IIC3253-2019/1 - Criptografía y Seguridad Computacional
Depto. de Ciencia de la Computación
Pontificia Universidad Católica de Chile
Tarea 2

Profesor: Tomás Barros

Fecha de Entrega: 22/5/2019

Se le pide implementar un software servidor y cliente en Python para un sistema de chat seguro. El servidor escucha conexiones TCP en un puerto configurable. Los clientes se conectan a este servidor donde escriben mensajes de texto, cuando un cliente manda un mensaje el servidor lo replica a todo el resto que esté conectado.

Requisitos:

- Los usuario (que se conectan con el software cliente para chatear) se identifican con un correo electrónico
- Suponga que todos los usuarios tienen un par de llaves pública/privada PGP (https://www.gnupg.org/) y que estas están publicadas en pool.sks-keyservers.net
- Los usuarios se debe autentificar con el servidor usando su llave PGP
- Los usuarios deben estar seguros que hablan con el servidor correcto (en otras palabras, su software cliente debe verificar la identidad del servidor)
- la comunicación entre el servidor y los clientes debe ser segura

La interfaz puede ser gráfica o un terminal, como le acomode más.

Su tarea debe tener un README comprensible de cómo se ejecuta. La calidad del código también será evaluada (nombres de variables, comentarios, coherencia... en resumen, siga las recomendaciones en https://www.python.org/dev/peps/pep-0008/) y podrá generarle que su nota disminuya o aumente según sea el caso.

Reglas de entrega:

- La tarea es **individual**, la copia no será tolerada.
- La entrega será hasta las 23:59:59 del miércoles 22/5/2019. **No hay atrasos, no habrá prórroga**
- Una tarea que no compila tiene automáticamente un 1.