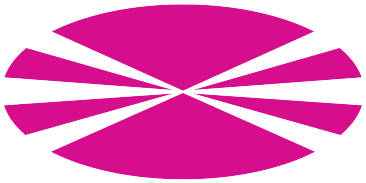

UNIVERSIDADE DA CORUÑA
Facultade de Informática

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

1. Criptografía moderna

1.1. Ejercicio 1

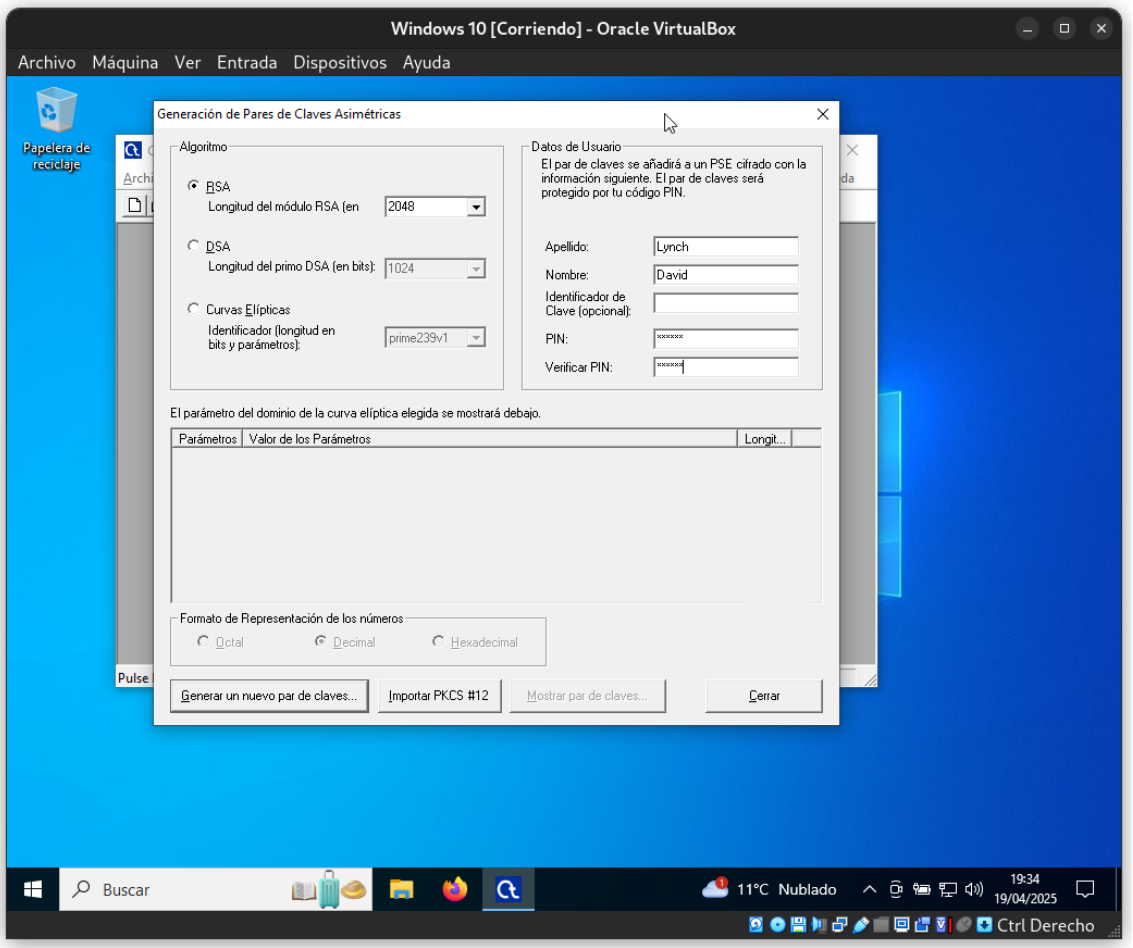

Figura 1: Generación del perfil del par de claves RSA

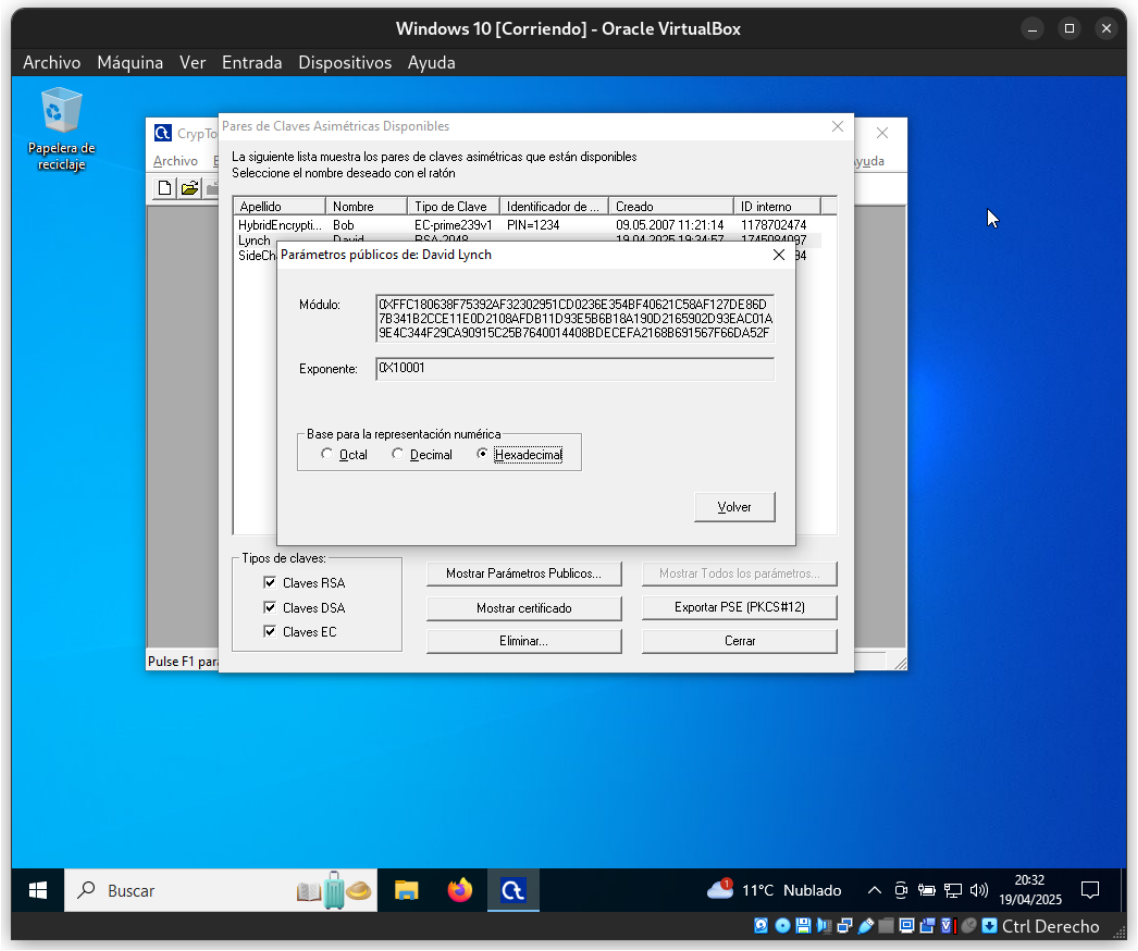

Figura 2: Parámetros públicos de la clave (n, e)

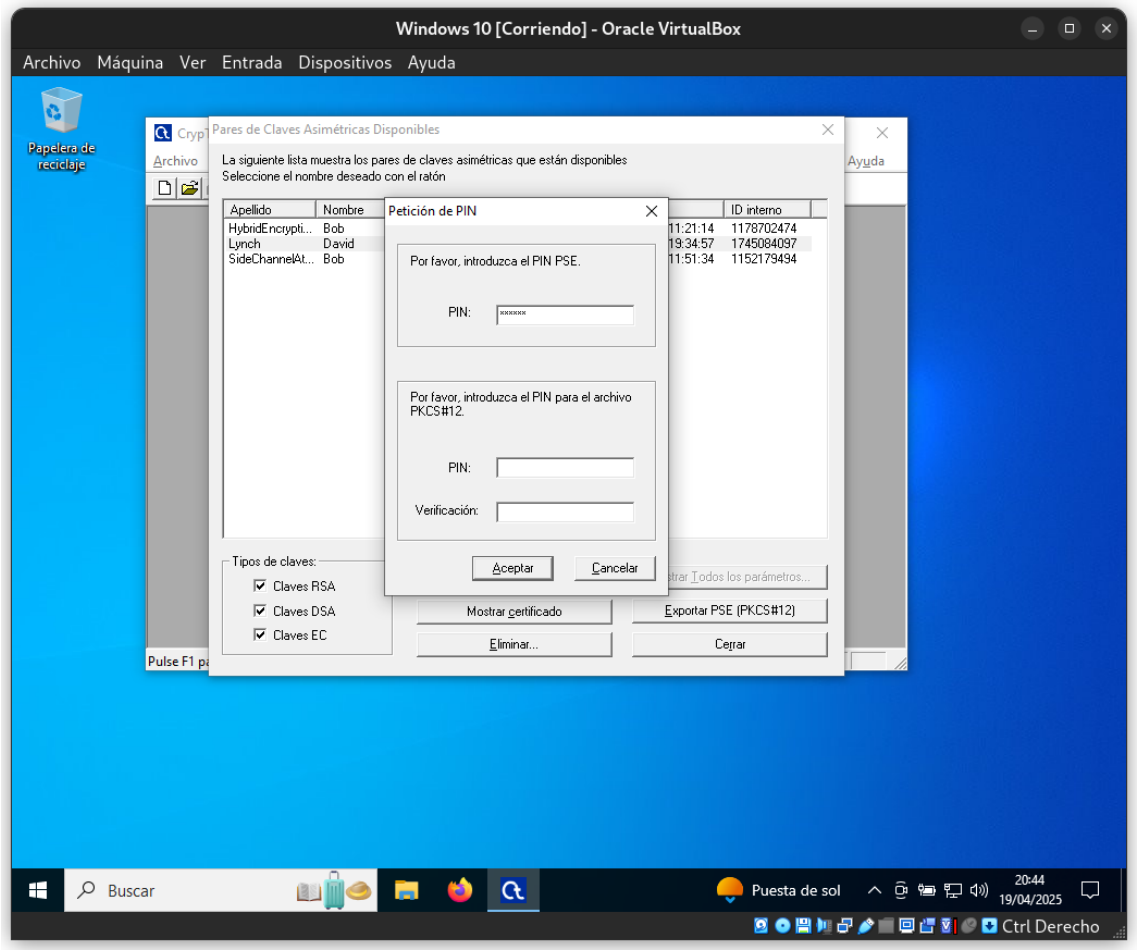

Figura 3: Pantalla del PIN de usuario

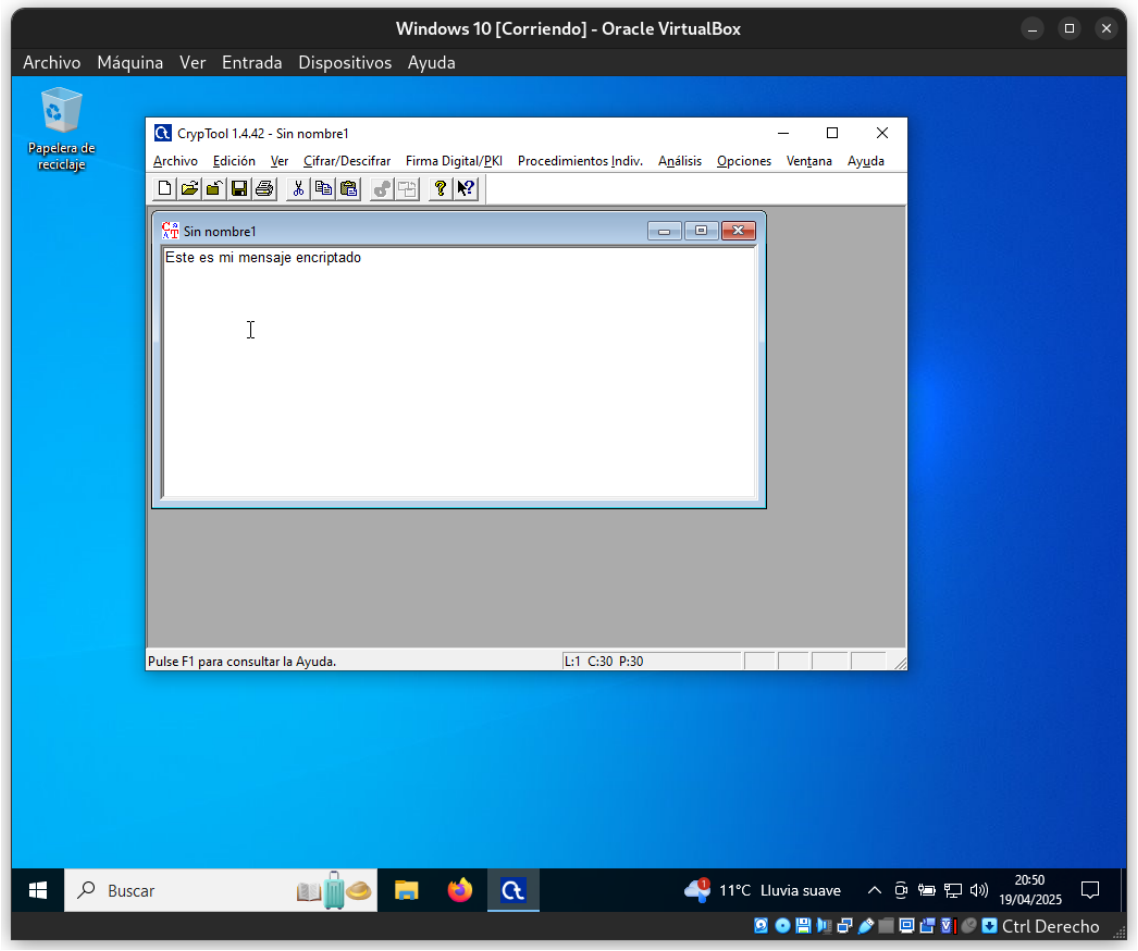

Figura 4: Texto de ejemplo para encriptar

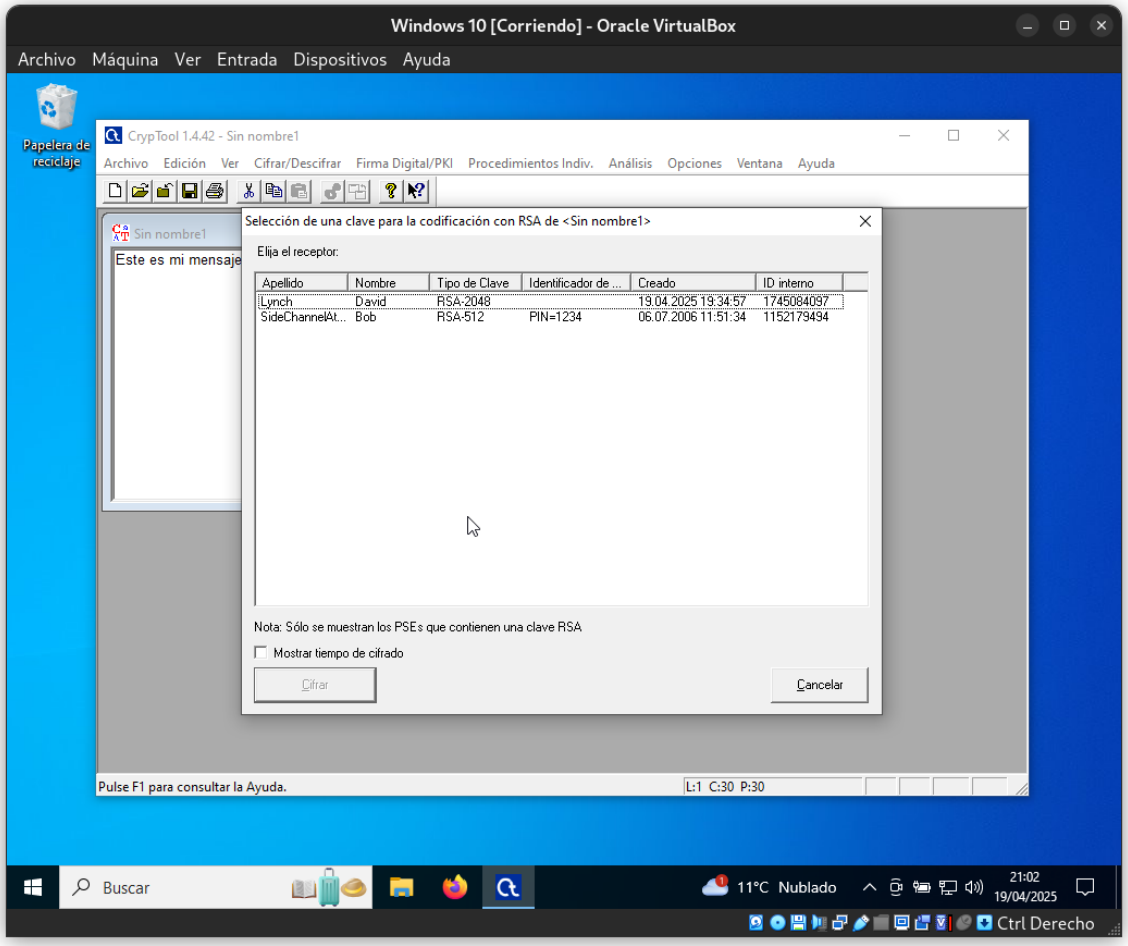

Figura 5: Generación del perfil del par de claves RSA

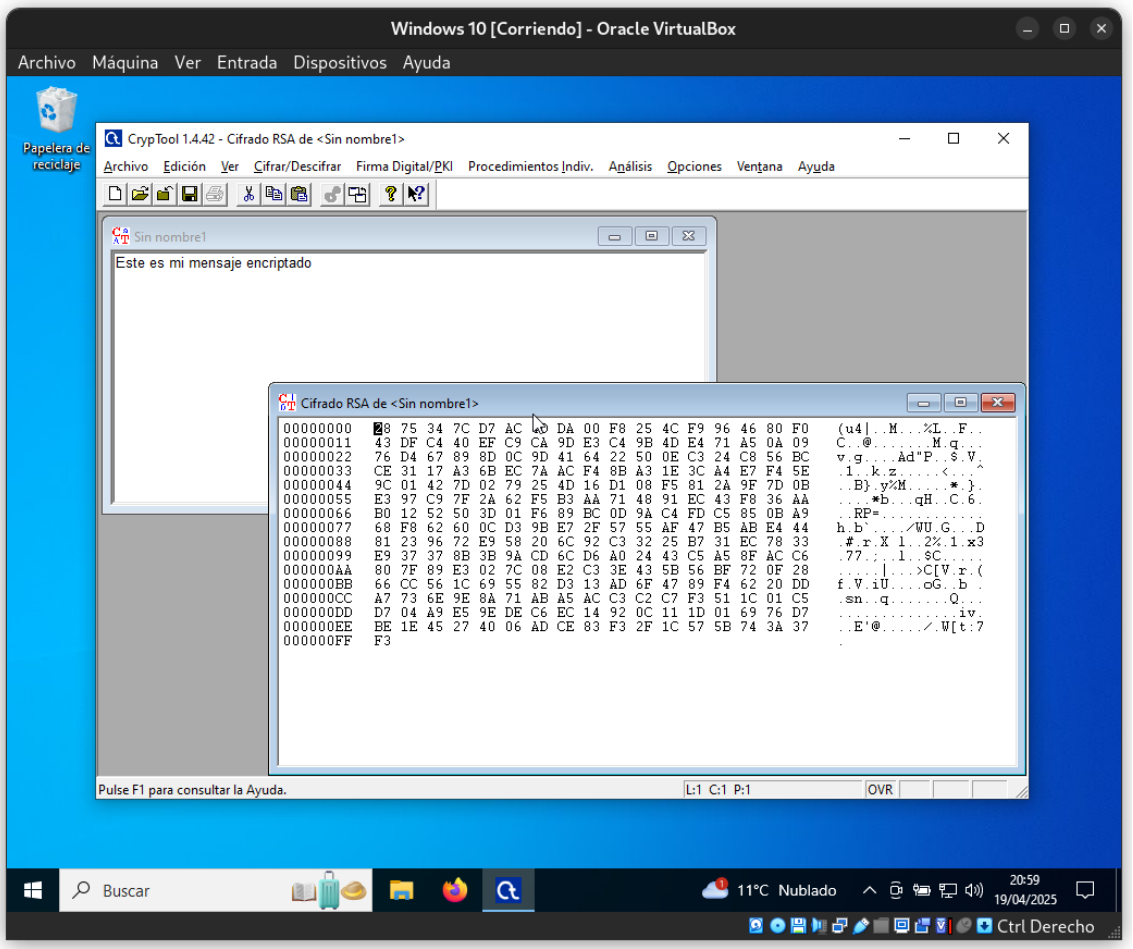

Figura 6: Generación del perfil del par de claves RSA

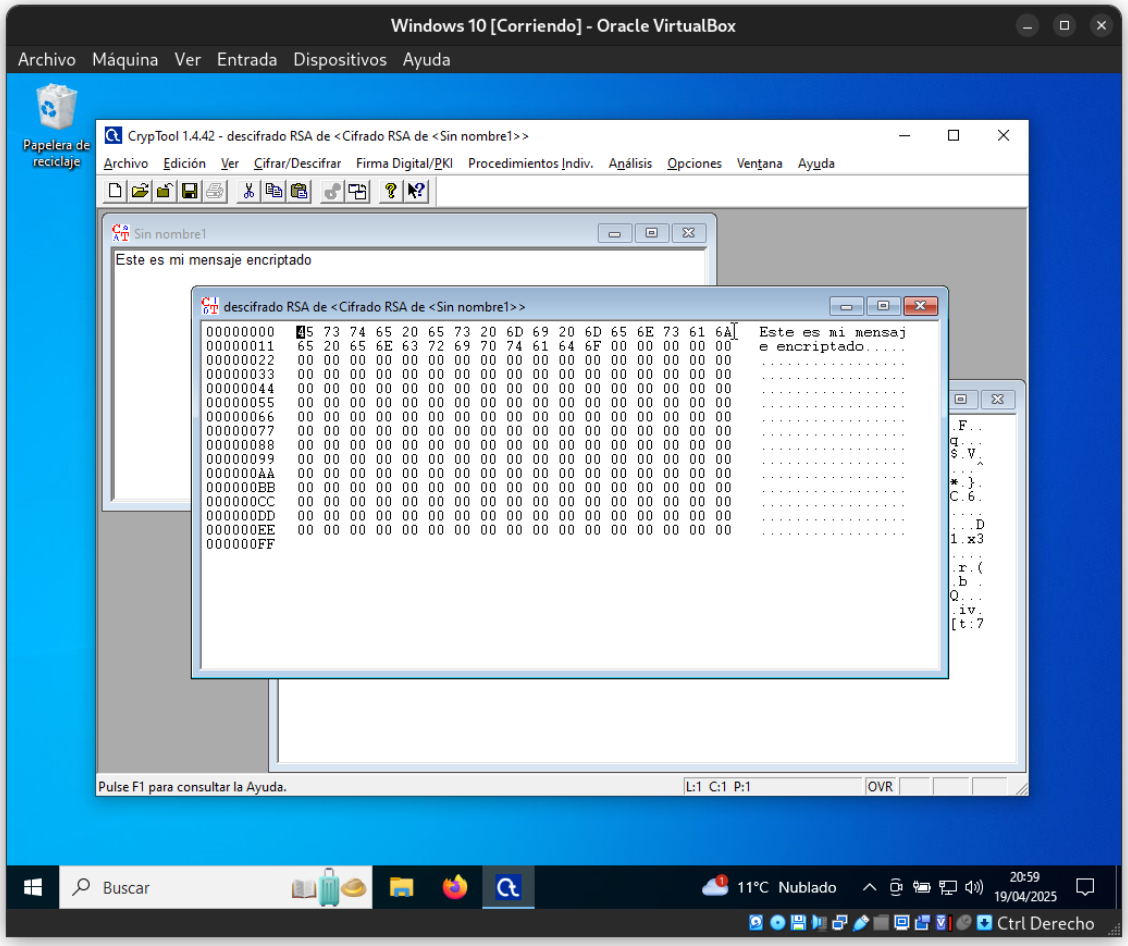

Figura 7: Generación del perfil del par de claves RSA

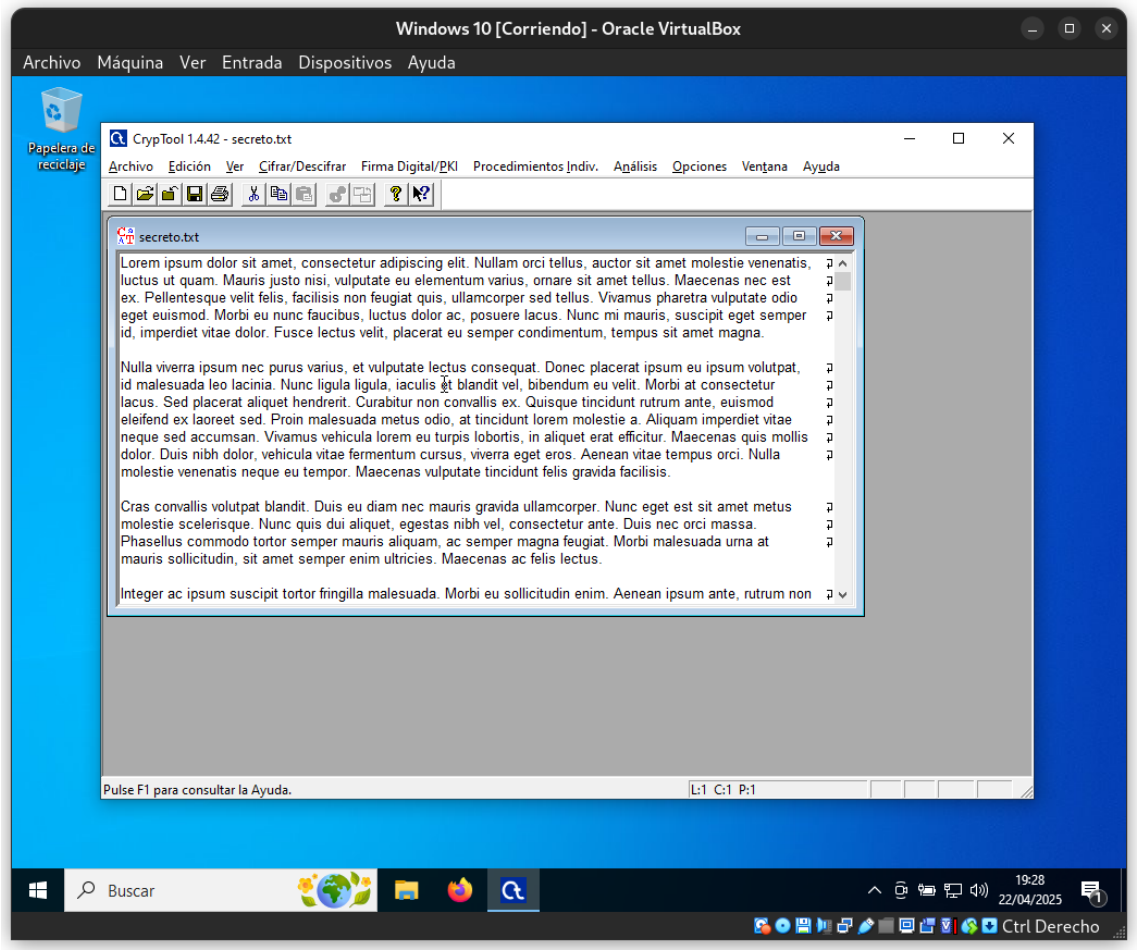

Figura 8: Generación del perfil del par de claves RSA

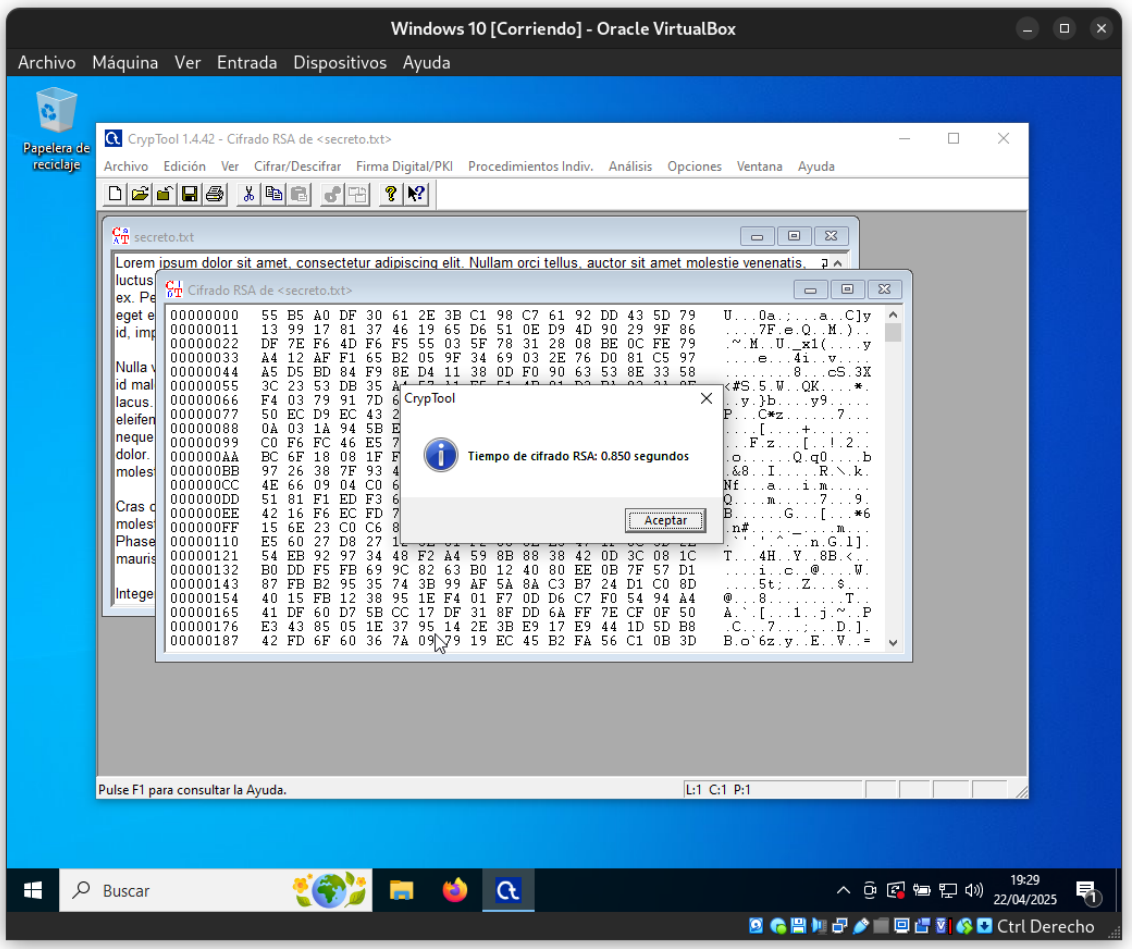

Figura 9: Generación del perfil del par de claves RSA

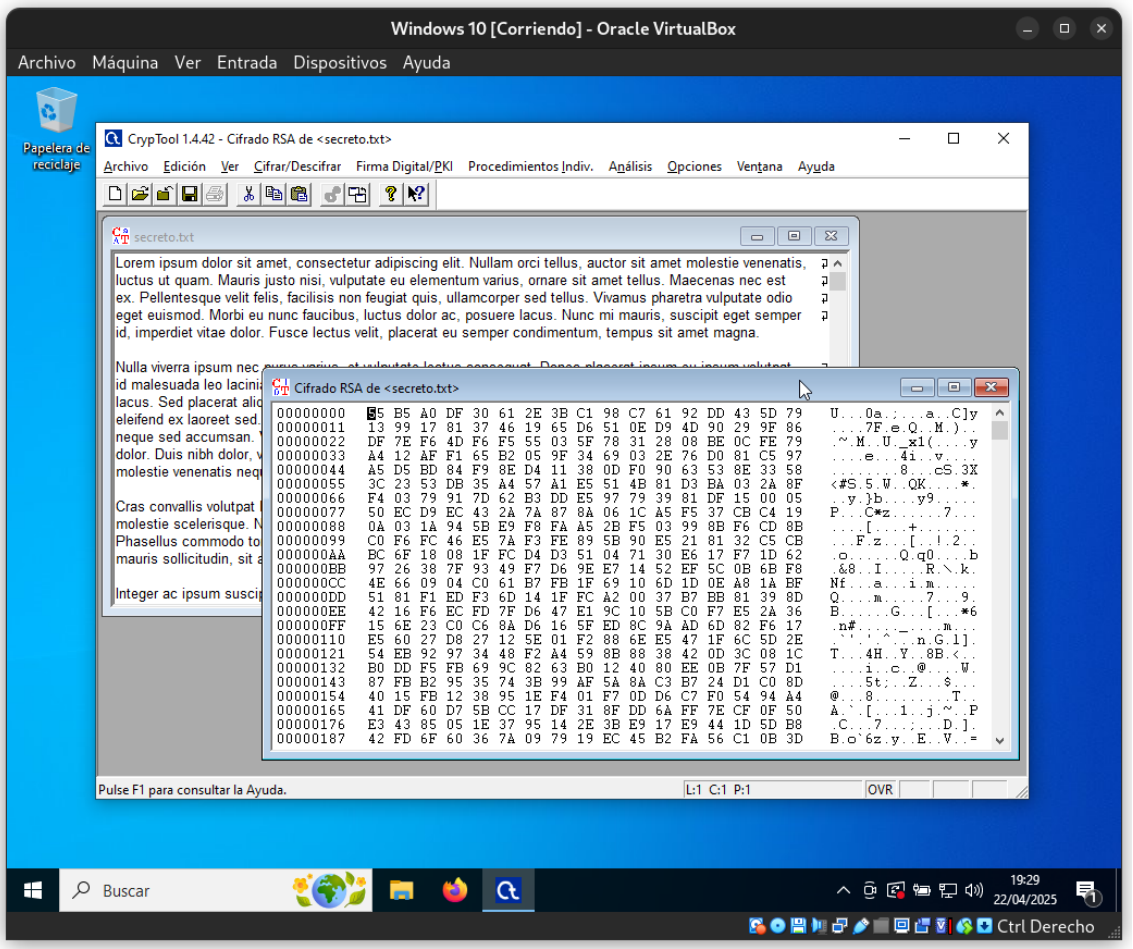

Figura 10: Generación del perfil del par de claves RSA

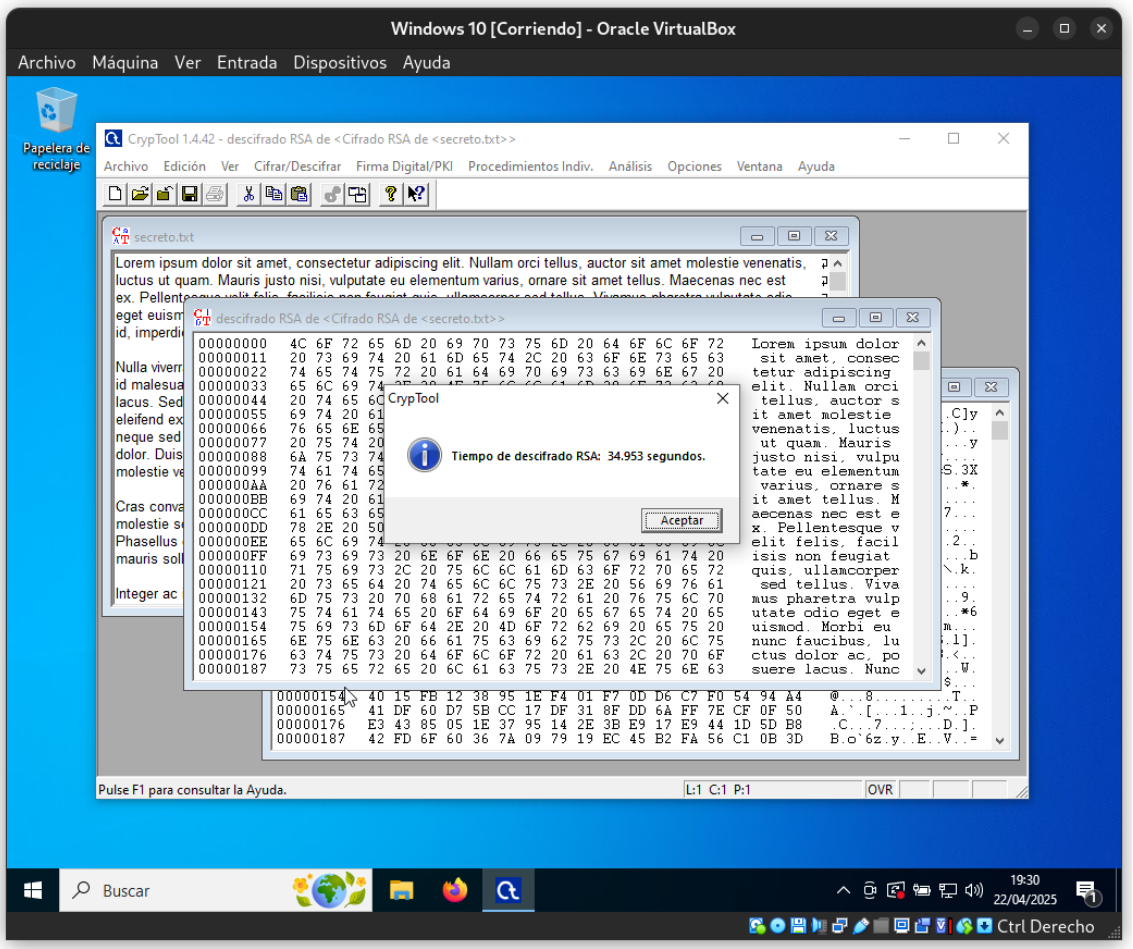

Figura 11: Generación del perfil del par de claves RSA

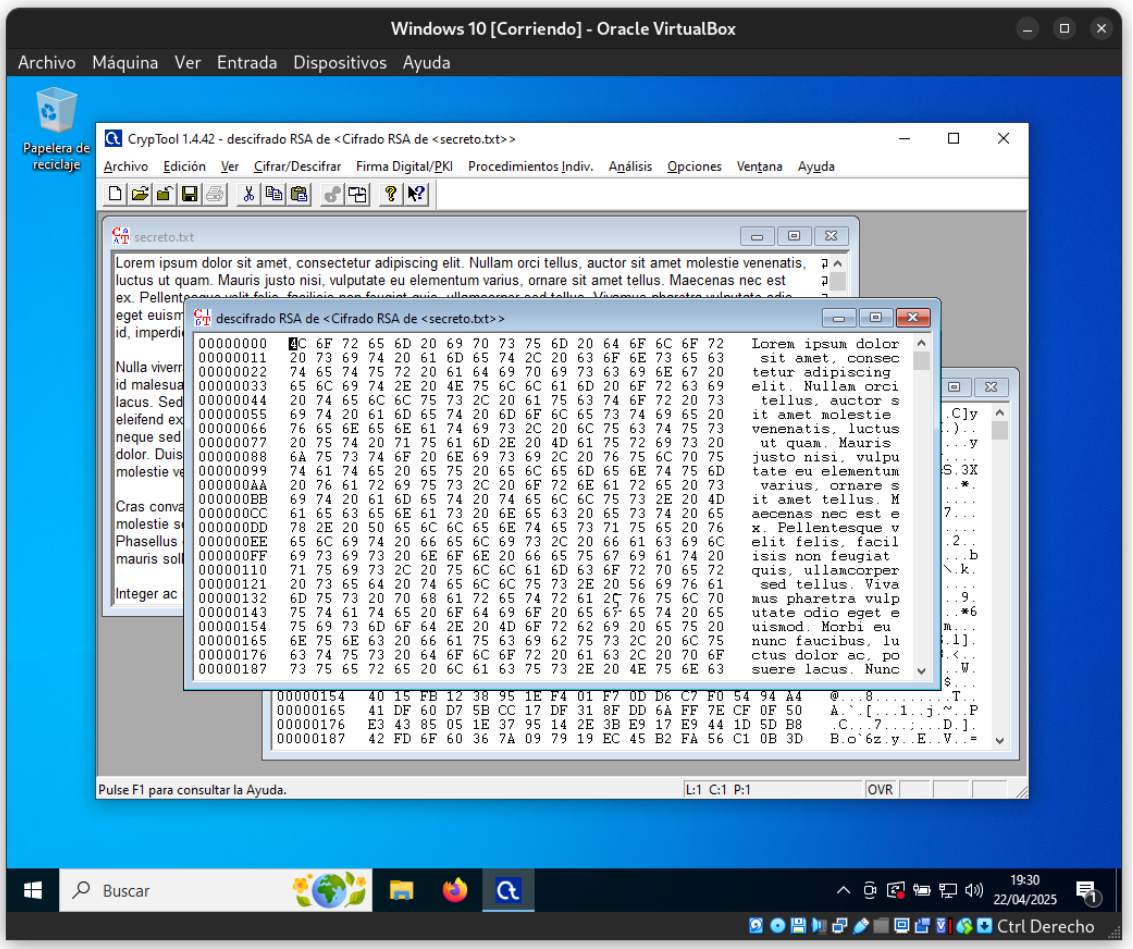

Figura 12: Generación del perfil del par de claves RSA

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
- delthia.com
- nap.transportes.gob.es
- udc.es
- wikipedia.org

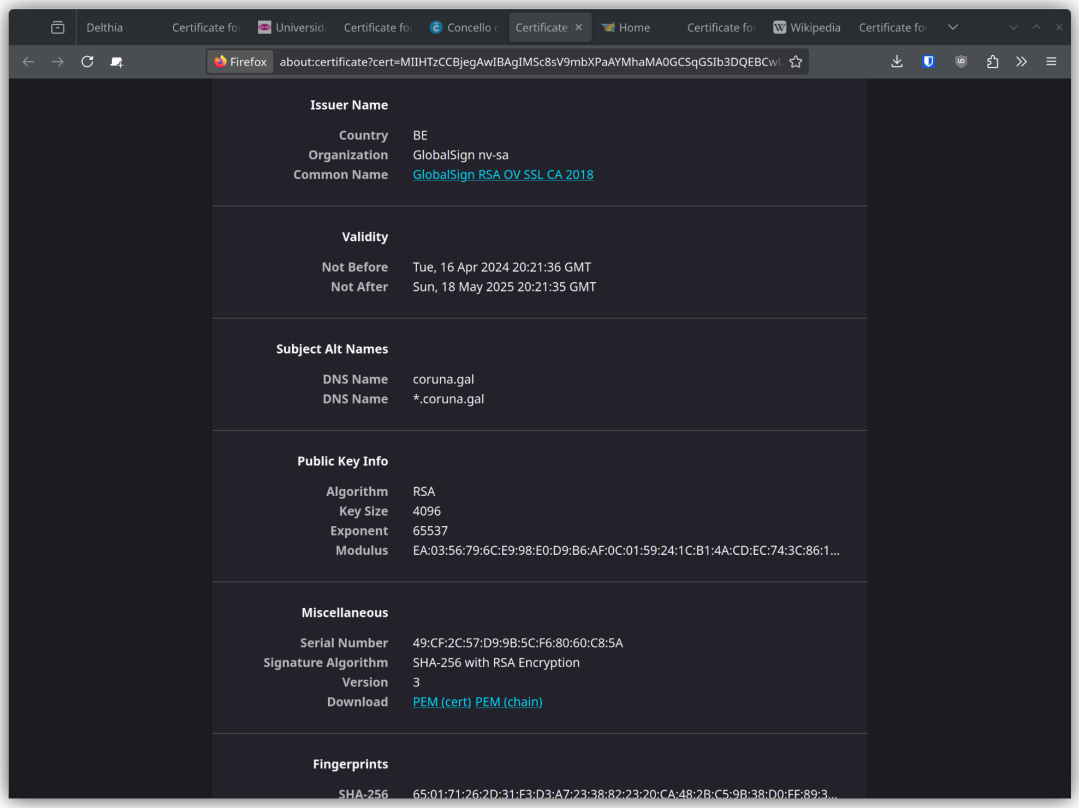

Figura 13: Certificado de `coruna.gal`

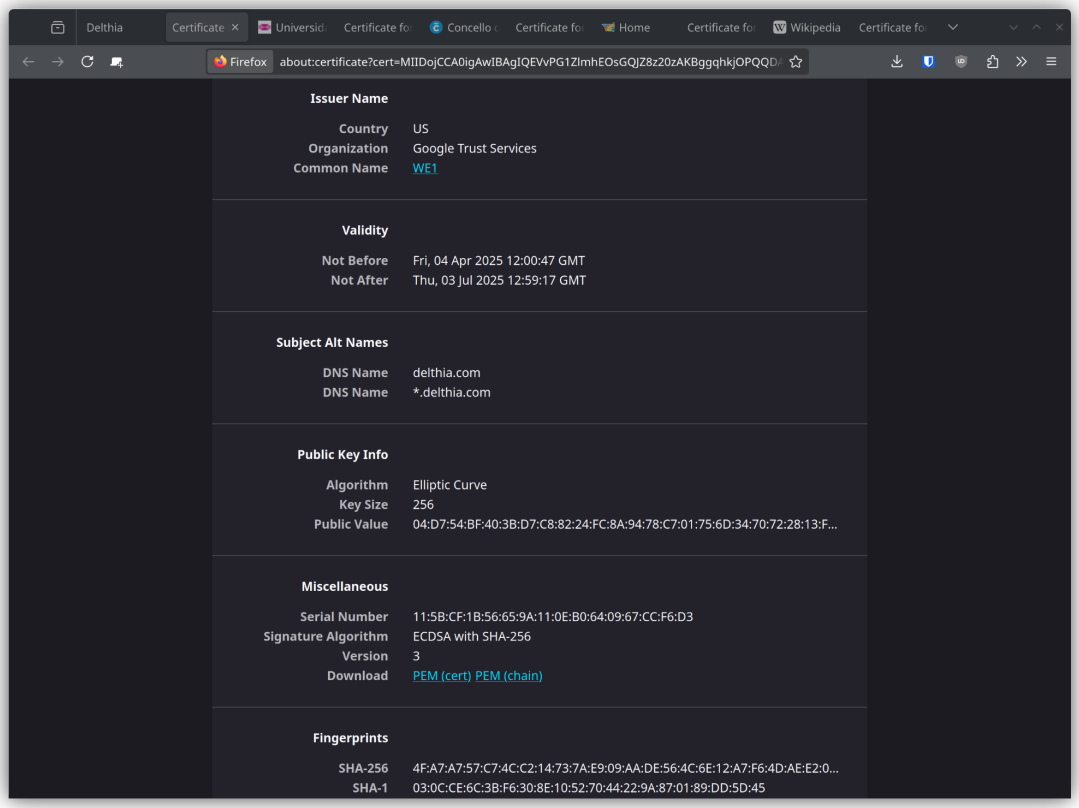

Figura 14: Certificado de `delthia.com`

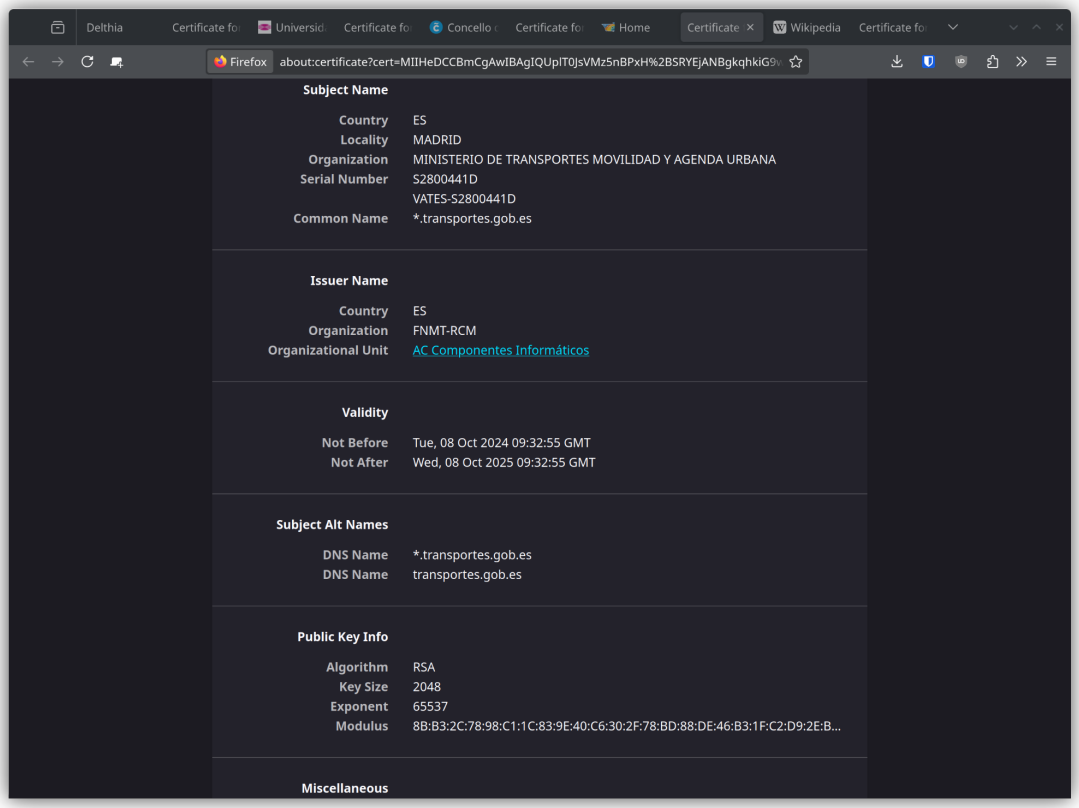

Figura 15: Certificado de `nap.transportes.gob.es`

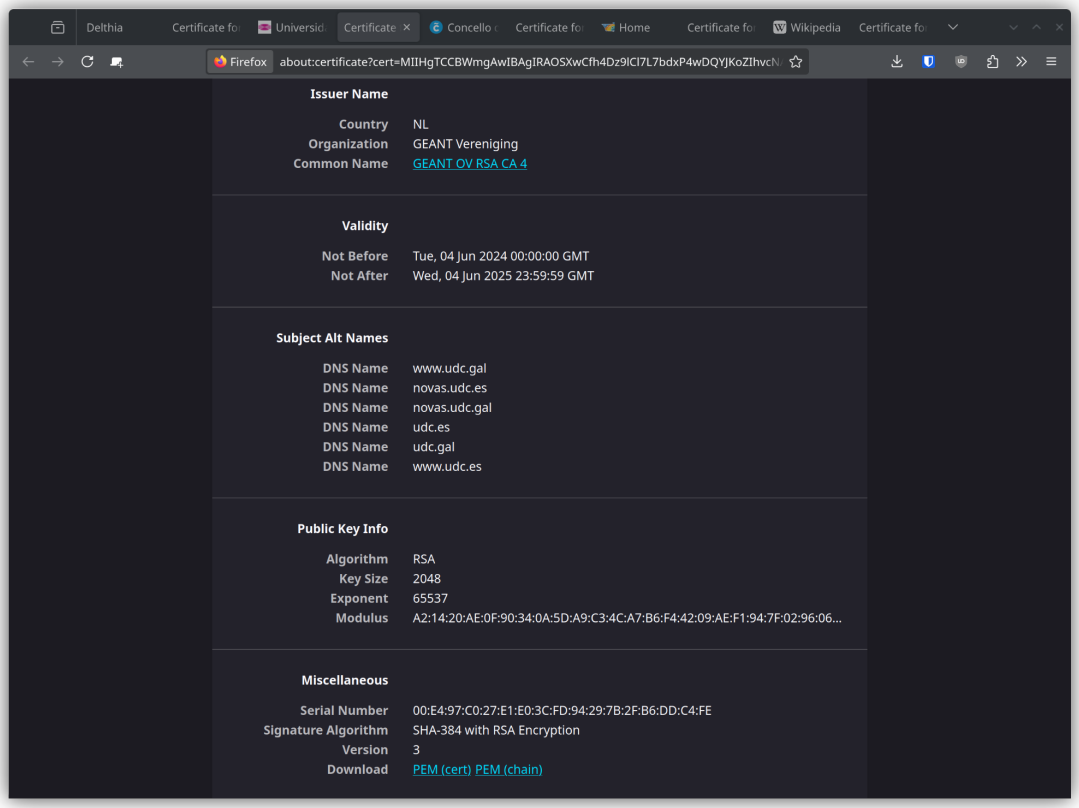

Figura 16: Certificado de `udc.es`

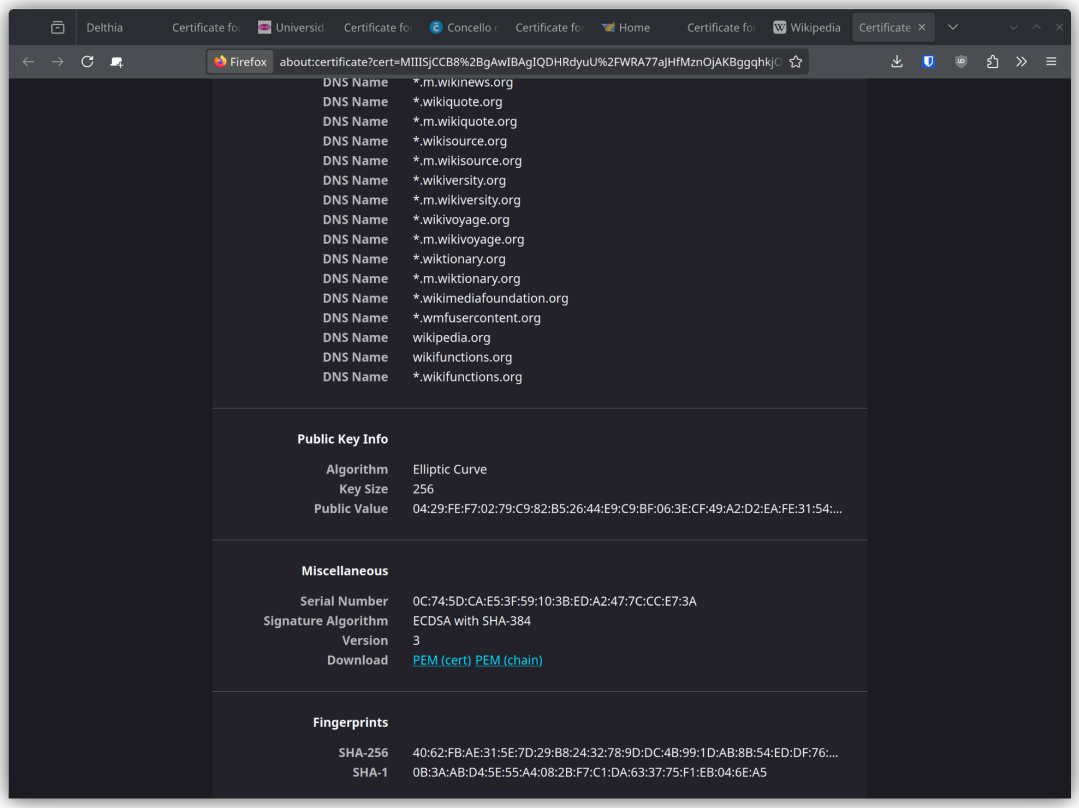

Figura 17: Certificado de `wikipedia.org`

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`.