Grado en Ingeniería Informática

Seguridad en Tecnologías de la Información
Curso 2017/18

Práctica Número 4

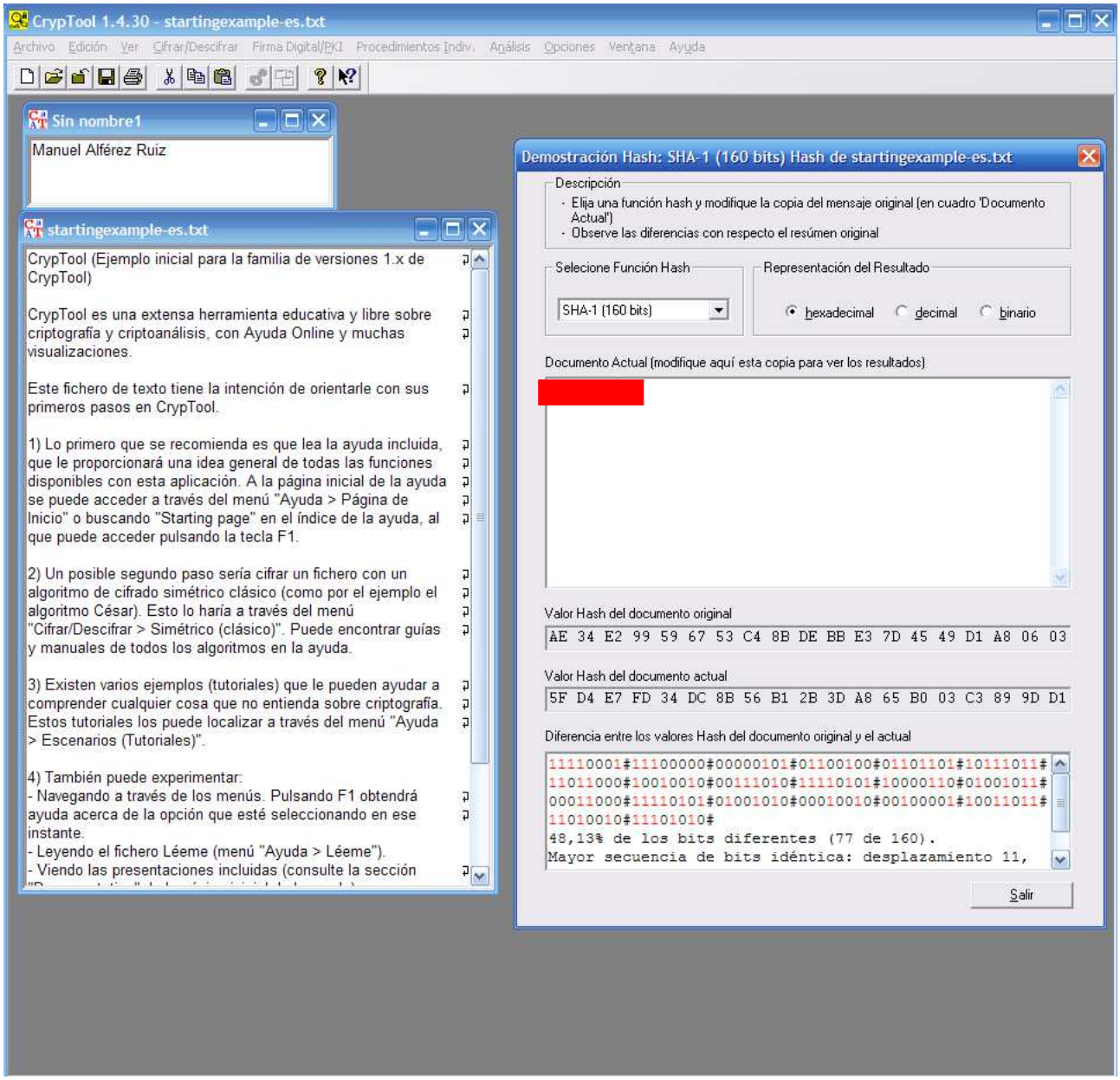
UNIVERSIDAD DE JAÉN

Autor: Manuel Alférez Ruiz

Hash

En esta primera parte procedemos a utilizar el *algoritmo SHA-1* y a introducir como texto mi número de *DNI* (sin letra), sin espacios y sin retornos de carro al final. Mi DNI es: [redacted]

Como se puede observar en la captura:



[1.png]

En la captura podemos mi documento actual, el *valor hash del documento original*, y en última instancia el *valor hash del documento actual*:

[redacted] 34 DC 8B 56 B1 2B 3D [redacted] 9D D1 91

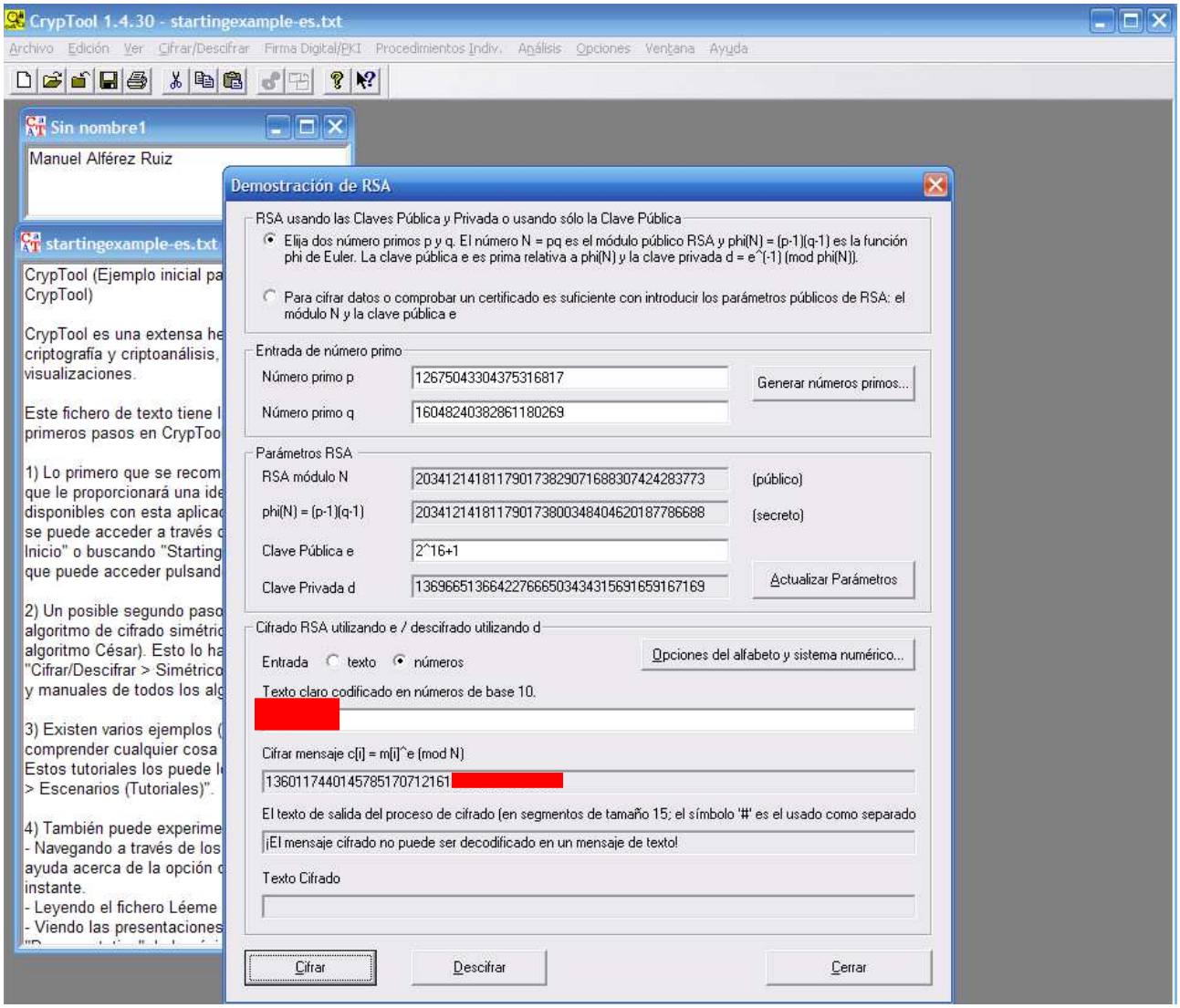
En azul tenemos los cinco primeros valores hexadecimales que nos piden.

Demostración de RSA

En esta segunda sección vamos hacer uso de como funciona el RSA y parra ello vamos a utilizar los números primos:

p= 12675043304375316817
q= 16048240382861180269

Como clave pública nos pide la configuración *e=2^16+1*



[2.png]

Como se puede observar en la captura, hemos cifrado mi DNI y justo debajo nos aparece nuestro mensaje ya cifrado:

13601174401457851707121619185280609848 5

En azul los 8 primeros dígitos que nos piden.