

UNIVERSIDADE DA CORUÑA

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`

Facultade de Informática

22 de abril de 2025

1. Criptografía moderna

1.1. Ejercicio 1

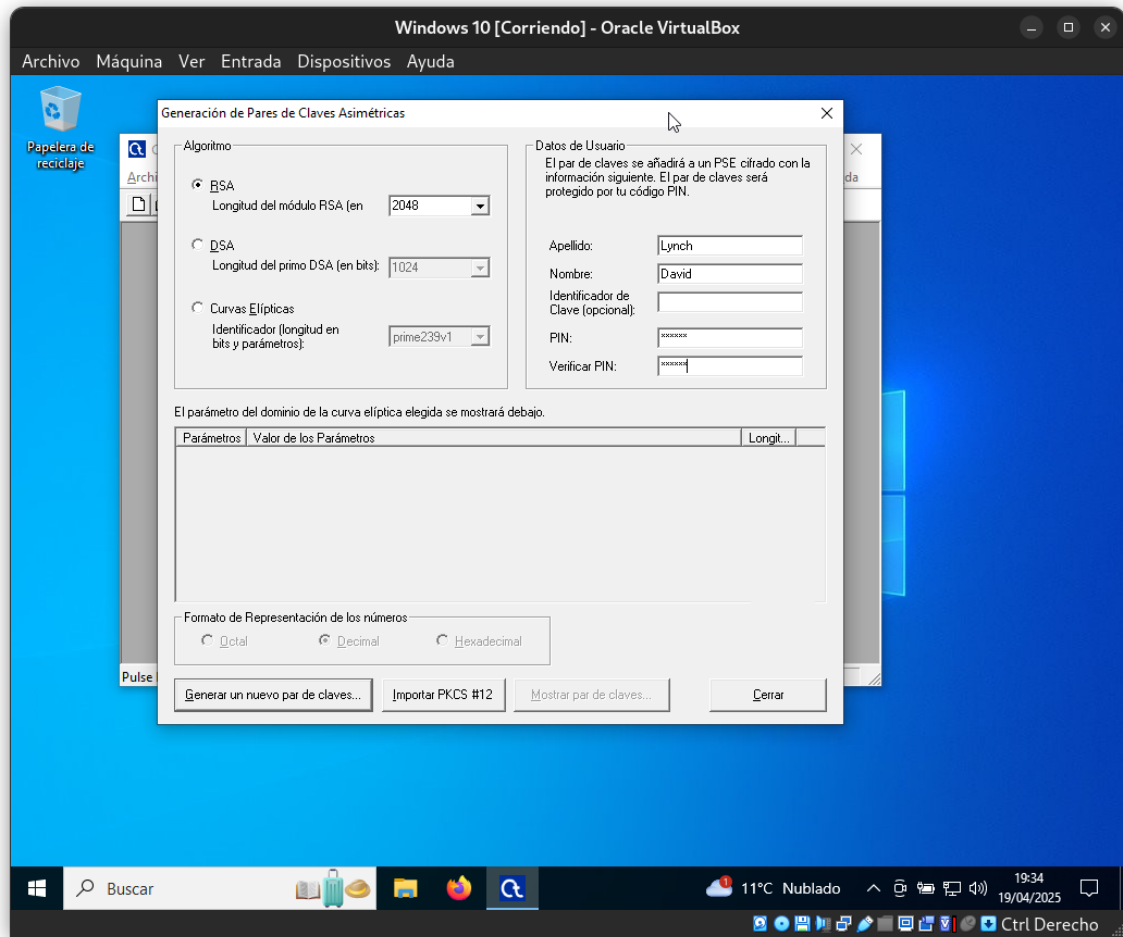


Figura 1: Generación del perfil del par de claves RSA

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

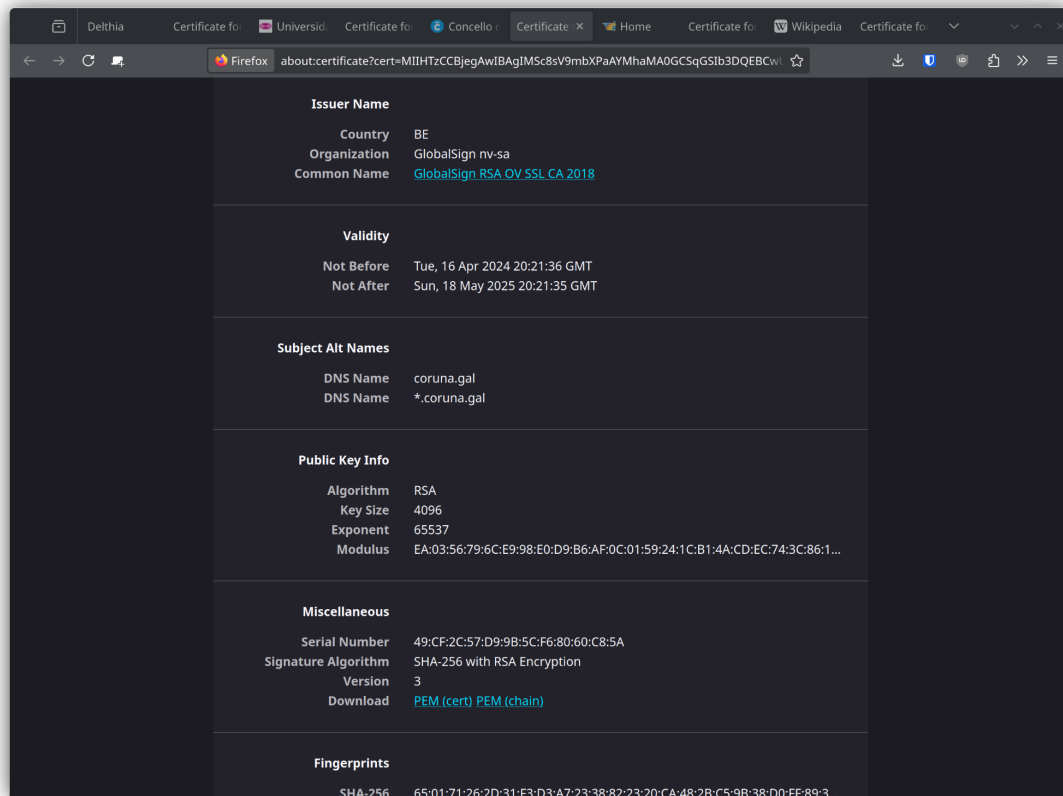


Figura 2: Certificado de coruna.gal

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
```

Es importante indicar el nombre de deominio 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`.

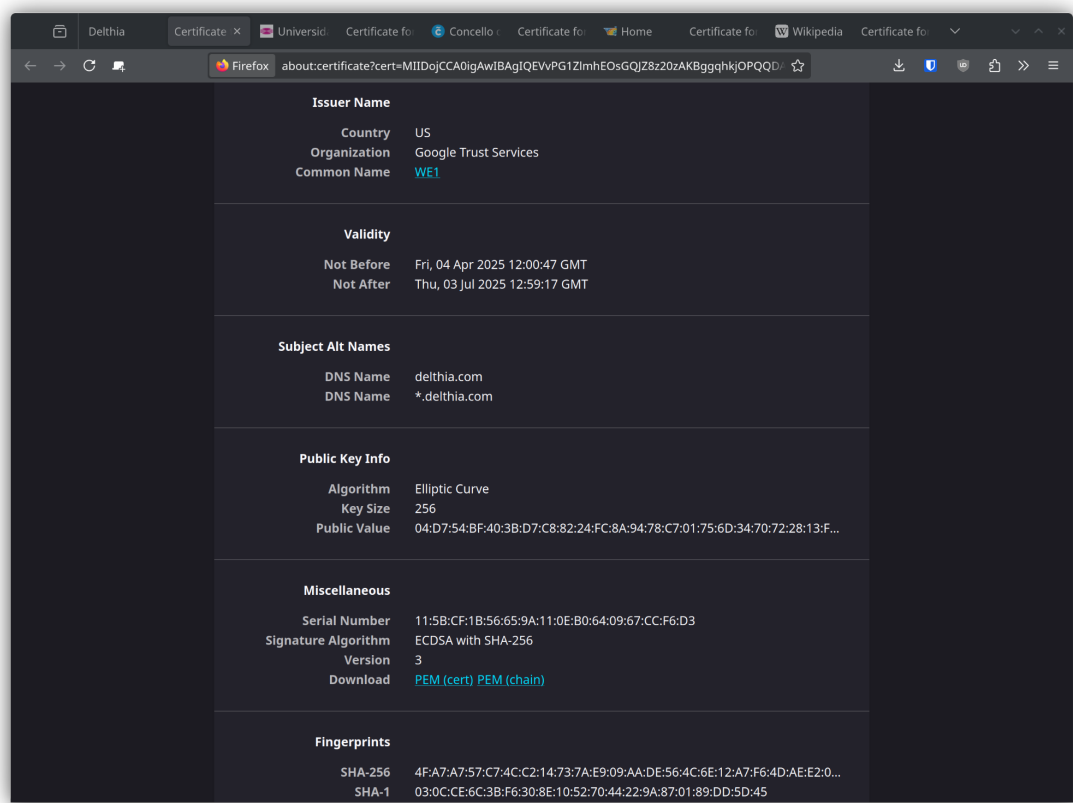
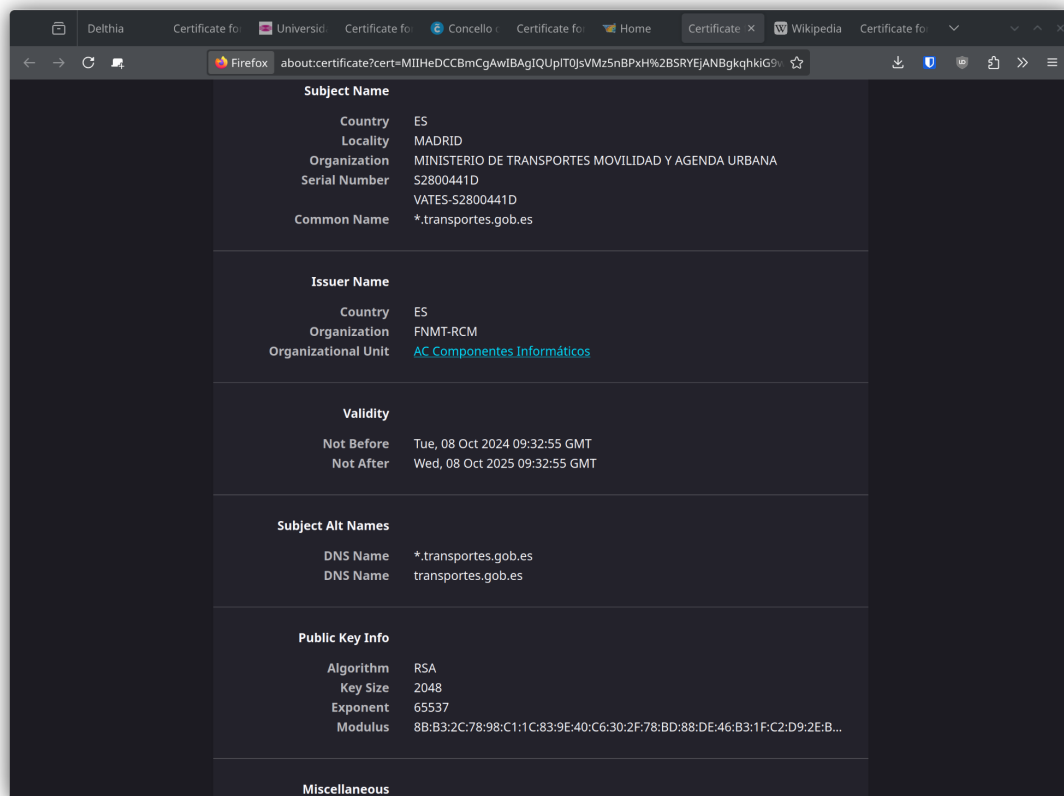


Figura 3: Certificado de delthia.com

Figura 4: Certificado de `nap.transportes.gob.es`

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

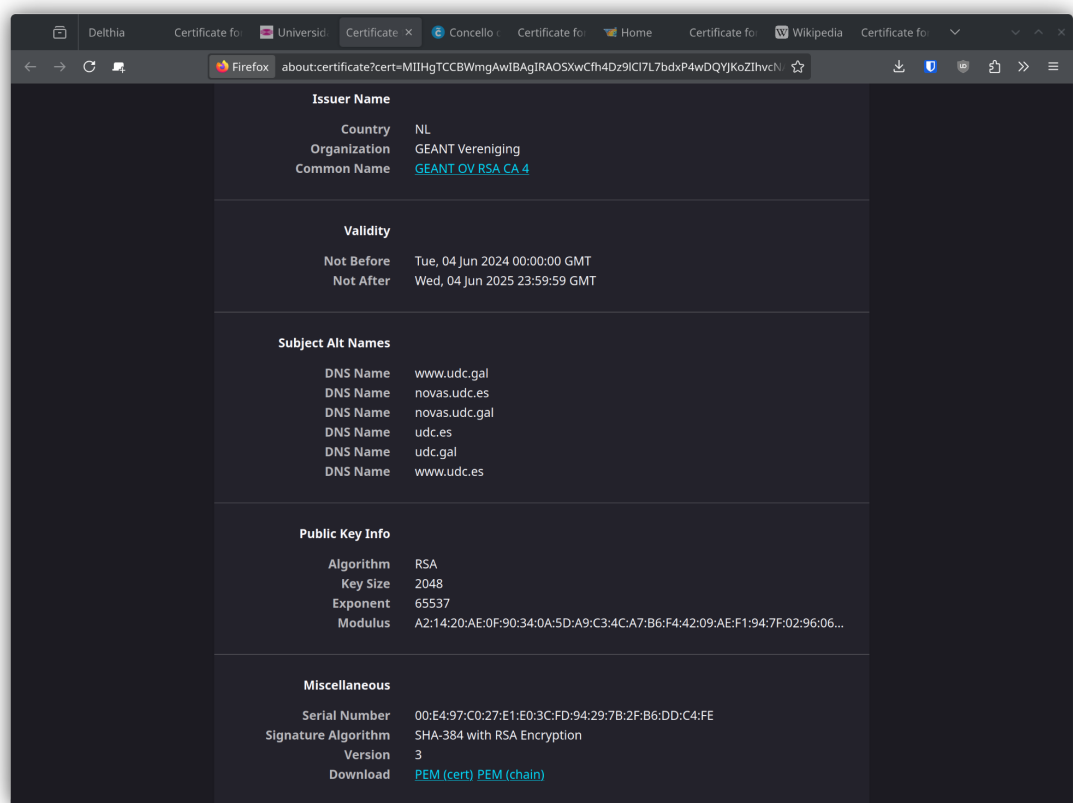


Figura 5: Certificado de udc.es

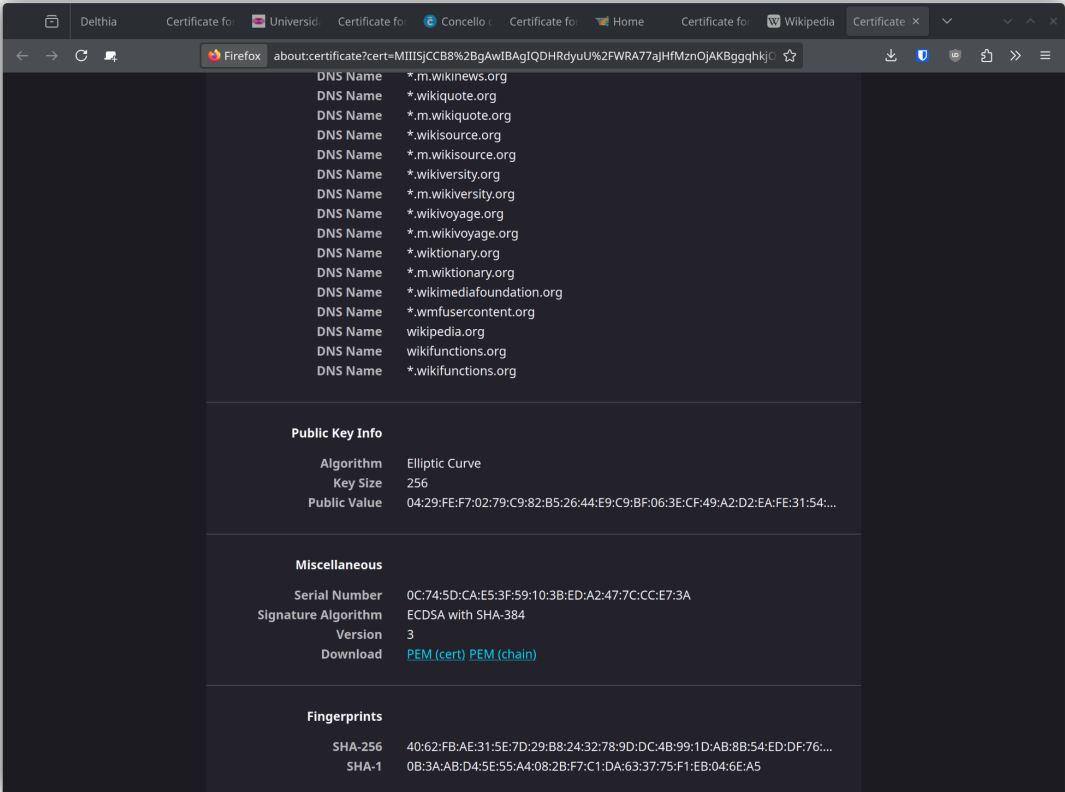


Figura 6: Certificado de wikipedia.org