Universidad del Norte
Departamento de Ingeniería de Sistemas y Computación
Estructura de Datos II

LABORATORIO 3

Fecha de entrega: 22 de mayo de 2024, 11:59 p.m.

El objetivo de este proyecto es intentar recuperar una serie de contraseñas que han sido almacenadas en una base de datos de manera segura, utilizando un protocolo de almacenamiento que funciona de la siguiente manera:

- Cada una de las personas tiene un par **`(username, password)`**, donde:
  - **`username`** es el usuario de Uninorte de la persona en cuestión.
  - **`password`** es la contraseña asociada a dicho usuario. Esta contraseña ha sido escogida de manera aleatoria del archivo **`rockyou.txt`**.
- Se requiere de una función Hash **`H`**.
  - En específico, **`H`** es la función Hash criptográfica **`SHA3-512`**.
  - Es importante mencionar que la salida de esta función Hash debe ser **determinista**.
- La contraseña **`password`** se convierte a bytes y se envía a la función **`H`**.
- Se genera un byte aleatorio **`(pepper)`** que se envía a la función **`H`**.
  - Este byte aleatorio corresponde a un número entero entre 0 y 255.
- Se genera una secuencia de 16 bytes aleatorios **`(salt)`** que se envían a la función **`H`**.
- Una vez que la función **`H`** este cargada con todos los datos se procede a calcular el valor hash **`(pwd)`** correspondiente a las entradas dadas.
  - En específico, se calcula **`pwd = H(password || pepper || salt)`**
- Finalmente, en la base de datos se guardan los valores **`(username, salt, pwd)`**, donde:
  - **`username`** es el usuario de Uninorte de la persona en cuestión.
  - **`salt`** es la representación hexadecimal de los 16 bytes aleatorios.
  - **`pwd`** es la representación hexadecimal de la salida de la función **`H`**.

Teniendo en cuenta lo anterior, deberán obtener la contraseña para **al menos** uno de los integrantes del grupo de trabajo utilizando como identificador el usuario Uninorte. Para ello, deberán utilizar el archivo de contraseñas comunes (**`rockyou.txt`**) y la base de datos (archivo de contraseñas) provistos.

Deberán **paralelizar** (mediante **hilos** y **sockets**) el proceso de búsqueda de contraseñas utilizando la arquitectura que prefieran (master/slave, P2P, etc.).

Es importante mencionar que todos los hilos de búsqueda se deben **detener** una vez encontrada la contraseña correspondiente.

Se recomienda utilizar la librería **`pycryptodome`** para el desarrollo del proyecto.

Para tener en cuenta:

- La solución (análisis) debe ser original.
- Puede utilizar Java o Python para desarrollarlo.
- Todos los códigos deben estar documentados por los integrantes del grupo.
- Este laboratorio es para desarrollar en grupos de mínimo 3 integrantes y máximo 4 integrantes, todo tipo de fraude será castigado según reglamento.
- Los grupos pueden estar conformados por los integrantes de los NRC **2357** y **2358**.
- Todo el código debe ser subido a un repositorio de **GitHub**.
- La sustentación del laboratorio se realizará durante la clase del día **23 de mayo de 2024**.
- Todos los integrantes del grupo deben estar presentes durante la sustentación del laboratorio.