UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
SISTEMA DE COMUNICACIÓN
LABORATORIO : CRIPTOGRAFÍA

Objetivos

Esta experiencia tiene como objetivo ahondar en los conceptos de criptografía, criptoanálisis y cómo desarrollar un buen sistema de encriptación simétrico de información para encubrir los ante posibles ciberataques.

Introducción

La criptografía se le conoce como el arte y técnica de escribir con procedimientos o claves secretas, de tal forma que lo escrito solamente sea inteligible solo para quien sepa descifrarlo. Esto con la finalidad de proveer autenticidad del emisor, confiabilidad e integridad de la información.

En este laboratorio se pretende diseñar un sistema criptográfico simétrico, el cual consta de una única llave que sea capaz de encriptar y desencriptar un mensaje, como se detalla en la Fig. 1. Se busca implementar un cifrador y descifrador por bloques, así como la llave correspondiente.

Figura 1. Cifrado simétrico

Además se busca evaluar el desempeño del sistema a través de la relación entre el tamaño del bloque y el tiempo de ejecución del algoritmo que diseñó. En los sistemas de encriptación se suele definir el *Throughput (1)* en base al tamaño del bloque en Kilobytes dividido por el tiempo de encriptación. Debe realizar pruebas con varios tamaños de bloque. Otra característica importante de un sistema de cifrado se conoce como *Efecto avalancha*. Se espera que el cambio de un bit en la entrada o en la clave, produce un cambio considerable en la salida, aproximadamente al 50% de los bits de salida

$$Throughput = \frac{Tamaño_{bloque}}{Tiempo_{encriptación}} \quad (1)$$

UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
SISTEMA DE COMUNICACIÓN
LABORATORIO : CRIPTOGRAFÍA

Instrucciones

1. El trabajo es en parejas.
2. Fecha de entrega: **Martes 12 de Julio del 2019 hasta las 23:55**.
3. La entrega consta de un informe de laboratorio (en PDF) y el código fuente con que se hicieron las pruebas.
4. La entrega tanto del informe (en PDF) como del programa debe ser en un archivo comprimido a través del link publicado en el curso de la plataforma Moodle www.udesantiagovirtual.cl
5. Cualquier copia detectada entre los trabajos será calificada con nota mínima y será causal de reprobación del laboratorio.

Herramientas

Se utilizará el lenguaje de programación Python 3 y algunos módulos de utilidad como: PyCrypto o hashlib.

Se recomienda utilizar algún IDE adecuado para el desarrollo de su trabajo por ejemplo: PyCharm o Spyder, entre otros.
La documentación de hashlib y de PyCrypto serán suficientes para abordar su diseño de cifrado simétrico. Si se usa otras fuentes de información, se debe citar, incluyendo los sitios web que usó como referencias.

Desarrollo

En clases se estudió el concepto de criptografía, criptoanálisis y los distintos cifrados. Cada sistema de cifrado tiene un propósito específico que está relacionado en cómo su diseño es capaz de cumplir con las premisas mencionadas en la sección Introducción. En base a las clases de cátedra se debe realizar lo siguiente:

1. Diseñar un cifrado simétrico.
    a. Puede influenciarse por un cifrado ya conocido, replicarlo, mejorarlo o diseñar una simplificación).
    b. Describa el algoritmo y/o las etapas de dicho cifrado.
    c. Describa cuál es el propósito o principales objetivos de su sistema.
2. Implemente el sistema de cifrado que diseñó con los siguientes aspectos:
    a. Tamaño de la llave o clave.
    b. Tamaño del mensaje a encriptar o desencriptar.
    c. Tamaño de los bloques a encriptar
    d. Función principal que realiza la encriptación (ej: Hash).
    e. Función principal para desencriptar.
3. Realice pruebas sobre su sistema de cifrado que permitan evaluar las siguientes características:
    a. Efecto avalancha.
    b. Grafique el *throughput* vs. tamaño del bloque del mensaje para la encriptación.
    c. Grafique el *throughput* vs. tamaño del bloque del mensaje cifrado para la desencriptación.

4. Análisis:
    - ¿Qué ocurriría si se usa una clave incorrecta para desencriptar??
    - ¿Compare las ventajas y/o desventajas de su diseño versus el algoritmo que usó como base?
    - ¿El diseño cumple con el propósito planteado? ¿Por qué?
    - ¿El diseño cumple con el efecto avalancha? Indique en qué parte del código se muestra dicho efecto. Muestre un caso de prueba.
    - ¿Cuál es el Throughput del sistema implementado? ¿Es eficiente?

Informe

Se debe enviar un informe de laboratorio en formato PDF con todo el trabajo realizado y que incluya al menos las siguientes secciones:

- **Introducción** (0.5 - 1.0 página): Contexto, objetivos e información bibliográfica de relevancia (no es necesario repetir información que existe en la bibliografía, pero sí citar y/o sintetizar). *¿Qué se hará y por qué?*
- **Marco Teórico:** Explicaciones básicas sobre todos los temas y tópicos tratados en la actividad.
- **Desarrollo y resultados**: Explicación del trabajo realizado, exponiendo la señal creada originalmente, todas las modulación realizadas y todos los resultados obtenidos. Incluir algoritmos y/o códigos (extractos, resumen), diagramas, imágenes y tablas. *¿Qué se hizo y qué se obtuvo?*
- **Análisis de resultados**: Análisis de cada resultado, está correcto?, por qué salió ese resultado, relacionar resultados con los contenidos del curso. *¿Tienen sentido mis resultados, por qué obtuve estos resultados?*
- **Conclusiones** (0.5 - 1.0 página): Síntesis de los principales resultados encontrados y su relación con los contenidos. Problemas encontrados y cómo fueron solucionados. Conclusiones personales. *¿Qué aprendí con este trabajo*?
- **Bibliografía**: Listado de referencias usadas en el trabajo. Todas!. Libros (indicando capítulos), publicaciones, sitios web y videos (enlace y fecha de última visita), material de clases, etc. Formato APA. *¿Qué fuentes utilicé en este trabajo?*

Se evaluará:

- Manejo de los contenidos, certeza de las aseveraciones.
- Calidad de la información presentada (gráficos, tablas, imágenes).
- Formato y redacción.
- Capacidad de síntesis y claridad.

Código

Se debe adjuntar el código del programa realizado, el cual debe cumplir con los principios de buenas prácticas de programación y documentación. Se evaluará:

- Completitud y correctitud: el código resuelve todo el laboratorio y funciona sin errores.
- Orden y documentación: el código está ordenado, es auto explicativo, presenta comentarios para explicar qué se resuelve en cada paso. (se valora/recomienda programar -funciones, variables- y comentar en inglés)
- Técnicas de programación: adecuado uso de paradigmas de programación (funcional, orientado a objetos, paralelismo, etc), estructura del código (correcto uso de funciones, clases, tipos de datos, estructuras de datos), testeo, documentación.
- Instrucciones de uso del código. Incluya instrucciones en el informe y/o en un archivo README.

Dudas y consultas por correo al ayudante y profesor de cátedra.