MA4402-1 Simulación Estocástica: Teoría y Laboratorio
Profesor: Joaquín Fontbona T.
Auxiliares: Bruno Hernández P. y Pablo Araya Z.
Integrantes: Carlos Antil y Nicolás Bravo

Redes Neuronales aplicadas al criptánalisis del Algoritmo de Cifrado DES

1. Introducción

Hoy en día los algoritmos criptográficos desempeñan un papel importante en la protección del transporte electrónico de todo tipo de datos, por ejemplo ayudan a prevenir el fraude de datos como el perpetrado por piratas informáticos que obtienen ilegalmente información financiera electrónica.

Existen varios algoritmos de cifrado los cuales permiten encriptar un mensaje antes de enviarlo y poder desencriptarlo al ser recibido con tal de evitar que el mensaje sea cifrado por adversarios en el camino. Estos generalmente dependen de información ("llave") que tiene el receptor y emisor del mensaje, pero no el adversario.

El criptánalisis es una área de la criptografía, la que se enfoca en *"quebrar"* los algoritmos de cifrado, es decir, se enfoca en crear algoritmos los cuales permitan a un adversario poder descifrar mensajes a pesar de no estar en conocimiento de la *"llave"* del algoritmo.

Este proyecto estará centrado en el algoritmo de cifrado DES (Data Encryption Standard). El objetivo es realizar un análisis, mediante redes neuronales, sobre la posible existencia de un adversario a DES, además de estudiar los recursos y tiempo que éste tomaría.

2. Presentación

Para la presentación se abarcarán los siguientes puntos:

- Implementación del algoritmo DES.
- Implementación de dos tipos de redes neuronales distintas.
- Entrenar y testear cada red neuronal mediante datos generados por el algoritmo DES.
- Comparar la efectividad de las redes neuronales aplicadas a DES.

3. Bibliografía

- https://en.wikipedia.org/wiki/Neural_cryptography
- http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81610/8/pnovasTFG0618memoria.pdf
- Introduction to Modern Cryptography, 2nd Edition, Chapman & Hall/CRC
- https://www.youtube.com/watch?v=XwUOwqSHzyo