INFORME PRÁCTICA 6

Seguridad Avanzada

Ana Gómez Simón

MANUAL USUARIO

Para el correcto funcionamiento del escenario de voto creado se deben seguir los siguientes pasos:

1. Se deben tener los ficheros y la carpeta de la Figura 1 en el mismo directorio de trabajo.

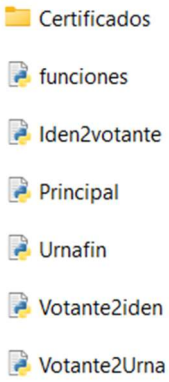

Figura 1. Ficheros necesarios

2. Se debe ejecutar el fichero Principal.py de la manera mostrado en la Figura 2. Hay que mencionar que dicho comando se debe ejecutar en el directorio donde se encuentran los ficheros anteriormente mencionados.

```
PS C:\Users\anags> cd '.\OneDrive\Desktop\Practicas Seguridad\P6'
PS C:\Users\anags\OneDrive\Desktop\Practicas Seguridad\P6> cd ..
PS C:\Users\anags\OneDrive\Desktop\Practicas Seguridad> cd .\Final\
PS C:\Users\anags\OneDrive\Desktop\Practicas Seguridad\Final> py .\Principal.py
```

Figura 2. Comando ejecución

3. A continuación, aparecerá una ventana como la de la Figura 3 para poder introducir el voto y los datos necesarios. En el caso del nombre únicamente permitirá votar a Alicia, Blanca y Carlos. En el caso del voto se ha realizado el programa para poder votar sí, no o en blanco (dejando vacía la casilla). Y por último, la sección de certificado se debe introducir el fichero de la clave privada del votante de la siguiente manera: \Alicia.pem. Una vez introducidos los datos, se debe pulsar el botón de guardar para que los datos se almacenen y después enviar para que el programa continúe.

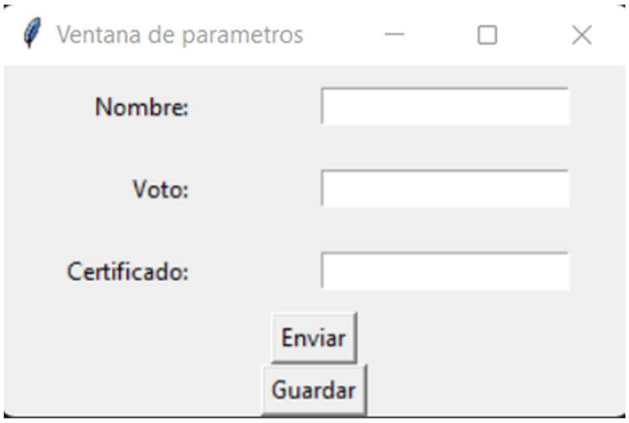

Figura 3. Ventana datos

4. En caso de que todo vaya correctamente se mostrará una advertencia como la de la Figura 4, y una vez pulsado en botón de OK se volverá a mostrar la venta de la Figura 3. Esto sucederá hasta que los tres votantes hayan votado, y en este caso el programa se cerrará y se tendrán almacenados los tres votos de los distintos votantes en sus correspondientes ficheros. En caso de que algo no vaya bien se mostrará un Warning con el mensaje correspondiente al error que ha surgido y una vez dado al botón de OK se parará el programa de voto. Los problemas que pueden surgir son:
    - El votante ya ha votado en otra ocasión
    - Datos mal introducidos
    - Voto nulo
    - Falta de datos
    - Mala validación de la urna
    - Mala validación del votante
    - Mala validación de la autoridad de identidades

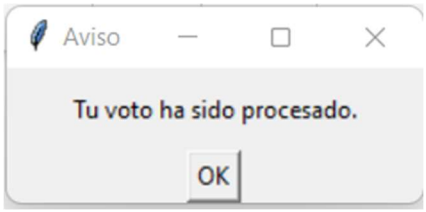

Figura 4. Ventana final

EXPLICACIÓN CÓDIGO

En esta práctica se ha realizado el ensamblaje de todas las prácticas anteriores de la asignatura para poder simular un escenario de voto. Para simular dicho escenario se ha realizado un modelo de firma ciega de la manera mostrada en la Figura 5.

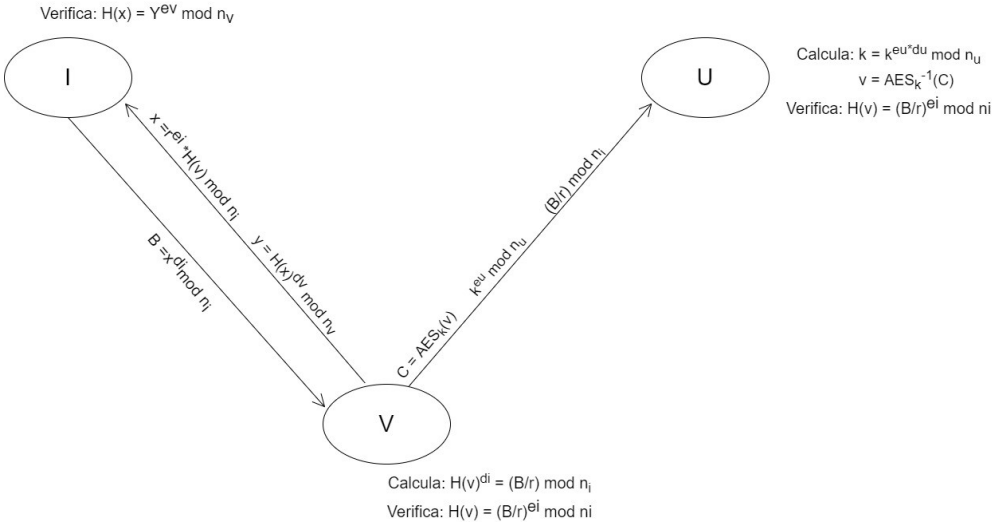

Figura 5. Escenario firma ciega

A su vez, para el correcto funcionamiento se ha seguido el diagrama de bloques mostrado en la Figura 6 en el script principal del escenario de voto.

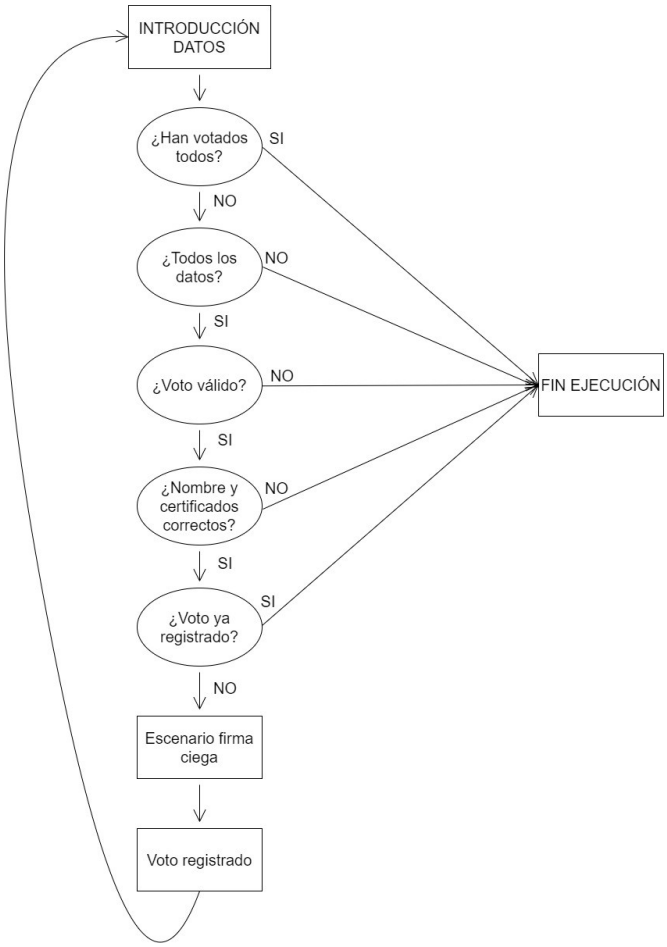

Figura 6. Diagrama de bloques

Se debe mencionar que para la firma ciega se han creado distintos scripts cada uno correspondiente a cada uno de los flujos de dicho escenario.

El primero de ellos corresponde con el flujo del votante a la autoridad de identidades, donde se recoge el voto y se le envían a la autoridad de identidades los parámetros x e y de la Figura 5.

El segundo script corresponde con el flujo de la autoridad de identidades al votante, en éste se verifica que el hash del parámetro x corresponde con el parámetro y firmado por la clave pública del votante. Una vez esto está verificado y es True se le envía al votante el parámetro B de la Figura 5.

El tercer script corresponde con el flujo del votante a la Urna, es el cual, se calcula primero la división B/r, donde r es un número aleatorio. Después de comprueba que dicho parámetro calculado y firmado con la clave pública de la autoridad de identidades corresponde con el hash del voto. En caso de que dicha comprobación sea correcta, se le envía a la urna el cifrado AES del voto con una clave k aleatoria, el cifrado RSA de dicha clave y el parámetro B/r anteriormente calculado.

El último script es el correspondiente a las comprobaciones de la Urna, primero se descifra la clave mediante RSA y con dicha clave descifrada se descifra el voto mediante AES. Una vez obtenidos estos parámetros se comprueba que el hash de dicho voto obtenido es igual al parámetro B/r firmado con la clave pública de la autoridad de identidades. En caso de ser True dicha comprobación se guarda el voto en un fichero.