Documentación Image Lockdown

Introducción

En las últimas dos semanas, nuestro equipo se ha enfocado en desarrollar una solución que permita la encriptación y desencriptación de imágenes satelitales, garantizando una transmisión segura y eficiente. Este informe detalla el proceso seguido, las herramientas utilizadas, la solución implementada y los resultados obtenidos.

Herramientas Utilizadas

Para abordar el problema, recurrimos a diversas herramientas que facilitaron el desarrollo y optimización de nuestra solución. A continuación, se describen las principales herramientas empleadas:

OpenSSL

Utilizamos OpenSSL y su documentación extensiva para implementar los algoritmos de cifrado y descifrado. Esta herramienta nos proporcionó las librerías necesarias para trabajar con criptografía de alto nivel.

Valgrind

Valgrind fue crucial para detectar y corregir fugas de memoria en nuestro código. Gracias a esta herramienta, podemos asegurar una gestión eficiente de los recursos de memoria, evitando posibles errores y optimizando el rendimiento.

Comando `time` de Unix

Empleamos el comando `time` de Unix para medir el tiempo de ejecución de nuestras funciones. Esto nos permitió realizar pruebas de rendimiento y ajustar nuestro código para mejorar la eficiencia.

gdb

Utilizamos gdb como depurador para identificar y eliminar bugs en nuestras funciones. Con esta herramienta, pudimos optimizar el código y asegurar su estabilidad y fiabilidad.

Explicación de la Solución

Tipo de Cifrado y Llaves Dinámicas

Nuestra solución se basa en un algoritmo de cifrado híbrido que combina AES-CTR-256 y RSA. El proceso de cifrado y descifrado se realiza de la siguiente manera:

1. Generación de Llave AES Aleatoria: El satélite genera una llave simétrica AES aleatoria.
2. Cifrado de la Imagen: La imagen satelital se cifra utilizando la llave AES generada.
3. Cifrado de la Llave AES: La llave AES se cifra utilizando la llave pública RSA, que se almacena en el satélite.
4. Transmisión de Datos: La imagen cifrada junto con la llave AES cifrada se envían a la base terrestre.
5. Descifrado en la Base Terrestre: En la base, se utiliza la llave privada RSA para descifrar la llave AES. Luego, se utiliza esta llave AES para descifrar la imagen satelital.

Este enfoque asegura que incluso si la transmisión es interceptada, la imagen no pueda ser descifrada sin la llave privada RSA, garantizando así la seguridad de los datos.

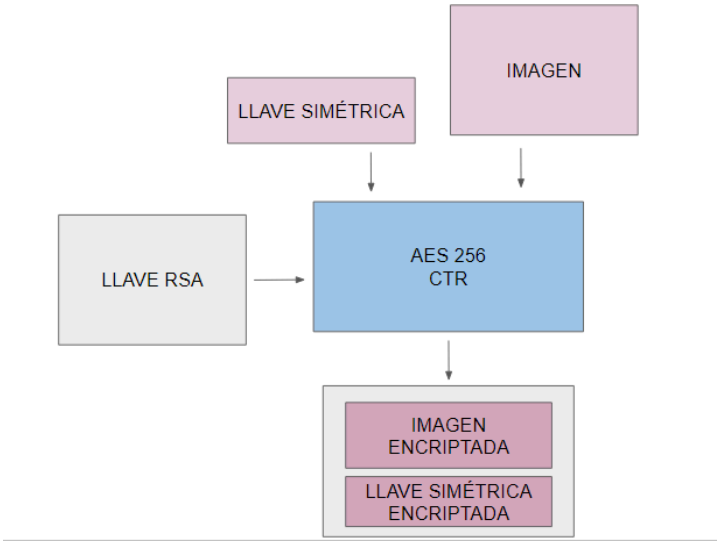

Figura 1. Encriptación de la imagen

Uso del Buffer y Pre-asignación de Memoria

Para manejar archivos grandes y evitar problemas de memoria, implementamos un buffer de 1MB. El código obtiene el tamaño del archivo y pre-asigna la memoria necesaria. Esta técnica reduce significativamente el tiempo de ejecución y asegura la eficiencia del programa, evitando sobrecargas y mejorando el rendimiento en sistemas con recursos limitados.

Tests Llevados a Cabo y Manejo de Errores

Verificación del algoritmo

Para verificar la efectividad de nuestras funciones, utilizamos el algoritmo **MD5** para comparar la imagen de entrada con la imagen desencriptada. Este enfoque nos permitió verificar la integridad de los datos sin necesidad de revisiones visuales. Al comparar los códigos MD5 generados, pudimos confirmar que la imagen desencriptada era idéntica a la original, asegurando así el correcto funcionamiento de nuestro sistema.

Conclusión

En conclusión, hemos desarrollado una solución eficiente y segura para la encriptación y desencriptación de imágenes satelitales. Utilizando herramientas como OpenSSL, Valgrind, el comando `time` de Unix y gdb, pudimos crear un sistema robusto que garantiza la integridad y seguridad de los datos transmitidos. Estamos ansiosos por recibir su feedback y responder cualquier pregunta que puedan tener.

Referencias

https://www.openssl.org
https://www.geeksforgeeks.org/rsa-algorithm-cryptography/?ref=gcse_ind
https://www.tutorialspoint.com/advanced-encryption-standard-aes