Criptosistema asimétrico de McEliece

Farid Abulias Farías[1]

[1]Escuela de Informática y Telecomunicaciones, Universidad Diego Portales, Santiago, CL

Se hablará acerca de la implementación del criptosistema de llave publica creado en 1978 por Robert McEliece, donde para su codificación y decodificación se utilizará el algoritmo de Hamming.

***Index Terms*—Hamming(15,11), Criptosistema McEliece, Criptografía de llave publica.**

I. Introducción

EN esta ocasión se solicito el reutilizar la implementación de Hamming que se había realizado hace un tiempo atrás, con motivo de realizar de apoyo para la codificación y decodificación para el criptosistema creado por Robert McEliece en 1974, donde se pueden aplicar variados métodos correctores de errores como lo es Hamming (codigos lineales), en otros ejemplos se utilizan bastante los códigos correctos Goppa

II. Desarrollo

Para realizar el procedimiento se requiere si o si de algo clave en Hamming, las que son su matriz G y H, con las que se procedera a realizar la base aún, no obstante en la matriz G hay variaciones, por ejemplo, la nueva matriz G se formara a partir de la multiplicación de la matriz S y matriz P, para realizar este proceso existen 2 funciones claves:

- def genSMatrix(k)
- def genPMatrix(n,keep=False)

Estas funciones permiten generar una matriz S de orden kxk y una matriz P de orden nxn.
Por otra parte y no menos importante tenemos la generación de una llave publica y una privada, la llave privada esta compuesta por (G, S, P) y la publica la compone $(G * S * P, t)$, donde :

- **G** es la matriz generadora de Hamming.
- **S** es una matriz no invertible.
- **P** es una matriz de permutación binaria.
- **t** es la capacidad correctora de Hamming.

En el presente informe no se pretende realizar una explicación detallada de lo que es el criptosistema mcEliece, ya que se asume que el lector maneja ciertos conceptos previos para su entendimiento completo y que este estudio esta basado en la utilización de McEliece como un criptosistema de llave publica apoyado por el Código Hamming para el caso en que se decida encriptar un mensaje del largo k.
Para realizar ambas pruebas existe un archivo Test.sh, este archivo debe ser ejecutado a través de la consola de comandos de Bash, donde se llevaran acabo 2 archivos, el primero realiza la encriptación y desencriptación de un mensaje fijo, mientras que el segundo test incorpora la utilización un segmento de la biblia como texto de prueba, en ambos finalmente.

farid.abulias@gmail.com

III. Conclusión

Se aprovecharon estructuras creadas anteriormente, como lo es el código Hamming para la utilización de un criptosistema de llave publica, la gracia de utilizar Hamming y no hacerlo por decirlo al azar es que la matriz Generadora de Hamming esta basada en la generación única de mensajes en una dimensión 2^n palabras posibles a utilizar.

Referencias

[1] Digital Signal Processing (4th Edition), Proakis.
[2] Apuntes de cátedra, profesor José Pérez B.
[3] [Online] https://en.wikipedia.org/wiki/McEliece_cryptosystem