

# Sistema de voto electrónico de la Universidad de Cádiz

## Manual de los miembros de la mesa de la votación

V 1.0 Marzo 2021

**1** Cada miembro de la mesa, de forma personal, procederá a la configuración de sus claves.

El miembro de la mesa recibirá en su correo electrónico el siguiente mensaje:

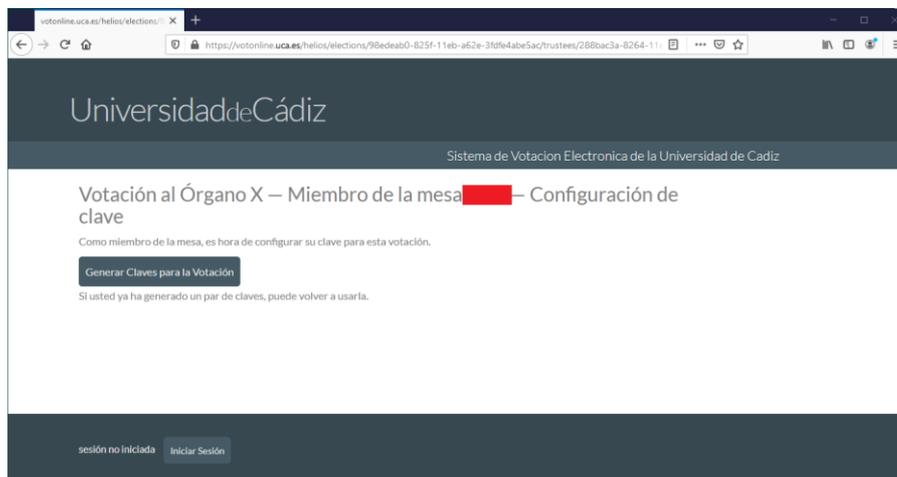
```
Usted es miembro de la mesa de Votación al Órgano X.  
Su panel de miembro de la mesa se encuentra en  
https://votonline.uca.es/helios/t/Votacion\_X/\[REDACTED\]/IRPMGS8byQUm  
--  
Sistema de Votacion Electronica de la UCA
```

Si pulsa en el enlace accederá a la siguiente página en la que configurará su par de claves para la descryptación del escrutinio una vez contabilizados los votos.

Una vez en la página, pulsará el botón ‘configure su clave’



Accederemos a la siguiente página y pulsaremos el botón ‘Generar claves para la votación’



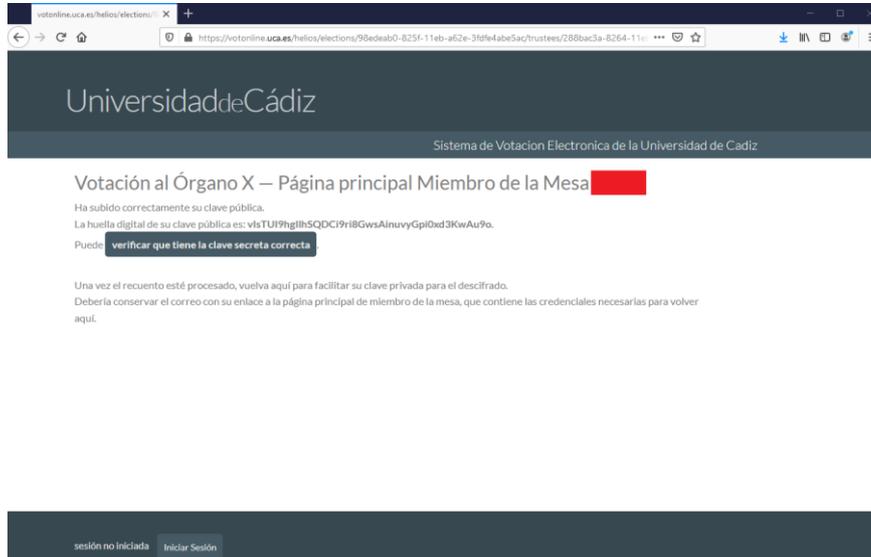
Pulsaremos el botón ‘Mostrar mi clave privada’



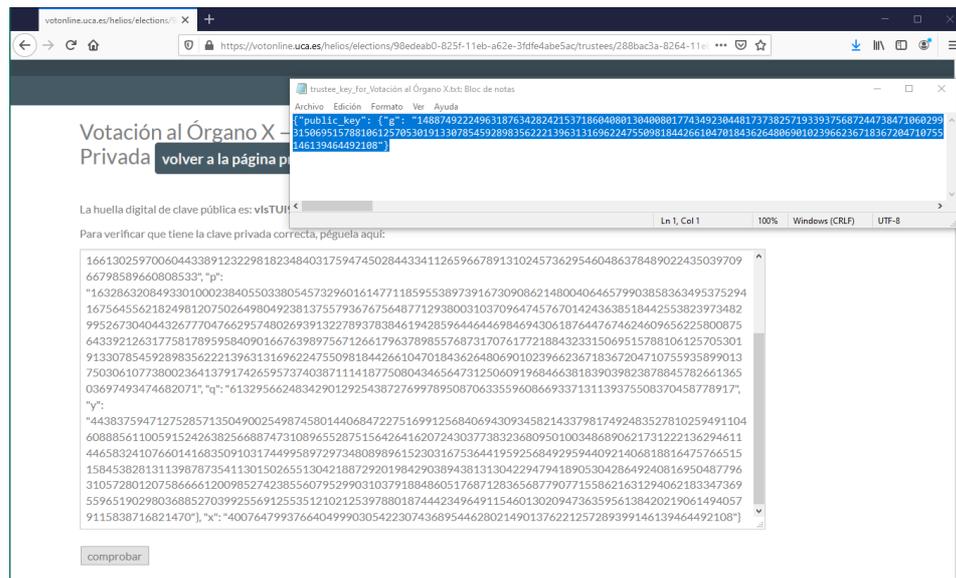
Nos aparecerá el contenido de nuestra clave privada y deberemos volcarla a un fichero de texto para su posterior uso. Una vez descargado el fichero de texto y almacenado en lugar seguro, pulsaremos el botón ‘Continuar con clave pública’. Puede ser muy conveniente y recomendable almacenar dicha clave privada en varias ubicaciones alternativas (como por ejemplo dispositivos de almacenamiento externo).

**MUY IMPORTANTE: ESTE FICHERO ES IMPRESCINDIBLE PARA REALIZAR LA DESENCRIPTACIÓN DEL ESCRUTINIO FINAL. SIN ÉL, NO PODREMOS SABER EL RESULTADO DE LA VOTACIÓN. DEBE GUARDARSE EN LUGAR SEGURO.**





Y en el cuadro que nos aparece pegamos el contenido completo del fichero de texto con nuestra clave privada



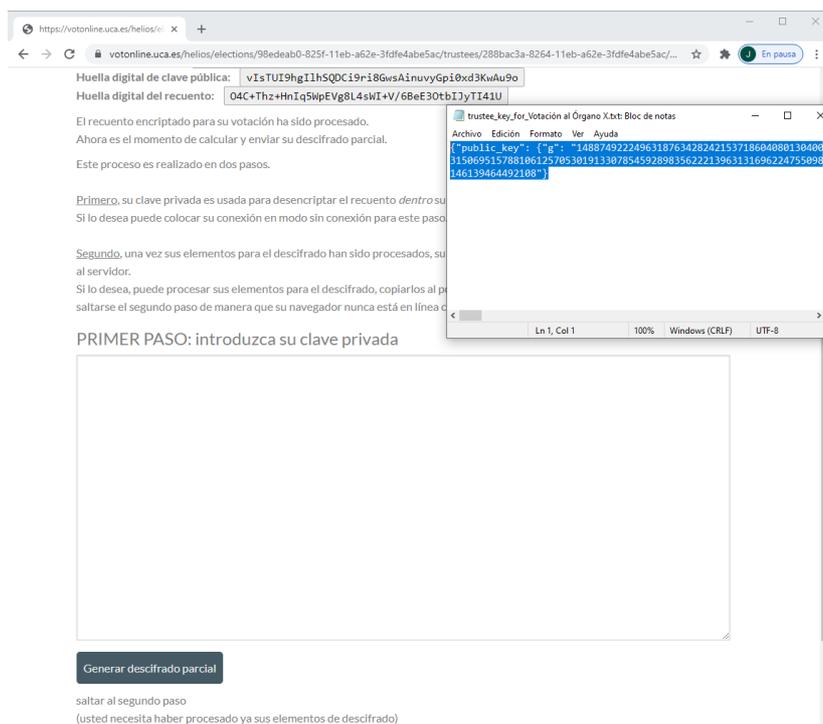
Si la clave privada es la correcta para nuestra clave pública nos lo indica en pantalla.

La huella digital de clave pública es: **vlsTUI9hgllhSQDCI9ri8GwsAinuvyGpi0xd3KwAu9o**  
su clave privada coincide

**2** Es el momento de abrir la urna. Una vez terminado el recuento, y para poder ver el recuento definitivo, los miembros de la mesa deben entrar en su panel de administración (correo que se les envió previamente). Pulsando en el enlace que aparece en dicho correo, entramos en esta página en la que se nos indica que el recuento cifrado está listo y que debemos proceder a subir nuestra clave privada para descryptarlo:



Pulsamos en ‘descifrar con su clave’:



Abrimos el fichero de texto con nuestra clave que teníamos descargado, copiamos su contenido íntegro, lo pegamos en el cuadro de texto de la web y pulsamos ‘Generar descifrado parcial’

#### SEGUNDO PASO: subir su descifrado parcial

Sus elementos y pruebas de descifrado parcial han sido generados a continuación.

Su clave privada ha sido eliminada de la memoria.

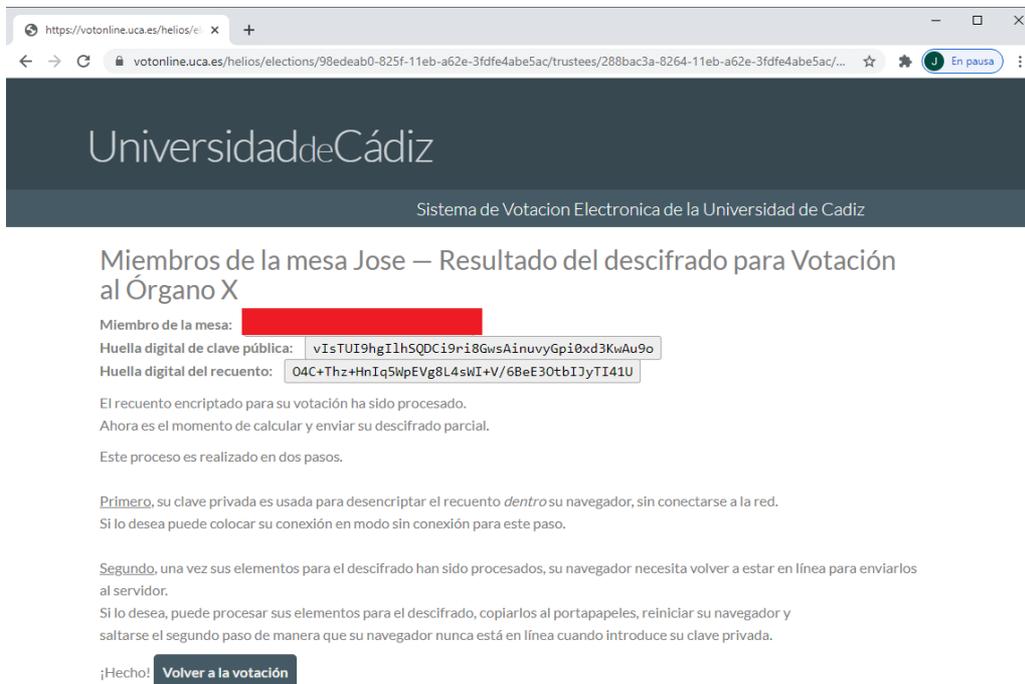
Cuando esté listo, puedes enviar este resultado al servidor.

Su descifrado parcial:

```
"712875341818128063062236065309916065258864981442984535896486783545744679098860596319397252222
0804891718829731868607737527502542506982895791664406874770183178656612578718760102181242896447
2083782921217516172732833051510235848374535721248985965290474078936273209360284347588410065430
6823912850617701769245277732446326652093085575932381079997080406733148543568809516442171448120
9742688498989545334924255816976882590333763054717351130667231290021179297598101131540840897231
7140646490596344549127994408162569269140001631960467238161573147745917881990648287827516890375
68512872321756137756518912827394454833418807145757236",
"342776147353486717288586647891890719043474762353323466143529913501860212854029328679089597662
4192112536899035055935862477183871822653812687600087462855638374512479871198258528851971718399
1318377010431939445833612197097310519988306932638264473056793183942463818670354084494076343624
1206096042493979725351890318495243977728945047477667304136195089178711627059573480121960839775
6797853713266197490795849134870138971893797081102715492746016055007920856551416223803772142669
7872689608672248626421266919788683942638730484889345266821397839404227853091070480913568163199
36022741543468984219679817544533966582676175296587790",
"428337628243967023097288683335775089741580899470003903121737737721342924912695692170358241425
22086212722659028158128278494027270802688729277687287056770126848222804225442242704140595594
```

Subir sus elementos de descifrado al servidor

Ahora pulsamos ‘Subir sus elementos de descifrado al servidor’ y si todo ha ido correctamente, debemos ver esta página:



https://votonline.uca.es/helios/e/ x +  
votonline.uca.es/helios/elections/98edeab0-825f-11eb-a62e-3fdfe4abe5ac/trustees/288bac3a-8264-11eb-a62e-3fdfe4abe5ac/... En pausa

## Universidad de Cádiz

Sistema de Votación Electronica de la Universidad de Cádiz

### Miembros de la mesa Jose — Resultado del descifrado para Votación al Órgano X

Miembro de la mesa: [REDACTED]

Huella digital de clave pública: vIsTUI9hgIIh5QDCi9ri8GwsAinuvyGpi0xd3KwAu9o

Huella digital del recuento: O4C+Thz+HnIq5WpEVg8L4slW+V/6BeE30tbIJyTI41U

El recuento encriptado para su votación ha sido procesado.  
Ahora es el momento de calcular y enviar su descifrado parcial.  
Este proceso es realizado en dos pasos.

Primero, su clave privada es usada para descifrar el recuento *dentro* su navegador, sin conectarse a la red.  
Si lo desea puede colocar su conexión en modo sin conexión para este paso.

Segundo, una vez sus elementos para el descifrado han sido procesados, su navegador necesita volver a estar en línea para enviarlos al servidor.  
Si lo desea, puede procesar sus elementos para el descifrado, copiarlos al portapapeles, reiniciar su navegador y saltarse el segundo paso de manera que su navegador nunca está en línea cuando introduce su clave privada.

¡Hecho! [Volver a la votación](#)