Laboratorio 1:
Cifrado simétrico y asimétrico en C++
Redes de Computadores

`Laboratorio de Redes y Ciberseguridad`

June 22, 2025

1 Contexto

Bienvenido al primer laboratorio de Redes de Computadores 2025-1. En esta experiencia práctica nos sumergimos en el universo de la criptografía. Para desarrollar el laboratorio deberán programar en `C++` usando la librería `Cripto++` para trabajar con los algoritmos solicitados. Trabajaremos con cifrado simétrico, usando el algoritmo **AES** (Advanced Encryption Standard) y, con cifrado asimétrico con el algoritmo **RSA** (Rivest, Shamir y Adleman), que conforman los estándares actuales usados en ciberseguridad.

Al completar los ejercicios se les solicita entregar además un informe escrito, desarrollado en LaTeX, contestando a las preguntas. Deben exponer sus resultados (mensajes cifrados o descifrados) e interpretarlos. Basta con destacar las características propias del método de cifrado usado y reflexionar sobre sus implicancias prácticas, fortalezas y debilidades.

Usted forma parte del *Orden de Alejandría*, una sociedad clandestina dedicada a la preservación de la sabiduría de pueblos pasados. La comunicación al interior del Orden es fundamental, sin embargo, es igual de importante conservar la clandestinidad.

Con el objetivo de conservar el secreto de las comunicaciones al interior del Orden se han empleado diversas técnicas de criptografía. Su tarea es analizar e implementar algunas de estas técnicas.

Objetivos de la experiencia:

- Comprender los principios y casos de uso de cifrado simétrico y asimétrico.
- Utilizar la librería `Crypto++` para cifrado y descifrado de mensajes.
- Familiarizarse con los algoritmos de cifrado AES y RSA.

2 Cifrado Simétrico

Elara desea enviar un mensaje confidencial a Teo, han acordado un clave secreta previamente al intercambio. Su tarea es cifrar el mensaje usando `AES`.

Mensaje Secreto

La cámara descansa bajo el sauce llorón en el jardín del martillo.

Clave Secreta Acordada

6F708192 A3B4C5D6 E7F8A2 ROLUSM

Donde deben reemplazar ROLUSM con el ROL de algún integrante de su grupo para los últimos 10 dígitos de la clave. Deben indicar cual es el ROL que utilizaron.

Observacion: Deben convertir la clave a binario.

3 Cifrado Asimétrico

La Hermana Lyra necesita su ayuda para enviar un documento sensible al Gran Maestro. Este documento solo debe ser legible por el Gran Maestro. Usted solo tiene acceso a la clave pública del Gran Maestro (archivo adjunto `gm_publica.pem`).

Mensaje Secreto

Los archivos antiguos, código MPSH476, revelan la ubicación del séptimo pergamino perdido.

Debe cifrar el mensaje y detallar instrucciones, tales que, al recibir el mensaje cifrado y las instrucciones el Gran Maestro tiene garantizado que:

1. El mensaje proviene de la Hermana Lyra.
2. Solo el Gran Maestro puede leer el mensaje.
3. Si alguién interceptó el mensaje no pudo obtener información acerca del emisor ni el receptor.

En caso de generar algún par clave pública/clave privada debe incluirlas en su entrega final y explicar el uso que le debemos dar. Puede generar las claves usando `openssl`.

4 Canal Seguro

Para mantener comunicaciones seguras dentro del Orden de Alejandría se debe crear un canal seguro. Particularmente para las comunicaciones entre el Gran Maestro y el Honorable Pedrius Godoyius. Proponga e implemente una estrategia para establecer un canal seguro de comunicaciones eficiente entre estos personajes. Debe utilizar los algoritmos que utilizó en las secciones anteriores y simular una interacción simple para verificar su solución.

5 Condiciones de entrega

- La entrega del laboratorio será de forma grupal, en el buzón de entrega del Moodle del laboratorio.
- La fecha de entrega es a las 23:55 del día 27/06/2025.
- Deberá entregar un informe, detallando el procedimiento seguido y los conceptos aplicados, no se extiendan demasiado.
- El código deberá estar comentado y bien estructurado.
- Se deben entregar las claves usadas durante la experiencia,
- El código, informe y las claves deben estra en un comprimido tipo tar.gz con el nombre Lab_1_GrupoX
- Parte de la evaluación del laboratorio será en una defensa oral de la entrega
- Se descontará 10 puntos por hora de atraso.