DESCRIPCIÓN DEL SISTEMA

Como se ha comentado anteriormente, nuestro proyecto se centra en el subsistema de ÁgoraUS, llamado Verificación.

Nuestro subsistema se encargará de verificar que un voto ha sido cifrado correctamente, proporcionando un par de claves pública y privada. Además, será el subsistema encargado de cifrar y descifrar los votos ofrecidos por los subsistemas integrados con Verificación.

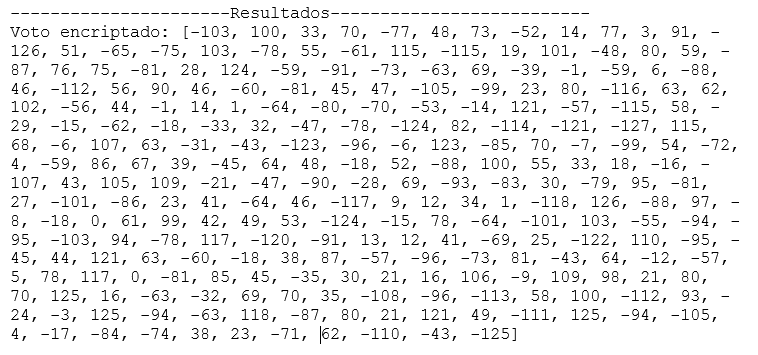
*Generación del par de claves pública y privada*

Cuando se crea una votación nuestro subsistema es el encargado de generar las claves pública y privada necesarias para el cifrado y descifrado de dicho voto. Dichas claves son de 2048 bits y se generan mediante el Algoritmo RSA. A continuación, se puede observar el formato de ambas claves:



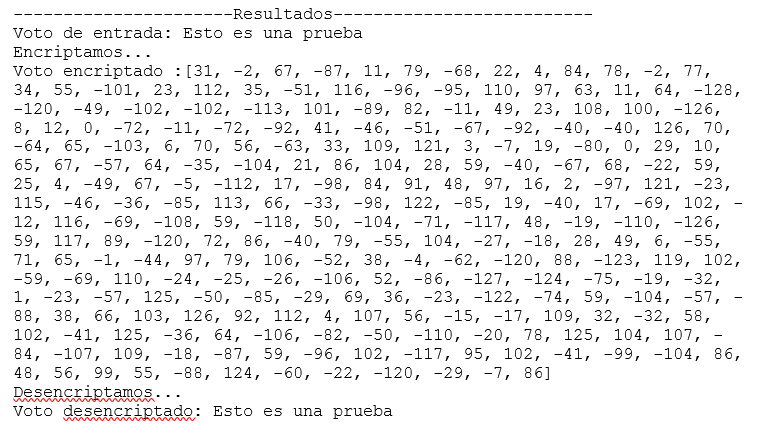
*Encriptado del voto*

Dado un voto y su clave pública generada como hemos explicado anteriormente, encriptamos el voto mediante RSA.



*Desencriptado del voto*

Dado un voto previamente cifrado y la clave privada relacionada con éste también generada previamente, desencriptamos el voto.



Previamente a la implementación de las anteriores funcionalidades descritas, ya que las heredadas del proyecto anterior no funcionaban correctamente, se procede a eliminar parte del código que no se va a usar para centrarnos exclusivamente en el algoritmo de cifrado RSA. Además de esto, se han eliminado todas las dependencias con la base de datos, ya que en nuestro caso no se van a guardar las claves públicas y privadas en ella, por mayor seguridad.

En cuanto a la planificación, al principio nos fuimos organizando bien, elegimos un día de la semana y quedábamos presencialmente en la universidad o mediante Skype, sobre todo los días previos a las fechas fijada para el seguimiento del proyecto. A parte de esto, también utilizamos como canal de comunicación la aplicación de mensajería Whatsapp. Hacer hincapié en los conflictos generados debido a la incompatibilidad horaria de todos los miembros del grupo, ya que cada uno tenemos un horario diferente y esto ha hecho difícil la planificación predecida al principio del desarrollo del proyecto.

A medida que íbamos avanzando en el proyecto nos íbamos dando cuenta de más funcionalidades del subsistema que no funcionan correctamente o que están desactualizadas, a parte de no estar integrado dicho año con ningún otro subsistema de Ágora US, lo cual nos hizo volver a reestructurar el susbsistema de la forma correcta.

Una vez reestructurado y limpiado el proyecto, pasamos a desarrollar lo que nos habíamos fijado para mejorarlo. Cada miembro del grupo se encargó de una parte del proyecto, pudiendo así trabajar en local.