Tema del trabajo

Diseño e implementación de un esquema e intercambio de clave para n-usuarios

Objetivos

El objetivo del trabajo es realizar una implementación del esquema desarrollado en el planteado en el paper “***Authenticated Key Establishment: From 2-Party To Group***” habiendo seleccionado como algoritmo 2-parte Cramer Shoup y se valorará sustituirlo por el algoritmo post-cuantico

Metodología seguida

La metodología seguida en el desarrollo del trabajo es la siguiente:

Una primera parte (Iteración 0) donde a partir de la documentación proporcionada por la directora del trabajo, se adquirió conocimiento sobre las herramientas criptográficas necesarias para la implementación del esquema a implementar.

En la fase de desarrollo se realizó siguiendo la metodología de desarrollo iterativo de dos semanas por iteración. Cada iteración presentaba a mi directora de trabajo los avances y planificábamos las tareas hasta la siguiente iteración.

Herramientas empleadas

Para desarrollar el trabajo, se ha utilizado Python como herramienta de programación, y las librerías (cryptography, sympy, dill) que se han requerido para poder implementarlo. Estas últimas están incluidas en el fichero requirements.txt con el fin de facilitar la instalación de las dependencias necesarias utilizando PIP (herramienta de instalación de librerías Python). Adicionalmente, se ha utilizado GitHub como herramienta de gestión de cambios.

Grado de avance

Actualmente la herramienta es funcional en dos formas de ejecución. La primera, menos realista, las instancias de todos los participantes están en una misma función de tal manera que los participantes se encuentran en el mismo proceso. Una segunda iteración, se implementó una ejecución más realista, donde los participantes se conectan a un proceso que simula ser un broadcast, y cada participante se ejecuta en un proceso independiente.

Dificultades encontradas

La mayor dificultad encontrada ha sido la implementación de la comunicación entre el broadcast y los clientes de los participantes. Esta dificultad se debe a la serialización de los mensajes y objetos que se comparten por el canal.

Planificación para terminar

Las tareas planificadas para terminar se componen de:

* Compleción de documentación en el repositorio
* Evaluación de posibles algoritmos post-cuánticos que remplacen el algoritmo Cramer Shoup y el algoritmo de intercambio de claves (Diffie-Hellman) por las correspondientes herramientas de Kyber-Cristal
* Redacción final de la memoria
* Incorporación de sugerencias y recomendaciones resultantes de la sesión de pre-defensa

Considerando el ritmo actual, se estima que será necesario un plazo entre 4-6 semanas para la realización de las tareas anteriores.

## Referencias

Incluir documentación de cryptography y sympy