UNIVERSIDAD CENTRAL DEL ECUADOR
COMPUTACIÓN
CRIPTOGRAFIA

Nombre: Espinosa Joel

Soria Nelson

Toscano Juan

Fecha: 05/11/2024

Algoritmos de Cifrado

Cifrado de sustitución (Cesar)

Un cifrado de sustitución reemplaza cada letra o símbolo en el texto plano con otro, de acuerdo con una regla o clave fija. Por ejemplo, el cifrado César desplaza cada letra en un cierto número de posiciones en el alfabeto.

Cifrado de transposición

Un cifrado de transposición reorganiza el orden de las letras o símbolos en el texto plano, de acuerdo con una regla o clave fija. Por ejemplo, el cifrado de la cerca del riel divide el texto sin formato en filas y luego las lee en diagonal.

Cifrado de Vigenère

El cifrado Vigenère es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado poli alfabético y de sustitución.

En términos matemáticos, puede expresarse la función de cifrado como:

$$E(X_i) = (X_i + K_i) mod\ L$$

Donde (X_i) es la letra en la posición i del texto a cifrar, (K_i) es el carácter de la clave correspondiente a (X_i) , pues se encuentran en la misma posición, y

L es el tamaño del alfabeto. En este caso L=27

Bibliografía

«¿Cómo se prueba la fuerza y seguridad de un cifrado de sustitución o transposición?», *www.linkedin.com*, 9 de marzo de 2023. https://www.linkedin.com/advice/1/how-do-you-test-strength-security-substitution-transposition?lang=es&originalSubdomain=es

«El cifrado de Vigenère». https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a11.htm