Universidad del Valle de Guatemala Facultad de Ingeniería



Laboratorio #2 Esquemas de detección y corrección de errores

Marco Antonio Jurado Velasquez 20308 Cristian Eduardo Aguirre Duarte 20231

Introducción

Los esquemas de detección y corrección de errores son utilizados en comunicación de datos para garantizar la integridad de la información . Estos algoritmos permiten detectar si ha ocurrido algún error durante la transmisión o el almacenamiento como el algoritmo CRC-32 y, en algunos casos, como lo es con el algoritmo de Hamming incluso corregirlos.

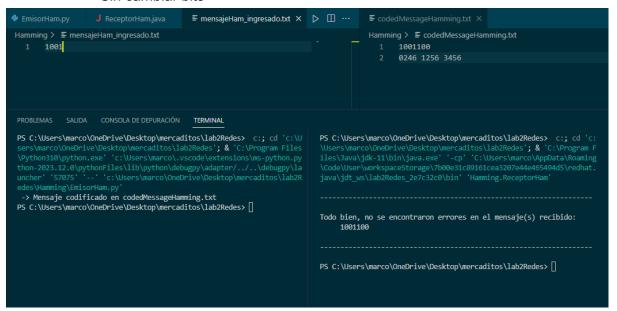
El algoritmo de Hamming es de detección y corrección de errores desarrollado por Richard Hamming. Este algoritmo realiza la adición de bits de paridad a un mensaje para detectar y así poder corregir errores de un solo bit en la cadena de mensaje codificada. Se colocan o se suman estos bits en casillas específicas para así poder diferenciar a la hora de encontrar un error en que bit específico se encuentra el error. Es utilizado por ejemplo en la memoria RAM de las computadoras.

CRC (Cyclic Redundancy Check) es un algoritmo de detección de errores que utiliza operaciones matemáticas de división. CRC-32 es una variante común del algoritmo que utiliza polinomios de 32 bits para calcular el valor de comprobación. En este caso se utilizó la variante vista en el curso. Al recibir el mensaje, el receptor también calcula el valor de verificación y lo compara con el valor recibido. Si ambos valores coinciden, se asume que el mensaje no tiene errores. CRC-32 se utiliza en sistemas de almacenamiento.

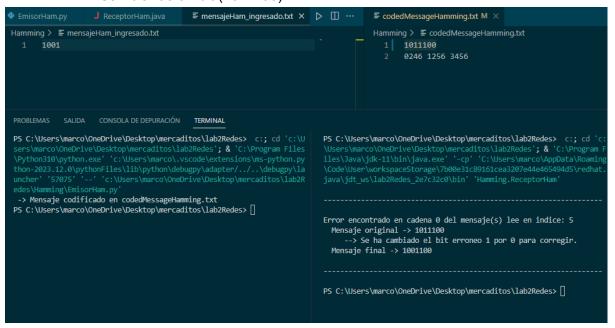
Resultados

Hamming

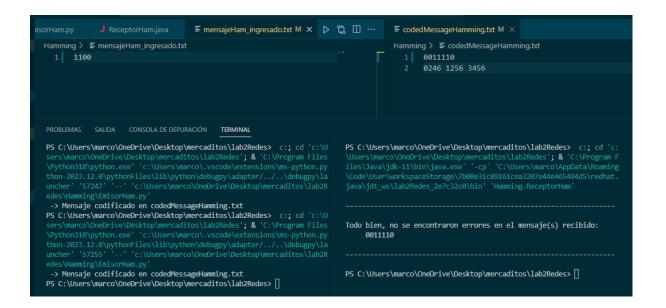
- Prueba con mensaje 1001
 - Sin cambiar bits



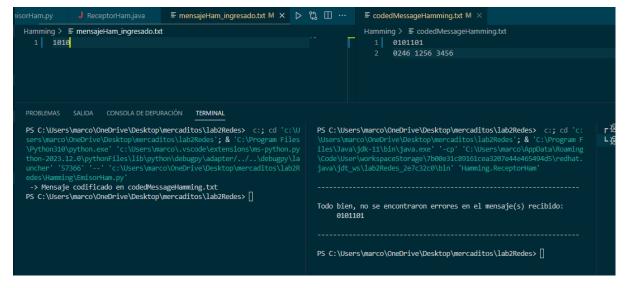
Cambiando un bit (1011100)



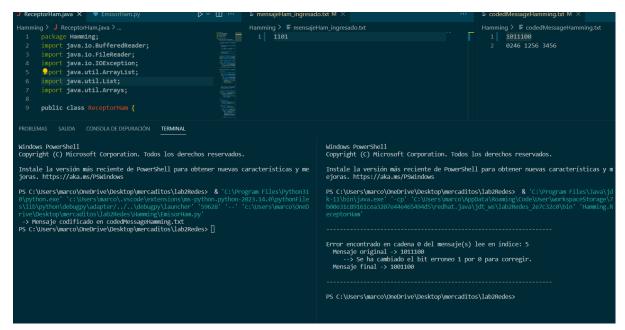
- Prueba con mensaje
 - Sin ningún error



- Prueba con mensaje
 - o Sin errores



- Pruebas cambiando un bit
 - o 1101
 - **1011100**

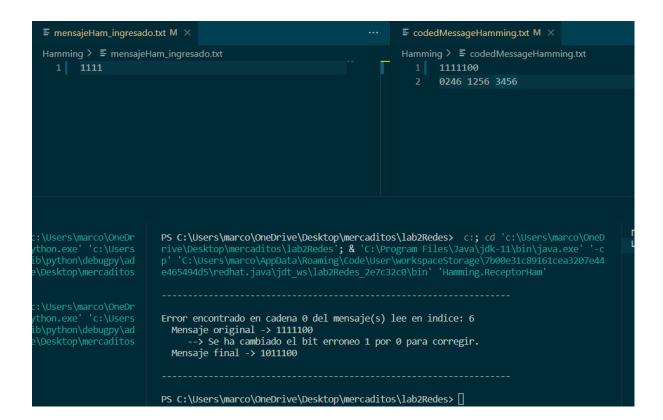


0 1011

■ En esta situación se ha cambiado de 1100100 a 1101100 esto sin embargo altera al algoritmo de hamming y este reconoce que la cadena no esta correcta pero lo modifica no al original pero a otra trama. Eso se debe a la verificación de los bits de paridad que estos tambien coinciden con la corrección para generar dicha trama resultante

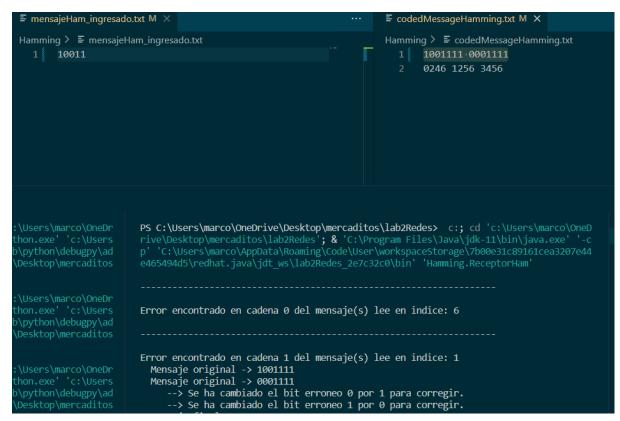


- o 1111
 - cambia de 1110100 a 1111100



De la misma manera los bits de paridad satisfacen dicha trama generada.

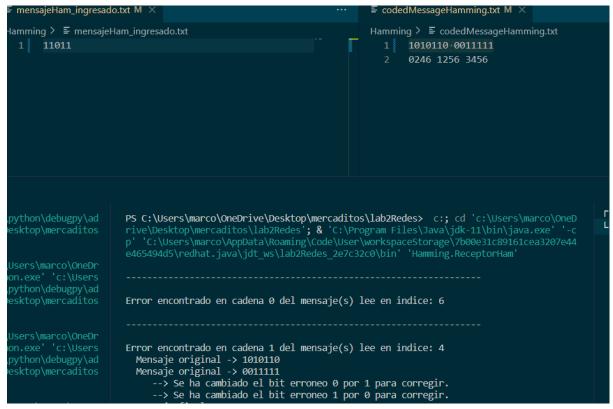
- Cambiar dos bits
 - 0 10011
 - En este caso la trama cambia de 1001100 0001111a 1001111 0001111



correctamente se detectan y se cambia

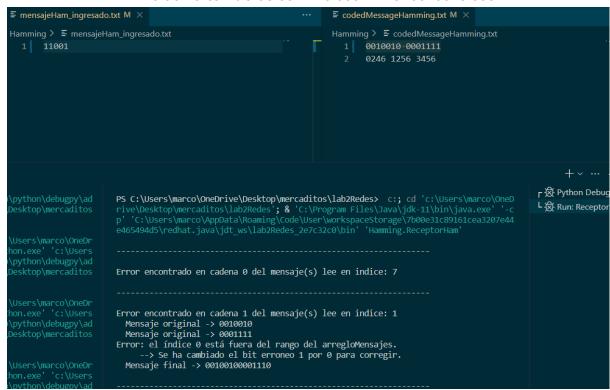
11011

la trama cambia de 1010100 0001111 a 1010110 0011111



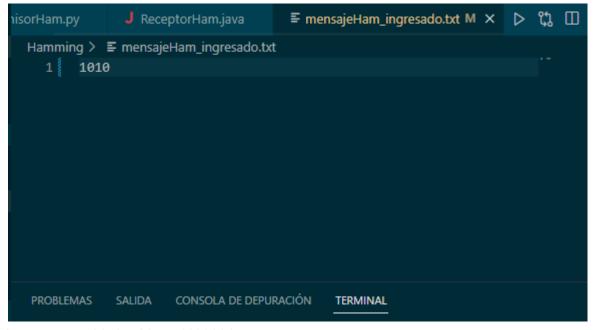
cambiando correctamente ambos bits.

la trama cambia de 0011110 0001111 a 0010010 0001111

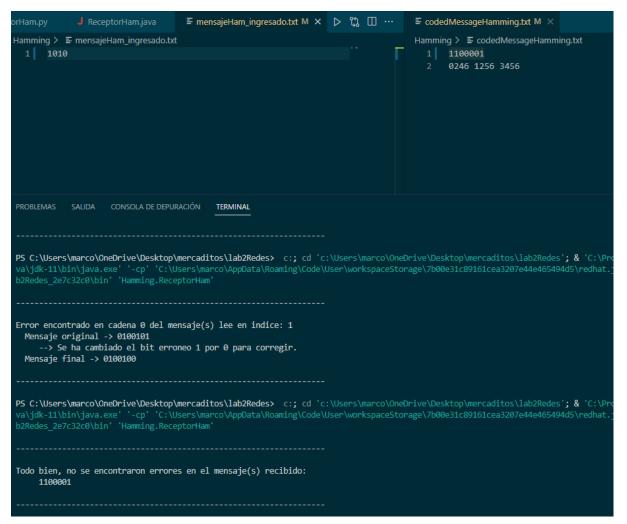


Cambiando ambos bits en la trama.

- Un error que Hamming no podrá detectar es cuando se cambian bits en alguna trama que no está cubierta por los bits de paridad
 - o mensaje 1010



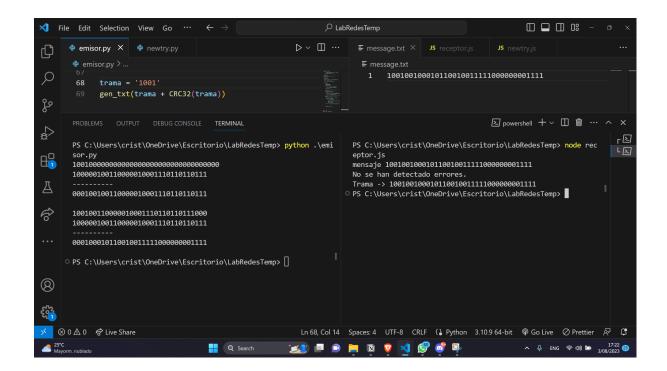
luego se cambia los bits a 1100001

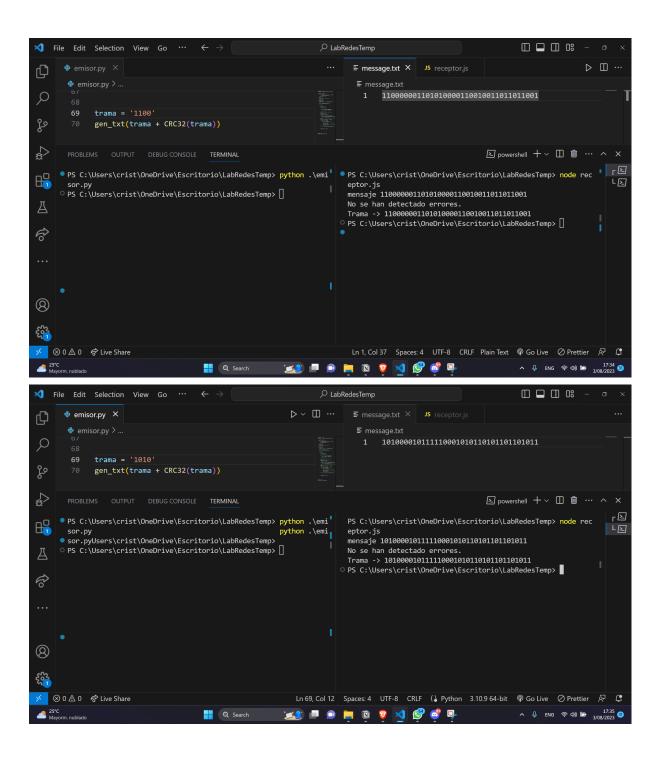


Podemos ver que Hamming dice que no hay errores pues si tenemos los errores presentes pues cambiamos 3 bits

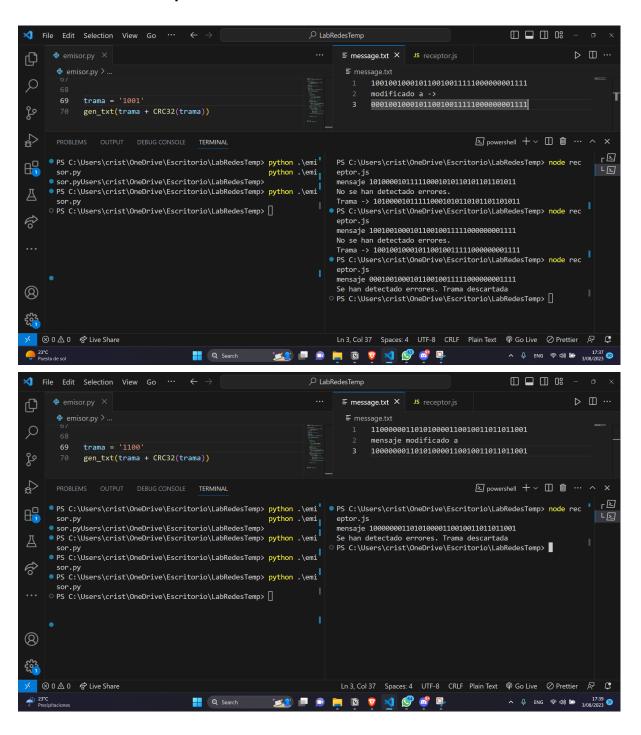
CRC-32

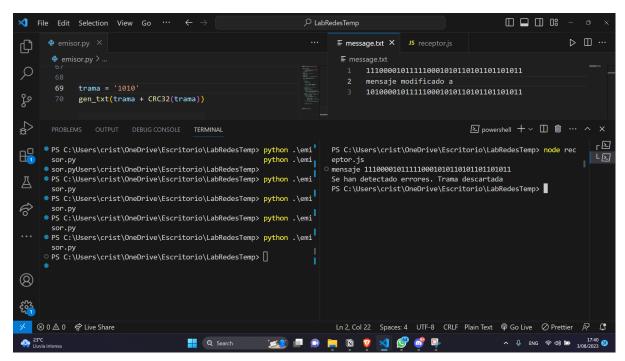
- Trama:



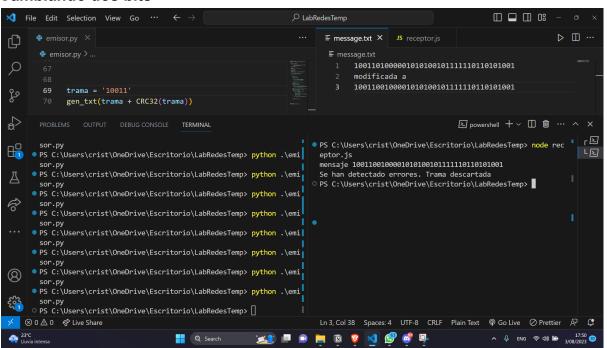


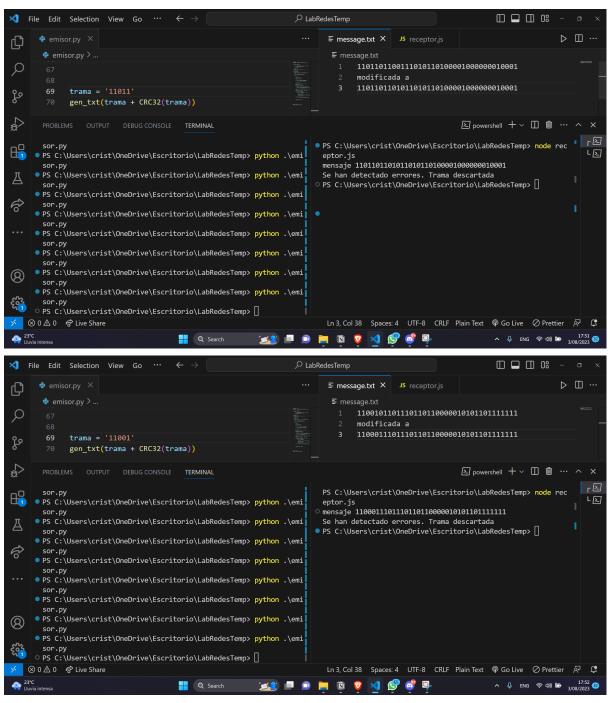
Tramas modificadas para detección de errores



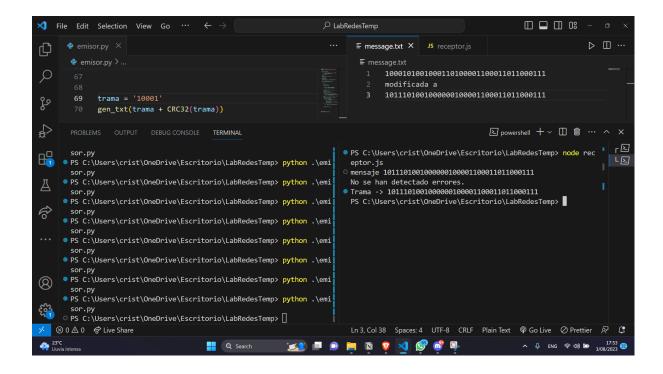


Cambiando dos bits





Trama modificada que no el algoritmo no detecta como error



Discusión

En los Esquemas de detección y corrección de errores, pudimos observar cómo se comportan los algoritmos de Hamming y CRC-32 durante su ejecución. Sin embargo, encontramos ciertas limitaciones en el algoritmo de Hamming en lo que respecta a la detección de errores, ya que depende en gran medida de los bits de paridad y su lógica de funcionamiento. En el algoritmo de Hamming notamos que cambiar dos o más bits en una trama puede generar situaciones en las que el mensaje parece estar correcto según Hamming. Un ejemplo de esto ocurre cuando ingresamos la cadena 1010 y aplicamos el algoritmo de Hamming. Inicialmente, el mensaje no muestra errores en su codificación. Después de aplicar la codificación de Hamming, obtenemos el código 0101101. Sorprendentemente, si modificamos algunos bits de este código y lo transformamos en 1100001, Hamming no detectará ningún error, ya que este nuevo código cumple con las reglas del algoritmo y se considera válido.

Esta particularidad del algoritmo de Hamming nos lleva a reflexionar sobre la importancia de complementar su uso con otros métodos de detección y corrección de errores, como el algoritmo CRC-32, que pueden proporcionar una mayor robustez en la detección de alteraciones en los datos transmitidos. Al emplear una combinación de estos algoritmos, podemos mejorar la fiabilidad y seguridad de nuestras comunicaciones y asegurar una detección más efectiva de posibles errores.

Comentario

 El algoritmo de Hamming a pesar de tener una explicación un poco más sencilla consta de muchas verificaciones de los bits de paridad lo cual lo hace más robusto pero no infalible.

Conclusiones

- Hamming es efectivo para detectar y corregir errores en la transmisión de datos, pero no es infalible pues podemos encontrar que al tener errores que satisfacen las reglas estos no son perceptibles por el algoritmo.
- 2. Es esencial no solo hacer uso de un algoritmo pues tenemos implementaciones de código más robustas como el crc-32 que llega a ser un poco más difícil de engañar con errores en las tramas.

Citas y referencias bibliográficas

Conway, J. H., & Sloane, N. J. A. (1998). Sphere Packings, Lattices and Groups (3rd ed.). New York: Springer-Verlag. ISBN 0-387-98585-9. (requiere registro).

History of Hamming Codes. (n.d.). Archivado desde el original el 25 de octubre de 2007. Consultado el 3 de abril de 2008.