UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
SISTEMAS DE COMUNICACIÓN

Laboratorio 2 Sistemas de Comunicación

Instrucciones

El objetivo de esta experiencia es que logren diseñar un sistema de encriptación simétrico y evaluar su rendimiento y funcionamiento a partir de una serie de métricas posteriormente detalladas. Esta experiencia contará de dos partes:

1. En primer lugar deberán diseñar el sistema de encriptación y a través de un informe explicar el algoritmo que hayan ideado para este propósito, además de incluir la evaluación de dicho sistema.

2. Luego de esto deberán implementar su algoritmo. Deberá tener una interfaz sencilla en dónde se pueda encriptar y desencriptar fácilmente ingresando un texto a elección del usuario. Además, se debe incluir un archivo README con las instrucciones de compilación de su programa.

A partir de las actividades descritas deberá redactar un informe con los siguientes incisos:

- Portada
- Introducción: Definición de objetivos, motivación y estructura del informe.
- Explicación del algoritmo de encriptación: explicar los pasos que sigue, el tipo de alfabeto utilizado, el tamaño de la llave, entre otros. Debe justificar por qué su sistema cumple con el efecto avalancha (el cambio en un bit de la entrada o de la clave produzca el cambio de aproximadamente la mitad de los bits de salida)
- Evaluación del algoritmo: En base a las métricas explicadas más abajo.
- Criptoanálisis: Explorar las opciones y estrategias para descifrar un mensaje codificado, siendo el mensaje original de al menos 8 caracteres.
- Conclusión: Sobre el trabajo y objetivos.

Este laboratorio debe ser realizado en grupos de 3 personas. En caso de copia será evaluado con nota mínima y es causal de reprobación del laboratorio. La fecha de entrega es el día 4 de Enero de 2019 a las 23:55, y tanto el informe como el código fuente debe ser entregado vía Moodle en el link habilitado para este propósito en un archivo comprimido con extensión 7z o zip. En cuanto al programa, este podrá ser implementado en Python 2.7 o JavaScript ES5. **RECUERDE** adjuntar el archivo README como se mencionó más arriba.

Criterios de evaluación del algoritmo

Al cambiar de tamaño los bloques, debe verificar si el tiempo de ejecución del algoritmo que diseñó varía o se mantiene constante. Para esto se deben hacer a lo menos 4 variaciones al tamaño de dichos bloques.

Además, se debe calcular el throughput para dichas variantes. En los sistemas de encriptación el Throughput está dado por el tamaño del bloque utilizado en Kilobytes dividido por el tiempo de encriptación.

$$T = \frac{Size_{bloque}}{T_{enc}}$$