Universidad Nacional Mayor de San Marcos

Facultad de Ingeniería de Sistemas e Informática

Proyecto de conteo y combinaciones

Llawi: Password manager basado en redes de sustitución-permutación

Alumno: Rodrigo José Alva Sáenz

Docente: Dr. Ciro Rodríguez Rodríguez

October 1, 2023

Tema

Gestor de contraseñas basada en el concepto de redes de sustitución-permutación que permita encriptar, almacenar y desencriptar contraseñas agrupadas de forma segura, rápida y minimalista.

Problema

Según estadísticas de websiterating.com, para enero de 2023, habían 5,569,200,301 de usuarios en Internet, esto, tomando también en cuenta que, en promedio, las personas tienen hasta 85 contraseñas asociadas a plataformas en las que tienen alguna cuenta registrada (de acuerdo a Cnet, 2020).

De acuerdo al Instituto Ponemon (2020), también, el 62% de las empresas que tienen actividad en la red no consideran haber asegurado la información que manejan en dispositivos móviles.

Esta realidad es bastante preocupante considerando que la mayoría de personas no suelen preocuparse por el manejo ni generación de contraseñas seguras para sus cuentas, por lo que son mucho más susceptibles a ataques de malware de terceros o brechas de información interna. Bajo esa realidad se nota que es necesario el desarrollo de sistemas basados en la gestión y encriptación de estas contraseñas.

Objetivos

Objetivo general

Desarrollar una aplicación que permita generar nuevas contraseñas mediante permutaciones aleatorias de grupos de caracteres y que además permita almacenar estas mismas contraseñas de forma encriptada y segura de forma local, usando una red de sustitución-permutación de múltiples rondas.

Objetivos específicos

1. Desarrollar un algoritmo que, realizando una permutación aleatoria sobre grupos de caracteres alfanuméricos y simbólicos (incluyendo espacios), permita generar contraseñas aleatorias.

2. Desarrollar un algoritmo que permita encriptar las contraseñas generadas mediante rondas múltiples dentro de una red de sustitución-permutación, además de que dentro de cada bloque de sustitución se utilice un caracter de una llave única para obtener la disyunción exclusiva.

3. Utilizar un bloque de permutación de orden determinista para alterar el orden de los caracteres de la contraseña en cada ronda tras la sustitución para que estos valores pasen a la siguiente ronda.

4. Almacenar la contraseña finalmente encriptada en un archivo local de un directorio determinado como archivo binario, de forma que no pueda ser fácilmente leído por vulneradores.

5. Desarrollar un algoritmo que permita buscar el archivo binario encriptado mediante el nombre de la cuenta asociada a la contraseña para luego aplicarle la red inversa de desencriptación, para finalmente entregarle el resultado al usuario.