Trabajo Evaluación Continua

Seguridad Informática
Curso 2018/19

Implementación de un sistema de voto electrónico con el esquema de Michael Merritt

Para la implementación del sistema, hemos usado la clase Cipher de Java. Para el cifrado de los votos, hemos usado RSA y como es necesario hacerlo por bloques, hemos implementado manualmente el modo ECB, donde cada bloque se cifra de forma independiente, ya que como se encadenan cifrados, hay un componente aleatorio. Para cifrar la llave privada y las cadenas aleatorias que se añaden al voto, hemos utilizado el AES en modo ECB también, ya que se lo que se cifra también tiene un componente aleatorio.

La aplicación ha sido desarrollada con un servidor Tomcat que se ejecuta solo localmente, por tanto, no habría problemas de seguridad porque no se puede acceder desde el exterior a este servidor, ya que el socket se crea en la IP 127.0.0.1 (localhost). No obstante, hubiera sido mejor desarrollarla con Swing y ser una aplicación completamente local, sin el uso de servidores Tomcat, pero hemos preferido el otro modo porque lo dominamos más.

Finalmente, hemos añadido una prueba en la que se intenta manipular la votación introduciendo otro voto y se puede observar como en todos los ordenadores sale una advertencia anunciando que la votación ha sido manipulada.

Jordi Miralles Comins
Fernando Ibañez Messeguer