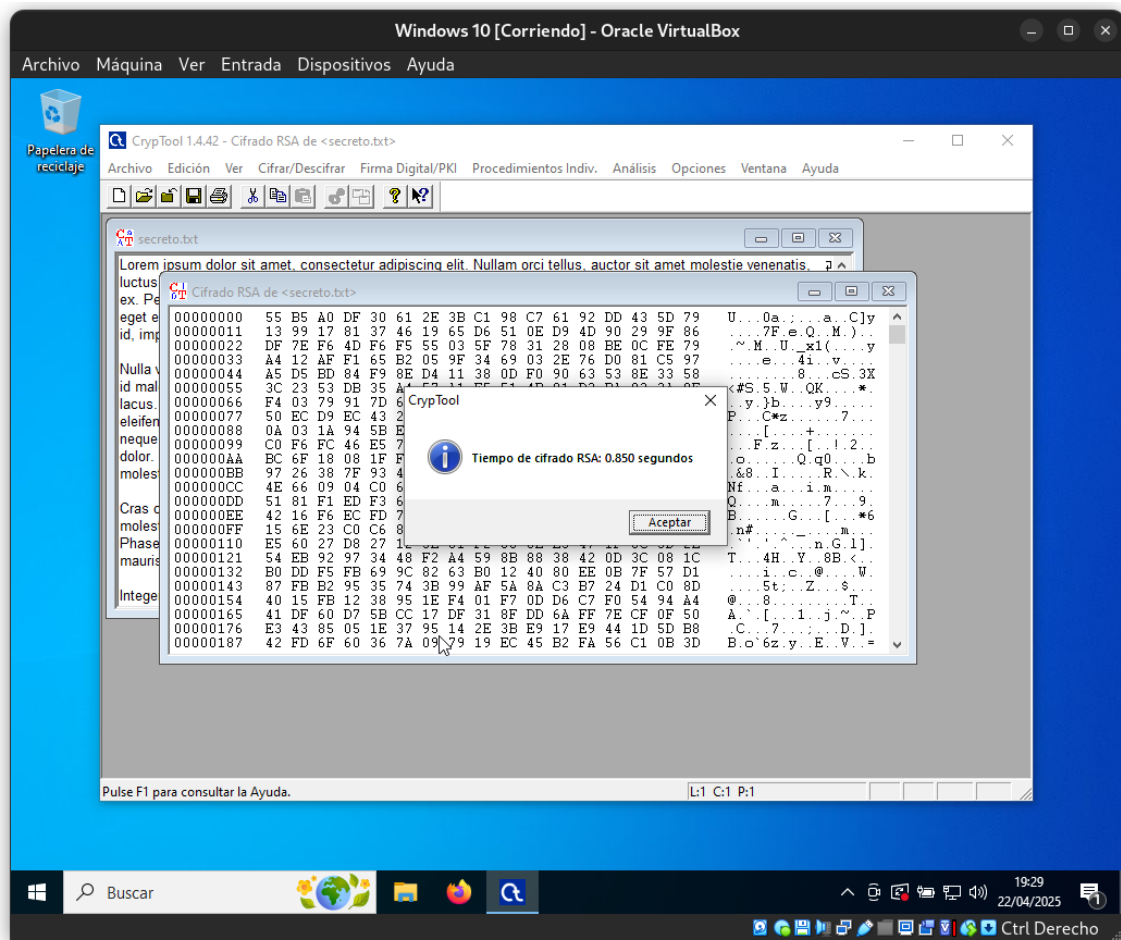


Figura 9: Generación del perfil del par de claves RSA

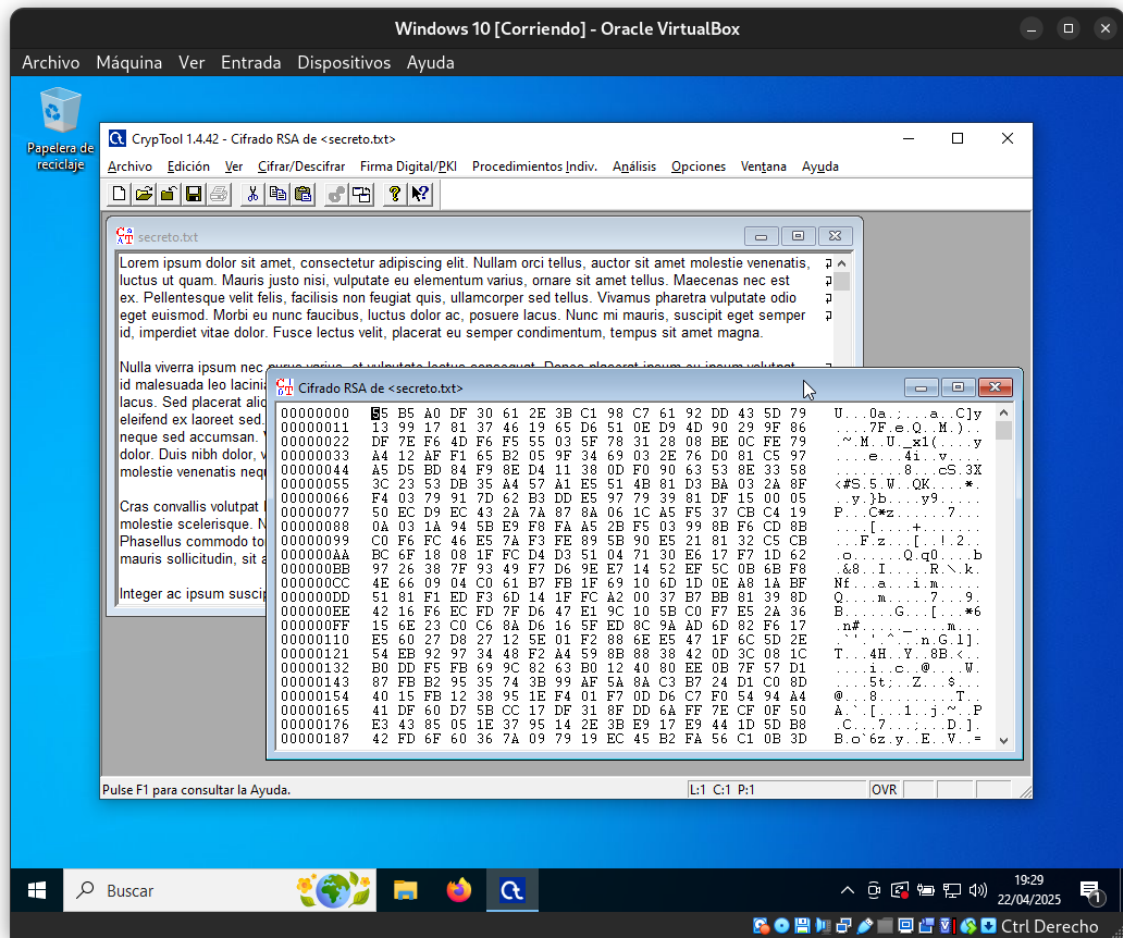


Figura 10: Generación del perfil del par de claves RSA

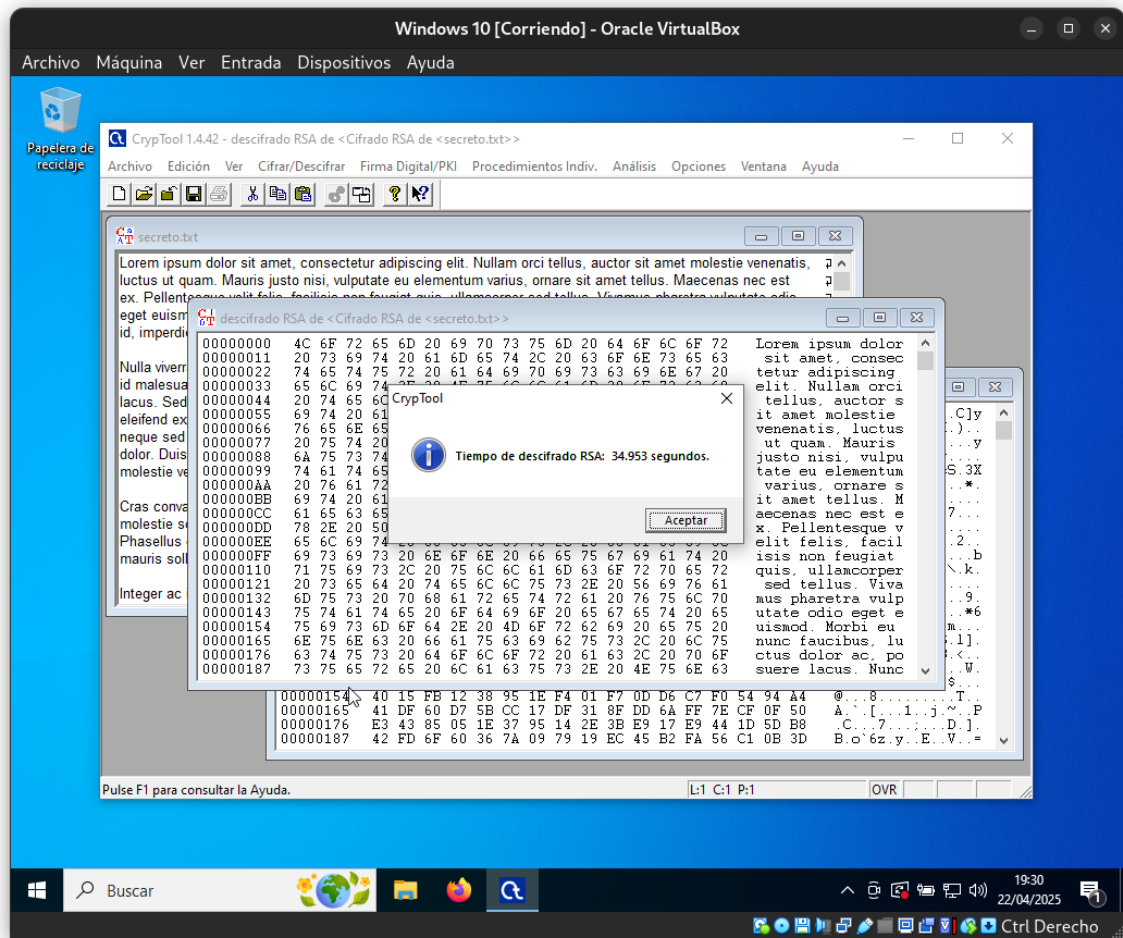
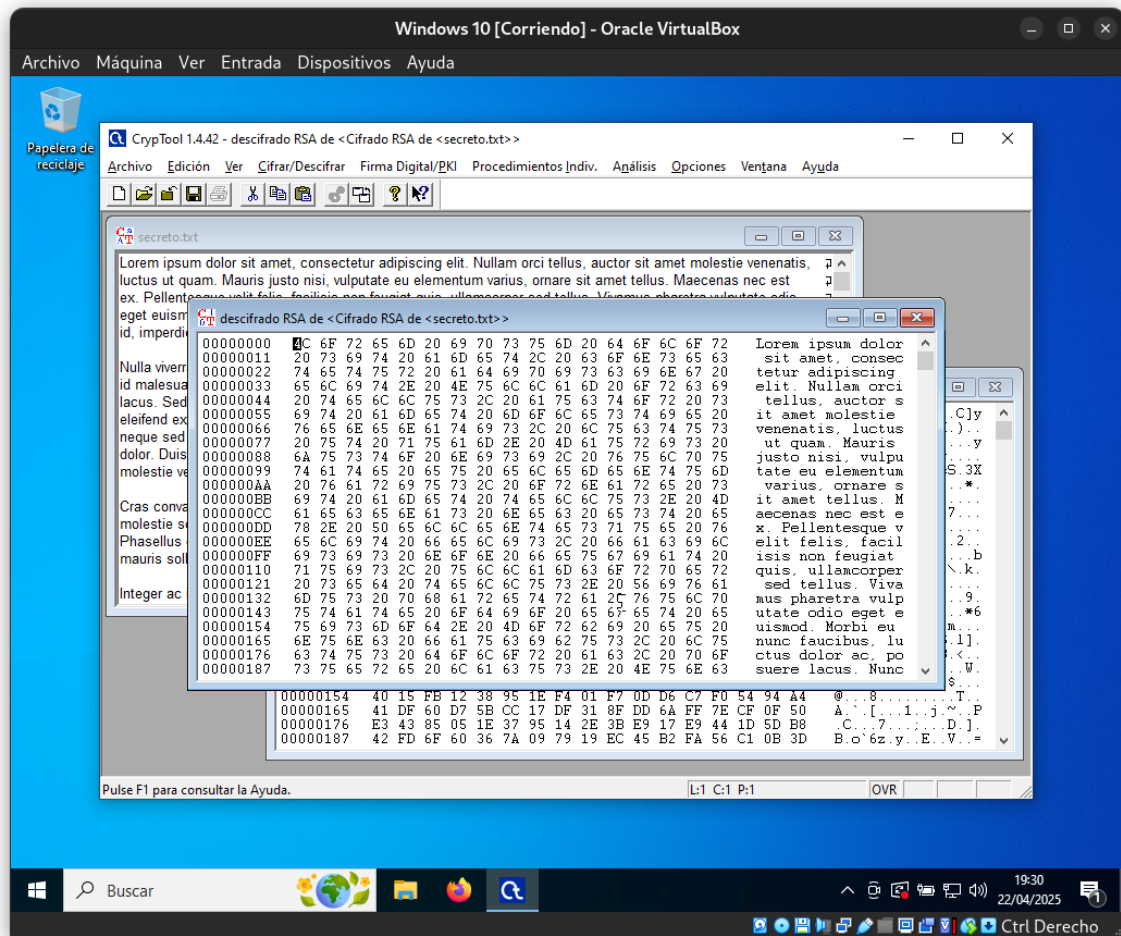


Figura 11: Generación del perfil del par de claves RSA



**Figura 12:** Generación del perfil del par de claves RSA

## 1.2. Ejercicio 2

### 1.3. Ejercicio 3

## 2. Certificados digitales

### 2.1. Ejercicio 4

### 2.1.1. Certificados web

Los sitios web seleccionados fueron:

- [coruna.gal](http://coruna.gal)
- [delthia.com](http://delthia.com)
- [nap.transportes.gob.es](http://nap.transportes.gob.es)
- [udc.es](http://udc.es)
- [wikipedia.org](http://wikipedia.org)

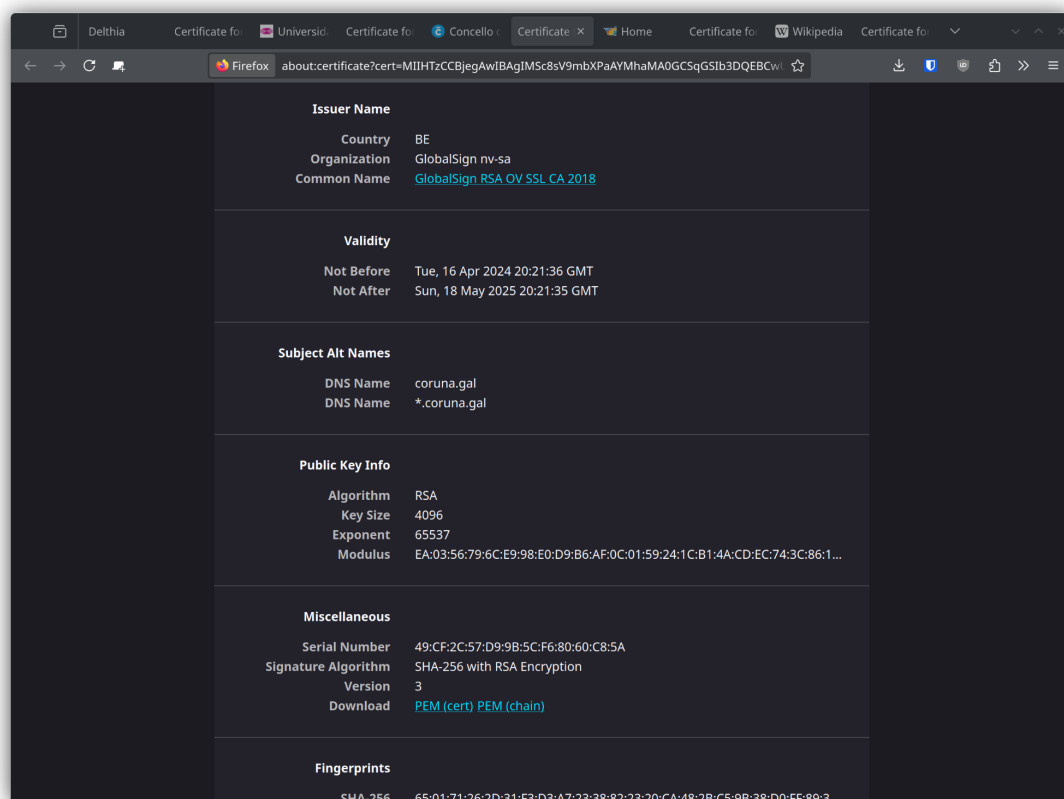


Figura 13: Certificado de coruna.gal

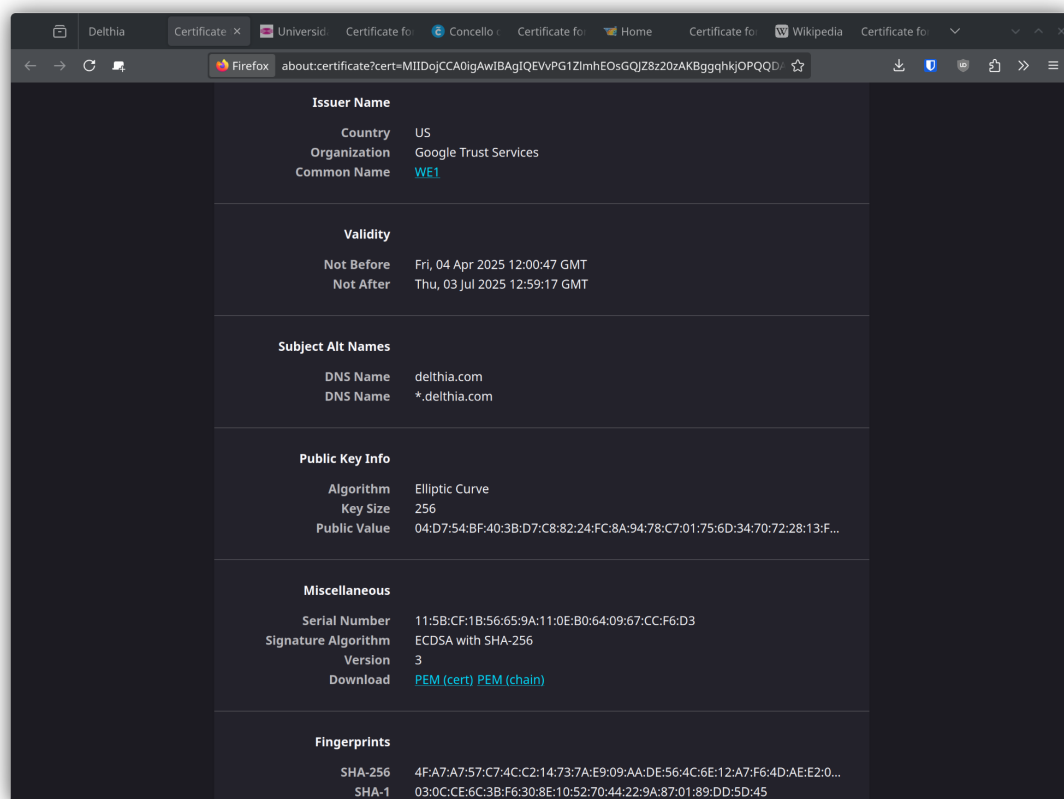
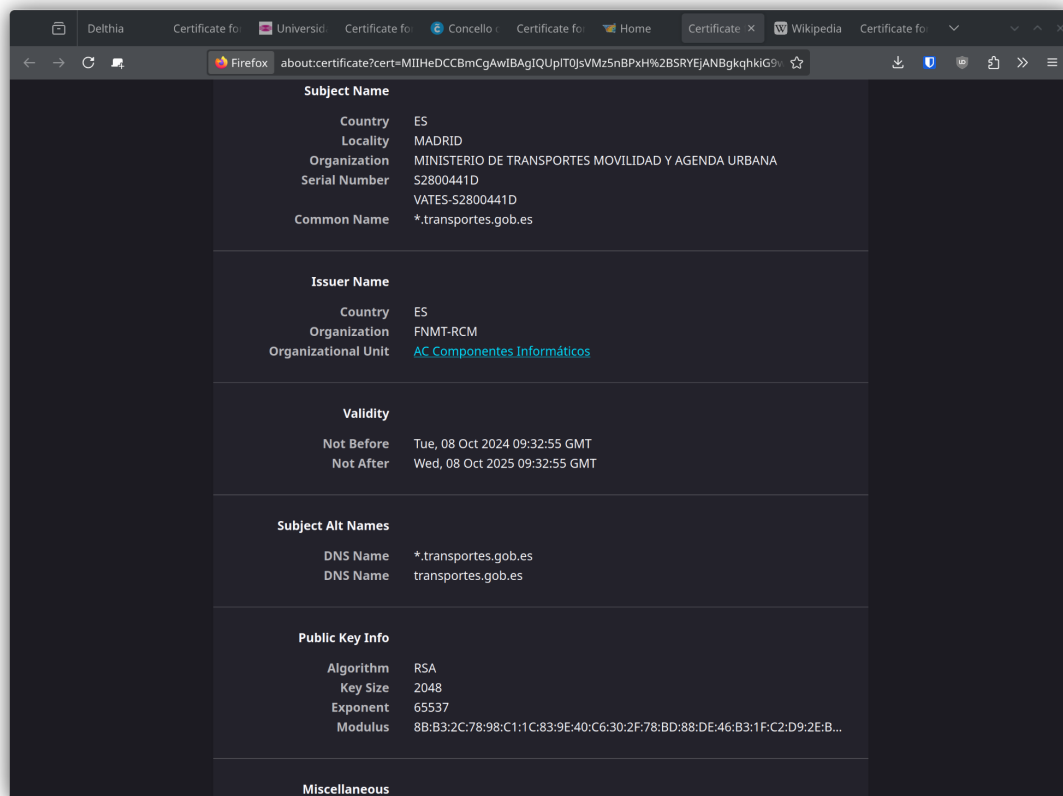


Figura 14: Certificado de delthia.com



Figura 15: Certificado de `nap.transportes.gob.es`

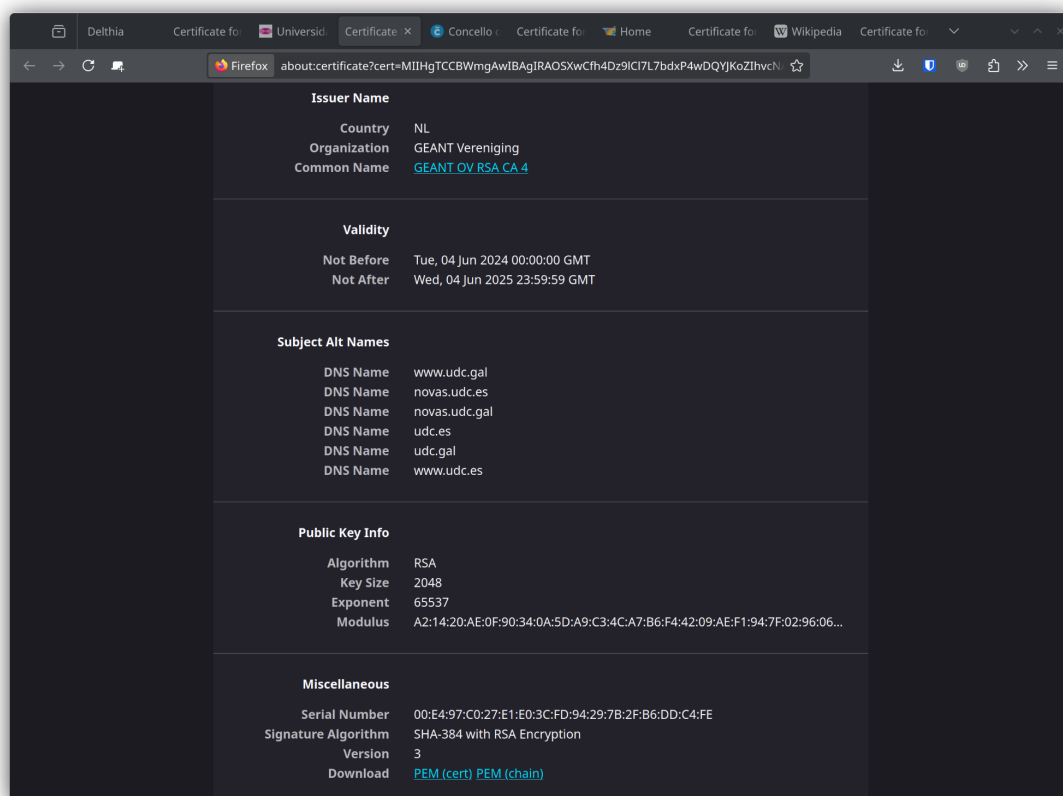


Figura 16: Certificado de udc.es

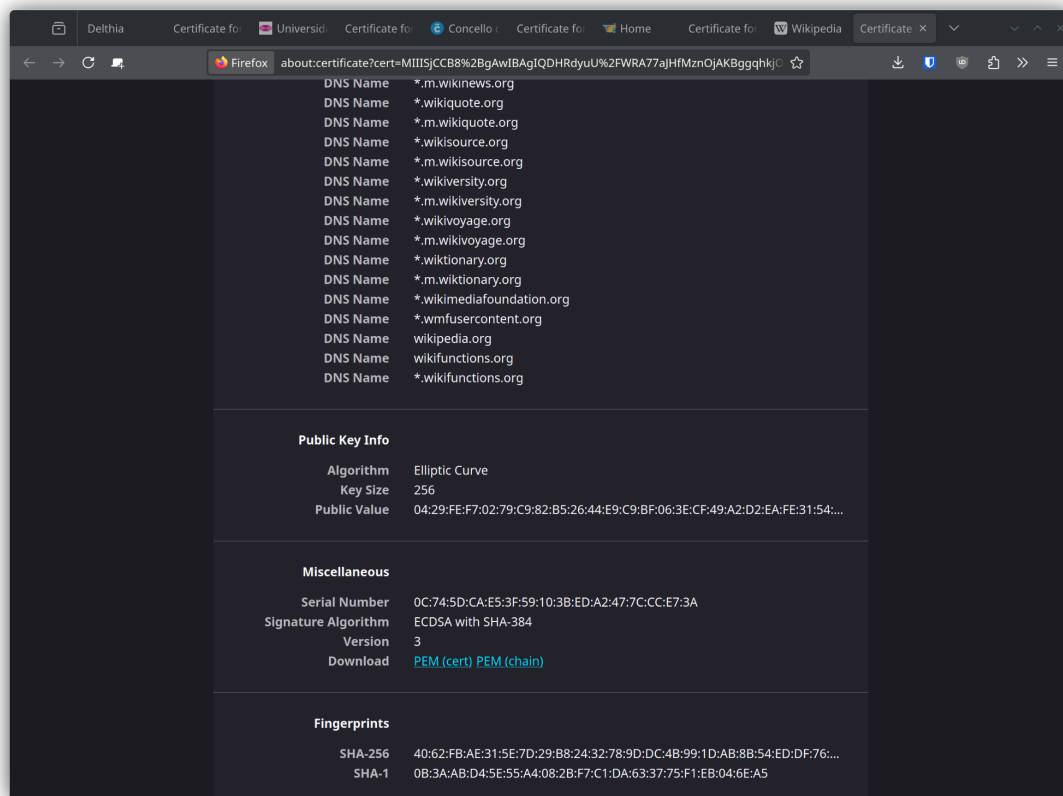


Figura 17: Certificado de wikipedia.org

### 2.1.2. Análisis con openssl

A continuación se analizan los certificados de `coruna.gal` y `udc.es`, para lo que utiliza OpenSSL para descargar el certificado y ver los detalles con el comando

```
openssl s_client -showcerts -servername coruna.gal -connect
↵ coruna.gal:443
```

Es importante indicar el nombre de dominio del que se desea obtener el certificado, ya que desde un mismo servidor con la misma dirección se pueden servir varios sitios web, dependiendo de la cabecera `host`.

## 2.2. Ejercicio 5

## 3. PGP y S/MIME

### 3.1. Ejercicio 6

### 3.2. Ejercicio 7

### 3.3. Ejercicio 8

### 3.4. Ejercicio 9

### 3.5. Ejercicio 10

### 3.6. Ejercicio 11

## 4. Privacidad

### 4.1. Ejercicio 12

### 4.2. Ejercicio 13

### 4.3. Ejercicio 14

### 4.4. Ejercicio 15

### 4.5. Ejercicio 16

### 4.6. Ejercicio 17