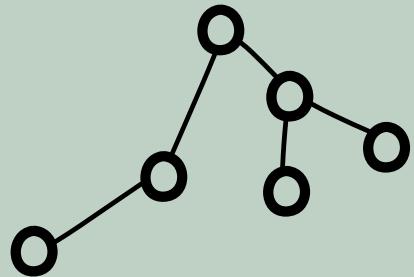


BÚSQUEDA DE CONTRASEÑAS CON DICCIONARIO

INTRODUCCIÓN



Este proyecto se ha estado trabajando a lo largo del semestre, incluyendo de forma directa los temas vistos en la materia. El proyecto es un programa de búsqueda de contraseñas por medio de diccionarios establecidos para buscar la vulnerabilidad de nuestras contraseñas y así poder determinar que tan fáciles son de descifrar por medio de una computadora.



OBJETIVOS

Como objetivo tenemos que el algoritmo permita al usuario ingresar sus contraseñas deseadas a revisar su vulnerabilidad, el algoritmo con base a unos diccionarios con diferentes tipos de combinaciones de contraseña pueda descifrar una o varias de las contraseñas ingresadas y marcar si logró descifrar alguna el tiempo en descifrarla. Finalmente implementar el algoritmo de Huffman para agilizar la eficiencia en la carga de los diccionarios.



METODOLOGÍA

El funcionamiento del algoritmo se basa en el uso de diccionarios definidos para la búsqueda rápida de contraseñas que han sido expuestas o que son comunes o fáciles de descifrar. Por medio de este código, se plantea ver las distintas vulnerabilidades que enfrentan las contraseñas que podrían ser las nuestras para así tenerlas en estudio y saber cómo proteger mejor nuestra información.



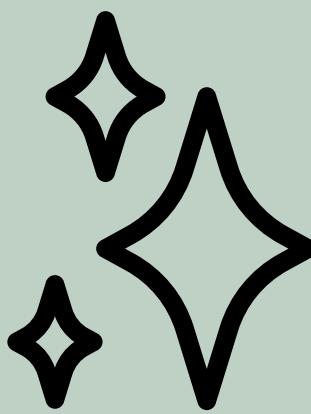
BRAULIO HURTADO ESCOTO
JUAN PABLO SOLIS REGIN
JORGE DANIEL HERNANDEZ
REYES

Análisis de algoritmos / D06
CUCEI -
JORGE ERNESTO LOPEZ ARCE
DELGADO



RESULTADOS

El proyecto queda terminado con el funcionamiento principal de búsqueda de contraseñas por medio de diccionario. Teniendo como resultado un algoritmo donde el usuario deberá de ingresar contraseñas que desea validar su vulnerabilidad, este mismo buscara distintas combinaciones propias y en los diccionarios con contraseñas ya establecidas para agilizar más el tiempo del descifrado, durante el proceso se muestra en pantalla el funcionamiento de la búsqueda de las contraseñas, mostrando las contraseñas descifradas y el tiempo que le llevó al algoritmo a descifrarla o en otro caso, muestra el algoritmo ejecutarse y terminarse sin haber logrado descifrar ninguna de las contraseñas ingresadas por el usuario.



CONCLUSIÓN

El análisis de rendimiento confirmó que el algoritmo es altamente efectivo para determinar la vulnerabilidad de las contraseñas, logrando descifrarlas en tiempo polinomial en la mayoría de los casos.

La implementación del Algoritmo de Huffman en la fase de diccionario redujo significativamente el tiempo de acceso a los datos. El análisis demostró que esta optimización mejora la complejidad asintótica en términos de búsqueda de elementos en el diccionario, pasando de $\mathcal{O}(N)$ a un rendimiento promedio cercano a $\mathcal{O}(\log N)$ para las combinaciones más frecuentes.

LOS NO GPUS