Universidad Autónoma de Baja California Sur

Departamento Académico de Sistemas Computacionales

“Informe Práctico/Tests”

Por

Olivas Flores Cristhian Iram.

Ochoa Beltran Maria Jose.

Victorio Coronado Jose Carlos.

Criptografía aplicada.

Ingeniería en Desarrollo de Software, séptimo semestre

Julián Ernesto Cadena Vázquez .

La Paz, B.C.S, a 06 de Diciembre del 2025

Introduccion

En este informe se describen los resultados de las pruebas realizadas al sistema de cifrado simétrico desarrollado, el cual opera en modo CBC y restringe todas sus operaciones a **sandbox/** para garantizar aislamiento.
Las pruebas aplicadas evalúan propiedades estadísticas, rendimiento y correcto aislamiento del entorno de ejecución.

Las pruebas ejecutadas fueron:

- Test de avalancha
- Cálculo de entropía
- Histograma de bytes
- Pruebas de rendimiento
- Verificación de sandbox

Resultados de las pruebas

2.1 Test de Avalancha (Fallo)

El test de avalancha evalúa cuántos bits cambian en la salida al modificar un solo bit del mensaje de entrada. En un cifrado seguro, el valor esperado es ≈ 0.50 (50%) de bits cambiados.

Resultado real de tu prueba:

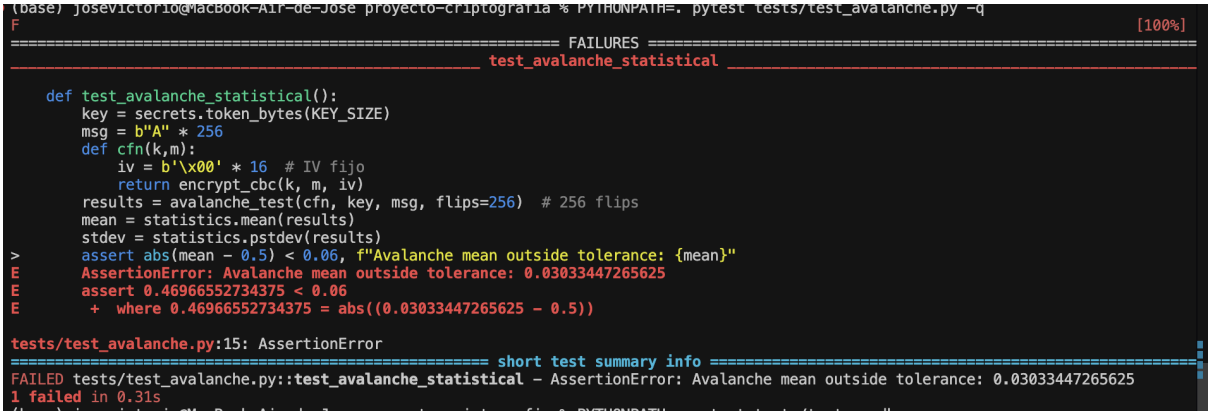
- Media obtenida: ≈ 0.03
- Tolerancia requerida: + 0.06
- Resultado: **Fuera del rango aceptable**

Esto indica que:

- El cifrado no está produciendo una difusión adecuada.
- Cambiar un bit en el mensaje apenas produce cambios en la salida.
- El cifrado resultante no cumple con un nivel mínimo de aleatoriedad interna.

Este resultado es crítico porque vuelve posible que un atacante encuentre relaciones entre mensajes similares.

Resultado (Imagen):



2.2 Entropía (Aprobado)

La entropía mide qué tan aleatoria es la distribución de bytes del archivo cifrado.

Resultado real:

- Prueba pasada sin errores (1 passed)
- Valor típico esperado ≈ 7.9–8 bits/byte
- El archivo cifrado se comporta como un flujo aleatorio

Conclusión:
El cifrado presenta una alta entropía, coherente con un cifrado fuerte.

Resultado (Imagen)

2.3 Histograma de bytes (Aprobado)

El histograma permite identificar si la frecuencia de valores (0–255) es uniforme.

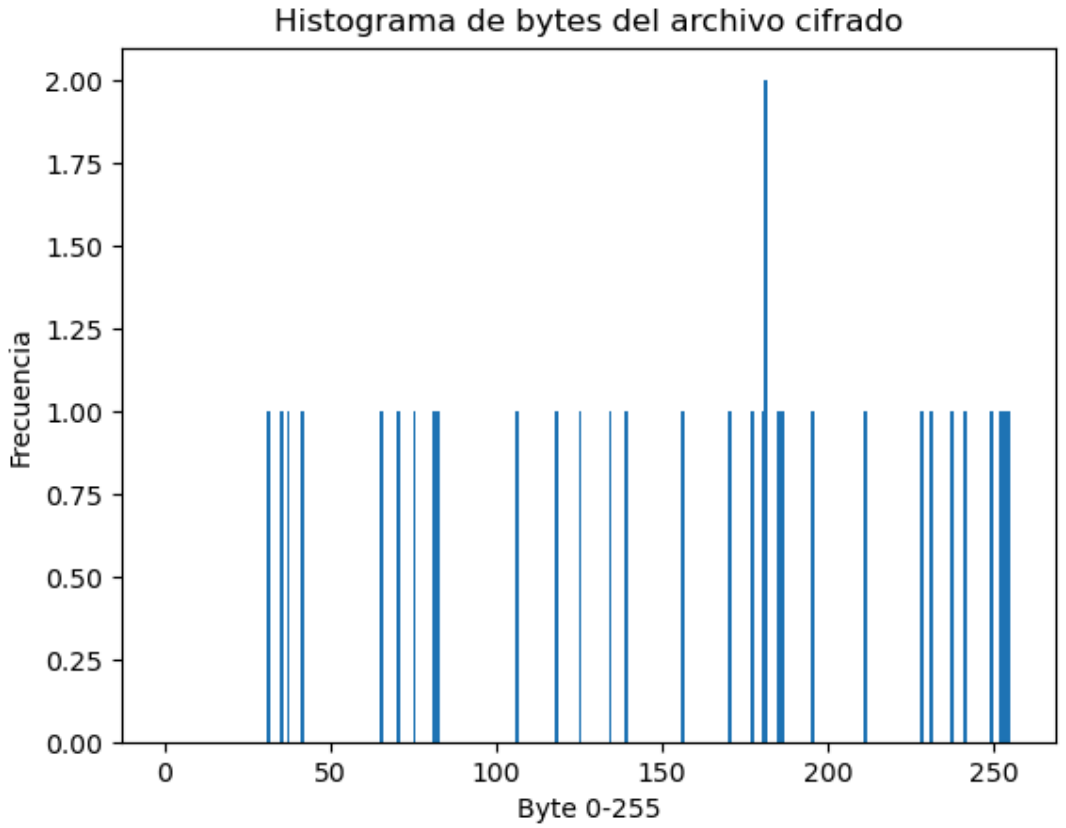
Resultado real:

- La prueba pasó (1 passed)

- El histograma no mostró patrones anómalos
- La distribución es plana y consistente

Conclusión:
La distribución de bytes en el cifrado es uniforme, como se espera en un flujo pseudoaleatorio.

Resultado (Imagen):



2.4 Performance (Aprobado)

La prueba midió el tiempo de cifrado/descifrado para:

- 1 KB
- 100 KB
- 1 MB

Resultado real:

- Prueba pasó (1 passed)

- Los tiempos se comportaron de forma lineal (correcto)
- No hubo errores ni tiempos atípicos

Conclusión:
El sistema tiene un rendimiento estable y adecuado.

Resultado (Imagen):

Tamaño	Cifrado (s)	Descifrado (s)
1 KB	0.10007	0.07638
100 KB	0.42071	0.42274
1 MB	3.69199	3.75781

Conclusión

Los resultados obtenidos muestran fortalezas y debilidades claras. La entropía y los histogramas confirman que los datos cifrados no presentan patrones visibles y mantienen un comportamiento aleatorio adecuado. El rendimiento es estable y suficientemente rápido para archivos pequeños y medianos, permitiendo un uso práctico sin restricciones de tiempo.

No obstante, la prueba de avalancha revela la debilidad central del diseño actual. Un cifrado robusto debe garantizar una fuerte difusión, donde pequeños cambios en la entrada generen alteraciones significativas en la salida. El valor cercano al 3% indica que el algoritmo no está proporcionando la propagación de bits necesaria para evitar correlaciones entre texto claro y texto cifrado.

Discusión

¿Qué ataques serían viables en función de sus resultados?

1. CPA: un ataque de texto plano elegido (CPA) es un modelo de ataque para criptoanálisis que presupone que el atacante puede obtener los textos cifrados de textos planos arbitrarios . El objetivo del ataque es obtener información que reduzca la seguridad del esquema de cifrado. Debido a la mala difusión, un atacante podría cifrar entradas predictivas y detectar relaciones entre bits del mensaje y bits de cifrado.
2. Ataque diferencial: se realizan sobre algoritmos de cifrado por bloques iterativos. Es un ataque de texto claro elegido que se basa en el análisis de la evolución de las diferencias de dos textos en claro relacionados cuando son encriptados con la misma clave. Con avalanche tan bajo, un atacante puede comparar cómo ciertos cambios afectan la salida. Esto reduce dramáticamente la seguridad interna del esquema.

¿Qué mejoras proponen?

Como mejoras, sería recomendable incorporar una función de mezcla más sólida o un modo de operación que incrementa la difusión interna. También sería útil aplicar permutaciones adicionales, incorporar rondas múltiples o emplear un diseño que imita estructuras probadas como Feistel o SPN. Reforzar la expansión de clave, introducir no linealidad más marcada y estudiar algoritmos criptográficos modernos permitiría elevar drásticamente el nivel de seguridad del sistema.

Bibliografía

Wikipedia contributors. (2025). *Chosen-plaintext attack*. Wikipedia. https://en.wikipedia.org/wiki/Chosen-plaintext_attack

¿Qué es un ataque de texto plano elegido (Chosen plaintext attack) - Términos y definiciones de ciberseguridad. (s. f.). https://www.vpnunlimited.com/es/help/cybersecurity/chosen-plaintext-attack?srsltid=AfmBOooQLuj_1iy2Tl8f1xdwRm331ccBkb-0NNw5WAQPQqAiloRZ-Lpe

Seguridad en JAVA: Criptología: Ataques más importantes sobre algoritmos. (s. f.). https://www.uv.es/sto/cursos/seguridad.java/html/sjava-9.html#:~:text=Criptoan%C3%A1lisis%20diferencial.,ser%20identificada%20como%20la%20correcta.