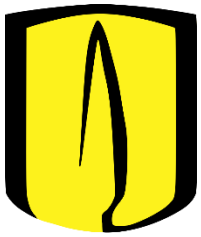
Caso de estudio 3 – Canales seguros

Sistema de rastreo de paquetes en una compañía transportadora



Infraestructura Computacional

Andrés Felipe Charry Camacho - 202214507

Andrés Botero Ruiz - 202223503

Introducción:

En este caso de estudio, desarrollamos un prototipo de comunicación segura entre un cliente y un servidor, para una aerolínea que ofrece servicios de consulta en línea. El principal objetivo es implementar mecanismos de cifrado y validación de datos que garanticen tanto la confidencialidad como la integridad de la información que se transmite durante las sesiones.

Para lograrlo, se construyeron dos programas, uno que actúa como servidor principal y otro como cliente. Ambos deben ser capaces de establecer una conexión segura usando algoritmos de criptografía estándar, como AES, RSA, Diffie-Hellman, HMAC y firmas digitales. Además de la implementación, el proyecto busca medir el desempeño de las operaciones criptográficas en diferentes escenarios, evaluando aspectos como el tiempo de cifrado, firmado y verificación de datos.

Resultados de desempeño y análisis

Tiempos de firma:

Tiempos de cifrado:

Para analizar el desempeño del proceso de cifrado, se midió el tiempo que tarda el servidor en cifrar la tabla de servicios utilizando cifrado simétrico (AES) en los dos escenarios propuestos. Para cada medición reportada, se realizó el escenario cuatro veces y se tomó el promedio de los resultados obtenidos.

Escenario	Conexiones	Tiempo 1	Tiempo 2	Tiempo 3	Tiempo 4	Tiempo promedio de cifrado (ns)
1	1	16178,125	15968,75	16009,375	15871,875	16007,03
2	4	47150	37825	37725	35775	39618,75
2	16	31137,5	31525	32725	26475	30465,63
2	32	25553,125	26862,5	28668,75	33706,25	28697,66
2	64	23642,1875	24114,0625	25320,3125	12855864,0625	3232235,16

Análisis:

Después de realizar nuevamente las mediciones de los tiempos de cifrado simétrico (AES) en los distintos escenarios, obtuvimos los promedios que se presentan en la tabla anterior.

- En el escenario 1, donde solo un cliente realizaba consultas de manera iterativa, los tiempos de cifrado fueron bastante bajos y estables, con un promedio alrededor de 16.000 ns, tal como se esperaba dado que no había competencia por recursos.

- En el escenario 2, con múltiples clientes concurrentes, se observó que para 4, 16 y 32 conexiones los tiempos aumentaron ligeramente respecto al caso iterativo, aunque siguieron estando en un rango muy manejable, mostrando la buena eficiencia de AES incluso con concurrencia moderada. Sin embargo, cuando se alcanzaron 64 conexiones simultáneas, el tiempo promedio de cifrado aumentó de manera muy significativa. Esto evidencia que, a partir de cierto punto, el servidor comienza a saturarse, afectando el desempeño del cifrado debido a la alta carga de procesamiento. Este comportamiento era esperado en escenarios de alta concurrencia, donde la infraestructura empieza a ser un cuello de botella cuando la cantidad de solicitudes aumenta drásticamente.

Tiempos de verificación:

Comparación de cifrado (tabla de servicios) simétrico y asimétrico

Para evaluar la diferencia de desempeño entre cifrado simétrico (AES) y cifrado asimétrico (RSA), se midieron los tiempos que tarda el servidor en cifrar la tabla de servicios usando cada uno de los métodos. Las mediciones se realizaron bajo las mismas condiciones de prueba que los escenarios anteriores, y se calculó el promedio de cuatro ejecuciones.

Escenario	Conexiones	Tiempo 1	Tiempo 2	Tiempo 3	Tiempo 4	Tiempo promedio de cifrado (ns)
1 Simétrico (AES)	1	15953,125	14731,25	19903,125	16237,5	16237,5
1 Asimétrico (RSA)	1	35362,5	33284,375	35512,5	31675	33958,59375
2 Simétrico (AES)	4	58275	81375	34300	54475	57106,25
2 Asimétrico (RSA)	4	62250	92275	79375	89850	80937,5

2 Simétrico (AES)	16	30337,5	37993,75	26562,5	24237,5	29782,8125
2 Asimétrico (RSA)	16	61193,75	80731,25	84187,5	69650	73940,625
2 Simétrico (AES)	32	23728,125	36006,25	42781,25	25659,375	32043,75
2 Asimétrico (RSA)	32	879315,625	73775	66031,25	88831,25	276988,28
2 Simétrico (AES)	64	47170,3125	25892,1875	38309,375	26004,6875	34344,141
2 Asimétrico (RSA)	64	86342,1875	61545,3125	910734,375	71145,3125	282441,797

Análisis:

Después de realizar las mediciones de los tiempos de cifrado simétrico (AES) y asimétrico (RSA) en los diferentes escenarios evaluados, se obtuvieron los promedios mostrados en la tabla anterior.

- En el escenario 1 (iterativo), donde solo había una conexión activa a la vez, el cifrado simétrico presentó tiempos considerablemente más bajos que el asimétrico, lo cual es consistente con las propiedades esperadas de ambos tipos de cifrado. Además, los valores registrados fueron estables, evidenciando un comportamiento predecible bajo baja carga.

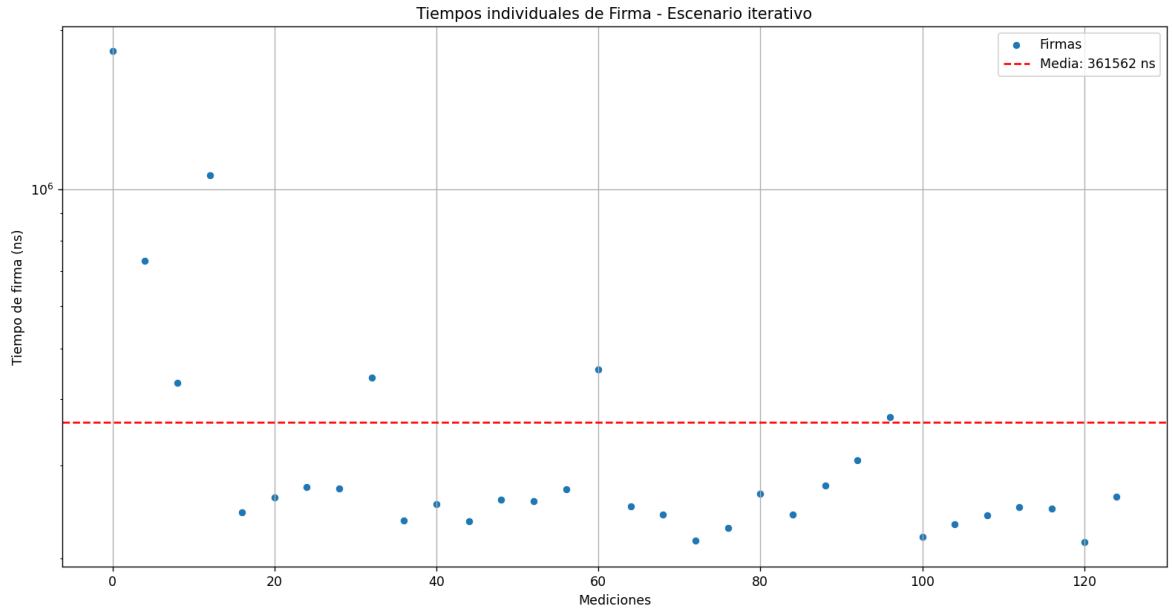
- En los escenarios con concurrencia (4, 16, 32 y 64 conexiones), el cifrado simétrico continuó mostrando mejores tiempos promedio en comparación con el asimétrico. Sin embargo, a medida que aumentaba el número de conexiones, se evidenció una mayor variabilidad en los tiempos de cifrado, especialmente en el caso de RSA. En particular, para los escenarios de 32 y 64 conexiones, se presentaron valores atípicos en los tiempos de cifrado asimétrico, con mediciones que superaron significativamente los valores promedio.

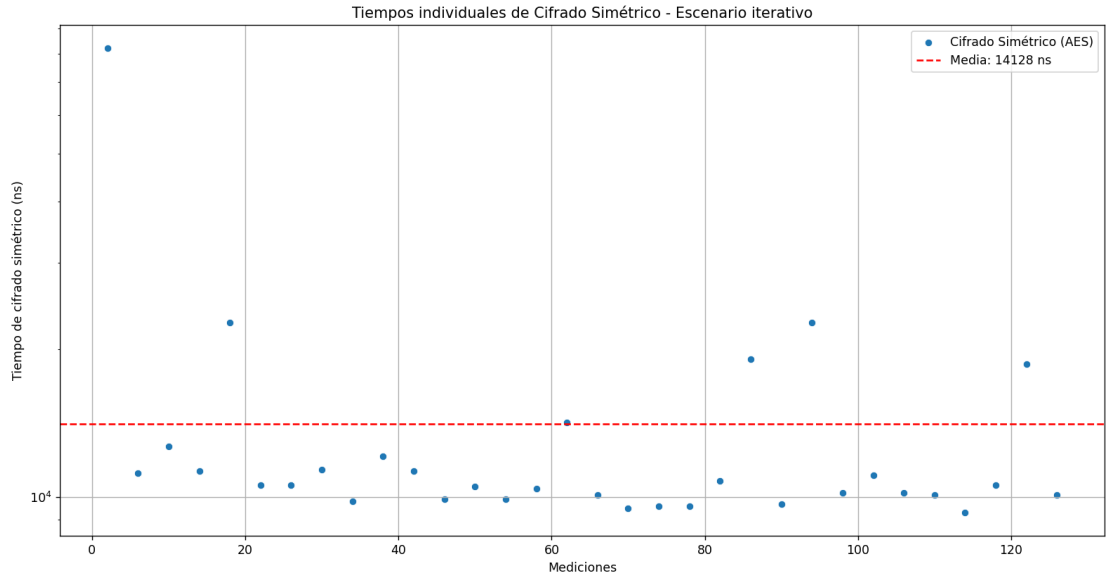
Este comportamiento era esperado, dado que el cifrado asimétrico, por su naturaleza, implica operaciones matemáticas más complejas que son más sensibles al aumento de la carga. Por otro lado, el cifrado simétrico, siendo más ligero computacionalmente, demostró mayor estabilidad y mejor tratamiento al incremento de la concurrencia.

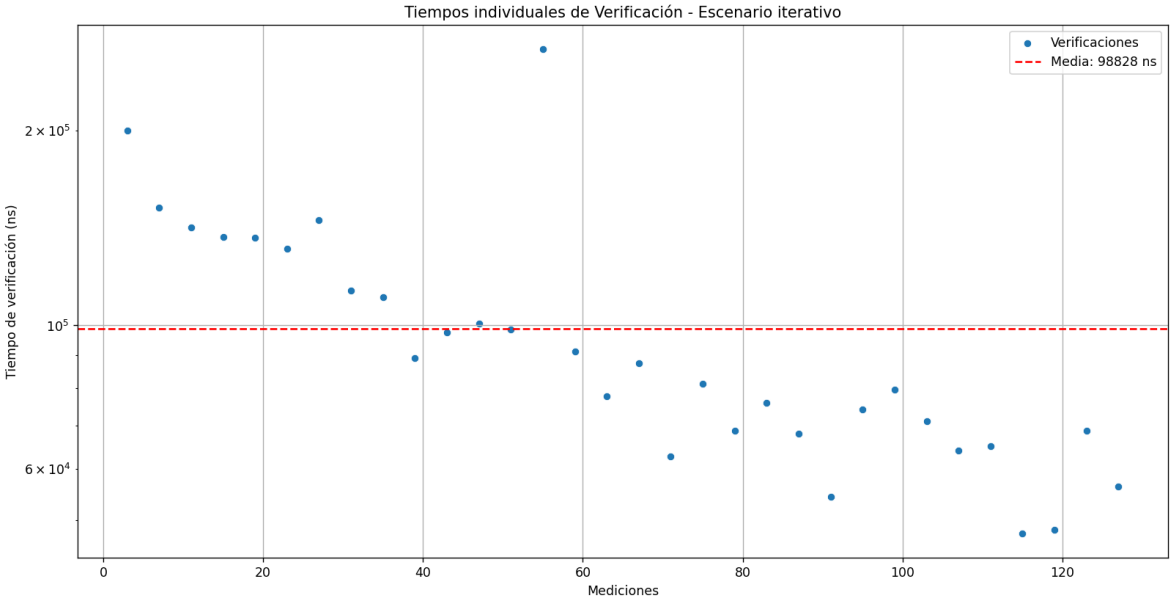
Graficas propuestas

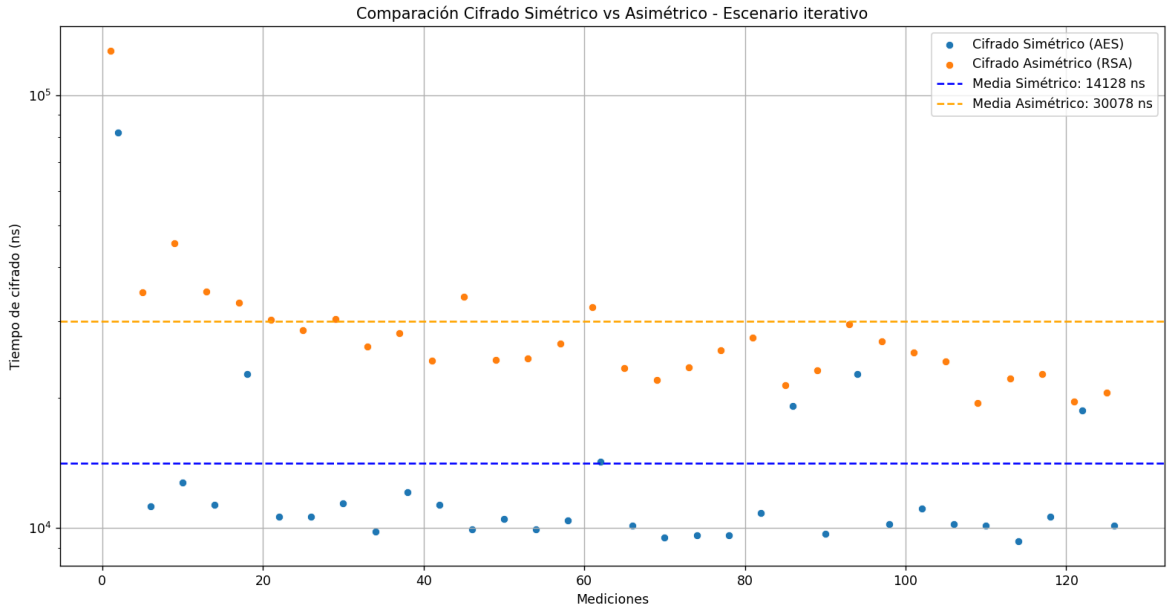
Para analizar el comportamiento de los tiempos de ejecución en los diferentes escenarios, se realizaron varias gráficas que permiten visualizar mejor los resultados obtenidos. Dado que los tiempos medidos se encuentran en nanosegundos y presentan valores relativamente grandes, se optó por utilizar una escala logarítmica en el eje vertical para facilitar la comparación entre las diferentes acciones y escenarios. Las gráficas incluyen mediciones individuales junto con la media correspondiente para cada acción, permitiendo identificar patrones de estabilidad o variabilidad en los datos. Además, se emplearon diagramas de caja para observar la distribución general de los tiempos y detectar posibles valores atípicos. De esta forma, se puede entender de manera más clara el impacto que tiene el número de conexiones concurrentes o iterativas sobre el desempeño del servidor.

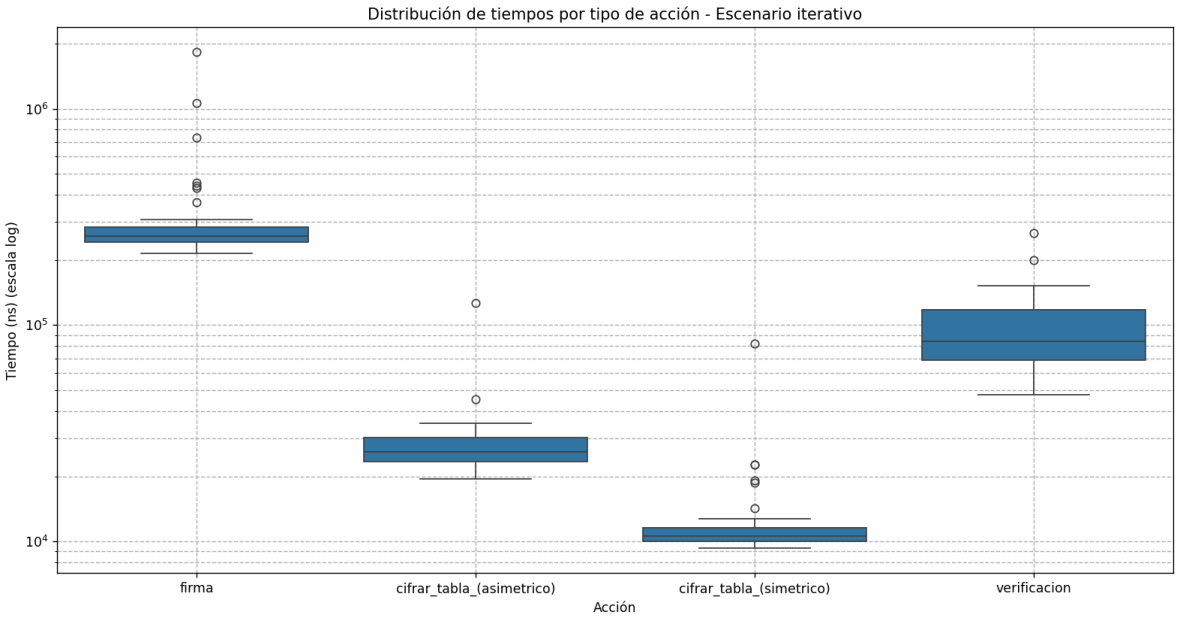
Gráficas escenario 1:




Tiempos individuales de Cifrado Simétrico - Escenario iterativo
Cifrado Simétrico (AES)
Media: 14128 ns
Tiempo de cifrado simétrico (ns)
10^4
0
20
40
60
80
100
120
Mediciones


Tiempos individuales de Verificación - Escenario iterativo
Verificaciones
Media: 98828 ns
Tiempo de verificación (ns)
2×10^5
10^5
6×10^4
0
20
40
60
80
100
120
Mediciones





Análisis de gráficas del escenario 1:

En el escenario iterativo, los tiempos de firma muestran un comportamiento bastante estable, con la mayoría de las mediciones por debajo de la media de 361562 ns. Aunque se presentaron algunas anomalías puntuales por encima de este valor, en general los resultados fueron consistentes, como era de esperarse al manejar solo una conexión a la vez, sin presencia de concurrencia ni sobrecarga en el servidor.

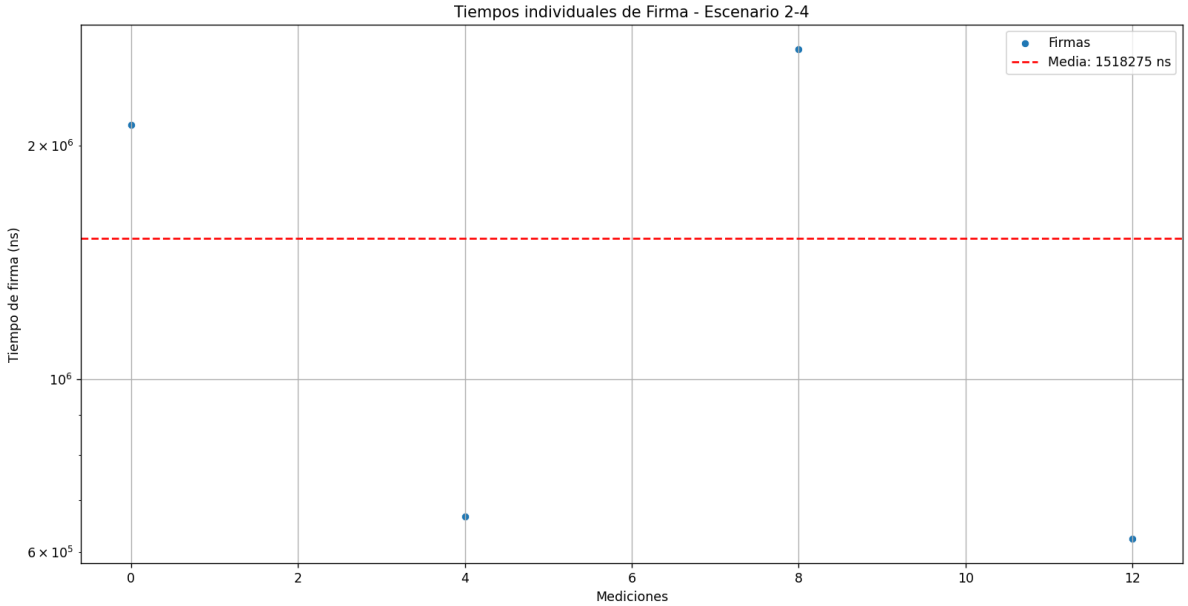
En el cifrado simétrico, los tiempos se mantuvieron muy estables, con una media de 14128 ns. Las mediciones se encuentran bastante próximas a este promedio, y se registraron muy pocos valores atípicos, lo que confirma que el proceso de cifrado no se ve afectado cuando el servidor atiende solicitudes de manera secuencial.

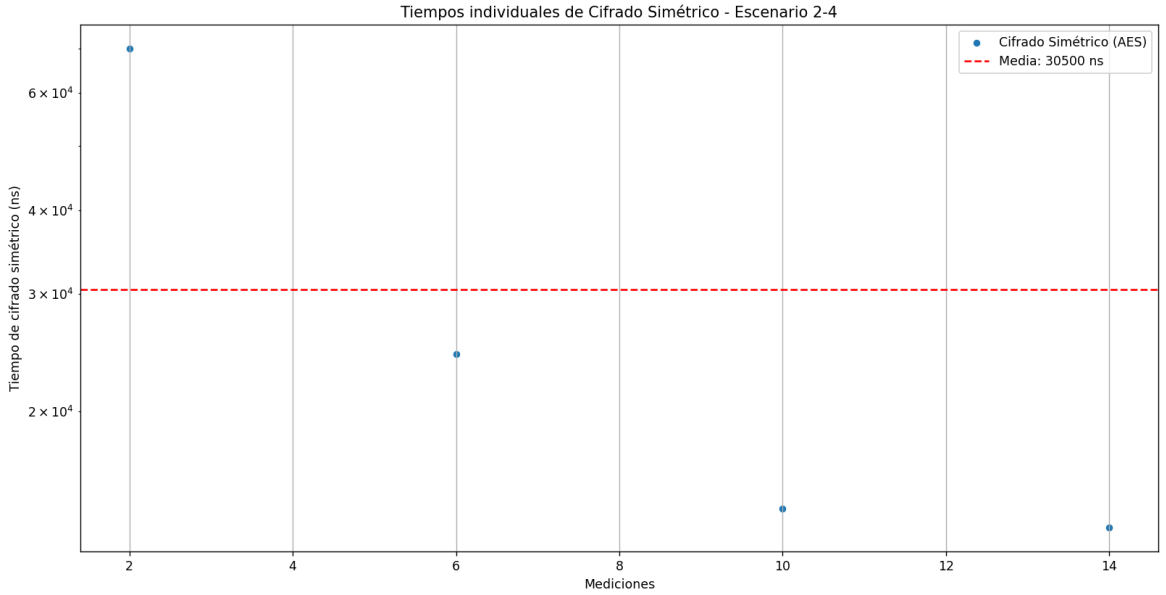
En el caso de la verificación, el comportamiento fue algo más disperso. Aunque la media fue 98828 ns, los valores oscilaron tanto por encima como por debajo de esta cifra, reflejando una mayor variabilidad en los tiempos de validación de los HMAC. Aun así, los tiempos no mostraron desviaciones extremas y se mantuvieron dentro de un rango aceptable.

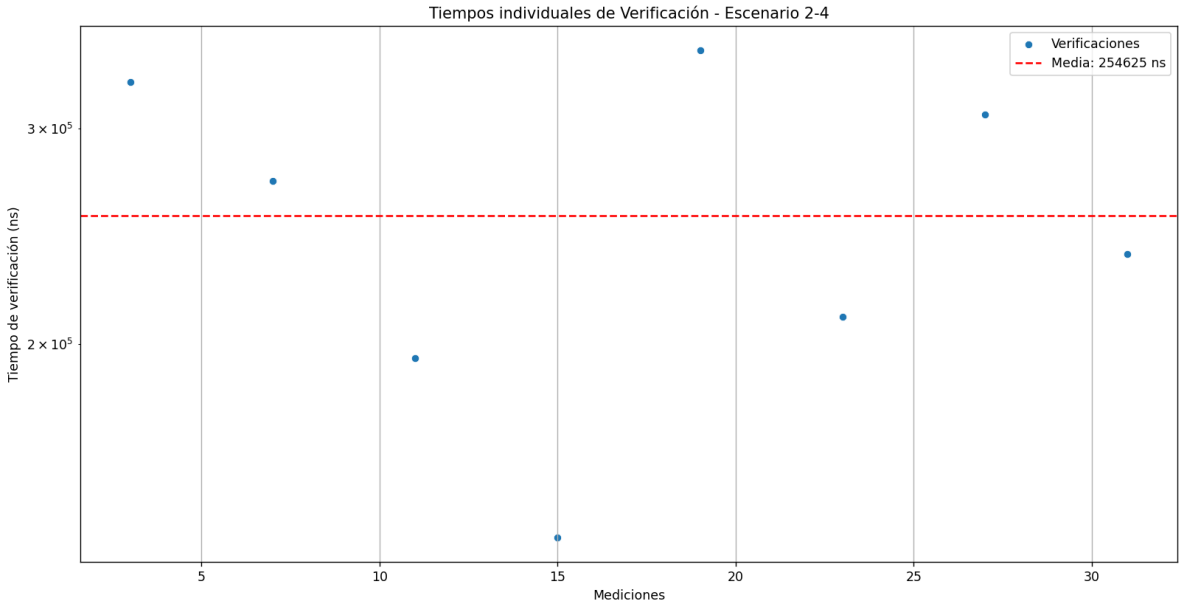
Al comparar los tiempos de cifrado simétrico y asimétrico, se observa que el cifrado asimétrico resultó ser más costoso en casi todas las mediciones, como era de esperarse dada la complejidad de las operaciones RSA frente a AES. Ambos tipos de cifrado presentaron un comportamiento relativamente estable alrededor de sus respectivas medias, aunque el cifrado simétrico mostró una mayor concentración de valores cercanos al promedio, mientras que el asimétrico presentó una dispersión un poco mayor.

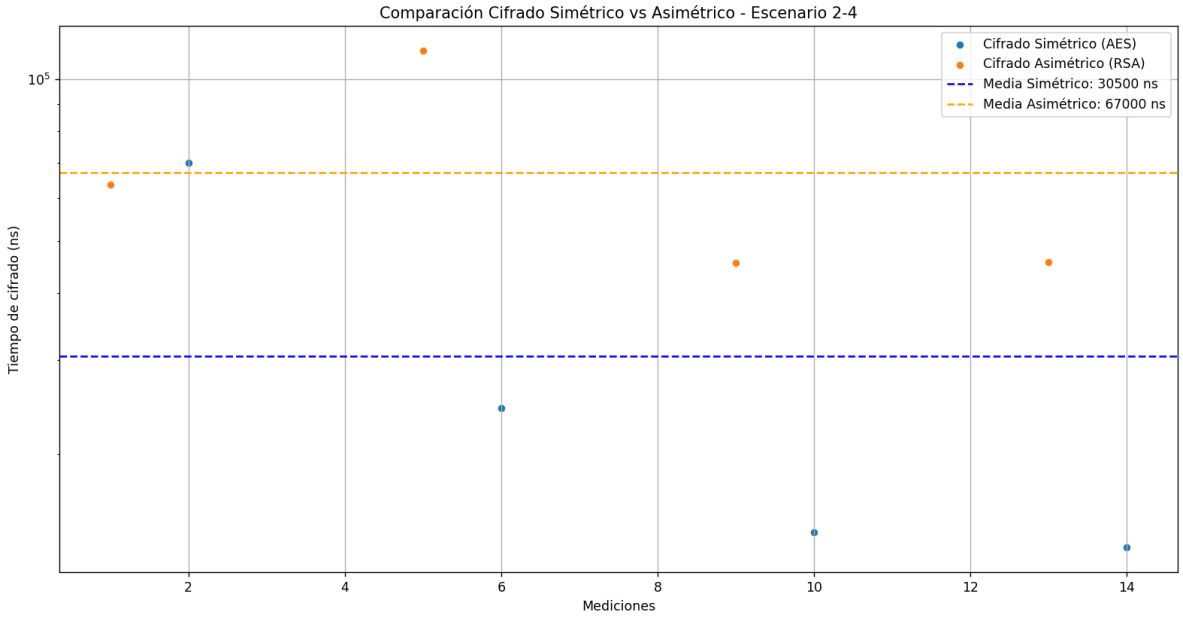
Finalmente, en el diagrama de caja se aprecia que la operación de firma es la más costosa en tiempo, seguida por el cifrado asimétrico, luego el cifrado simétrico y finalmente la verificación.

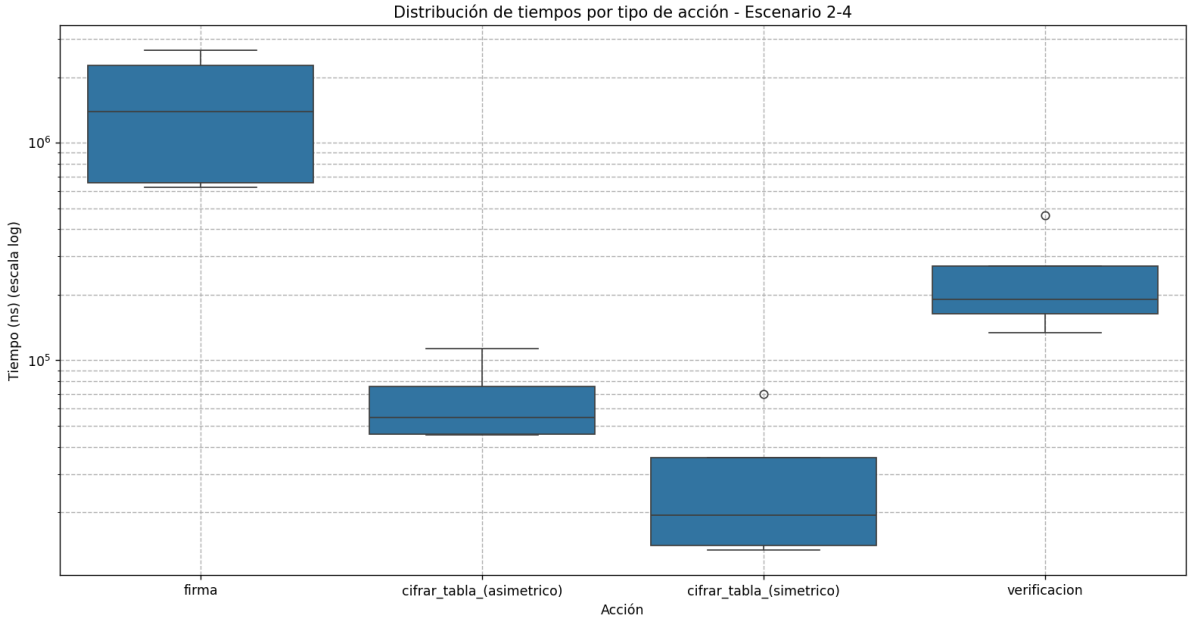
Graficas escenario 2 – 4 conexiones:




Tiempos individuales de Cifrado Simétrico - Escenario 2-4
Cifrado Simétrico (AES)
Media: 30500 ns
Tiempo de cifrado simétrico (ns)
6×10^4
4×10^4
3×10^4
2×10^4
2
4
6
8
10
12
14
Mediciones


Tiempos individuales de Verificación - Escenario 2-4
Verificaciones
Media: 254625 ns
Tiempo de verificación (ns)
3×10^5
2×10^5
5
10
15
20
25
30
Mediciones





Análisis:

En el escenario de 4 conexiones concurrentes, los tiempos de firma mostraron un comportamiento bastante estable, con la mayoría de las mediciones por debajo de la media de 1518275 ns y solo algunas puntualmente por encima. A pesar del aumento en la cantidad de solicitudes simultáneas, el servidor pudo mantener tiempos de firma razonablemente consistentes, sin variaciones extremas.

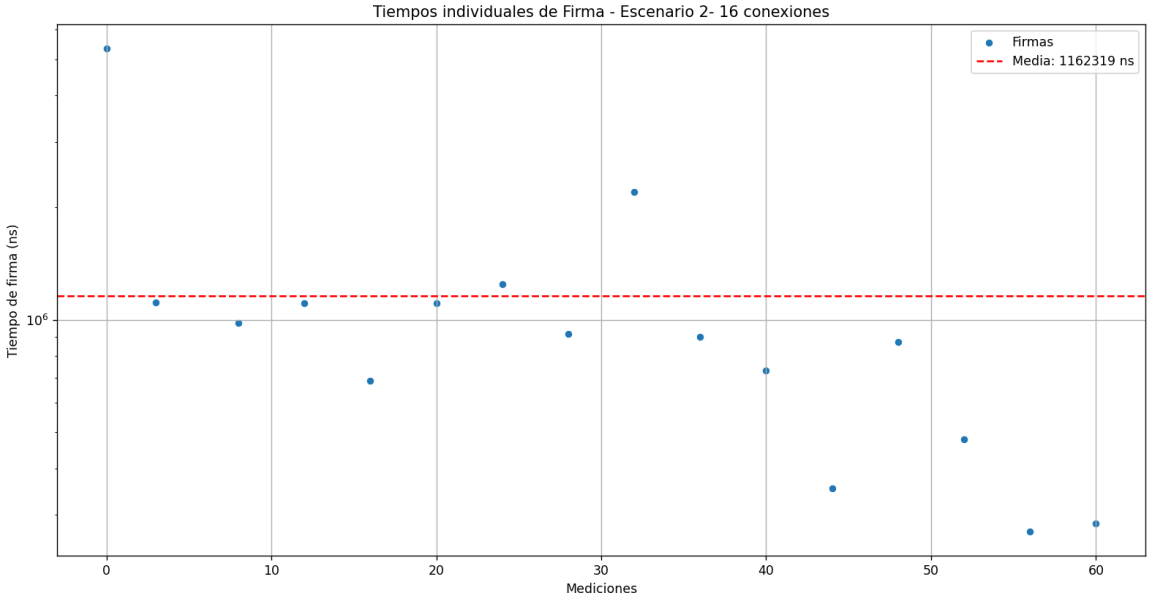
Para el cifrado simétrico, se observó que tres de las mediciones se ubicaron por debajo de la media de 30500 ns y solo una ligeramente por encima. Este comportamiento evidencia una buena estabilidad en el proceso de cifrado, aunque los tiempos fueron un poco mayores en comparación con el escenario iterativo, como era de esperarse debido a la presencia de concurrencia.

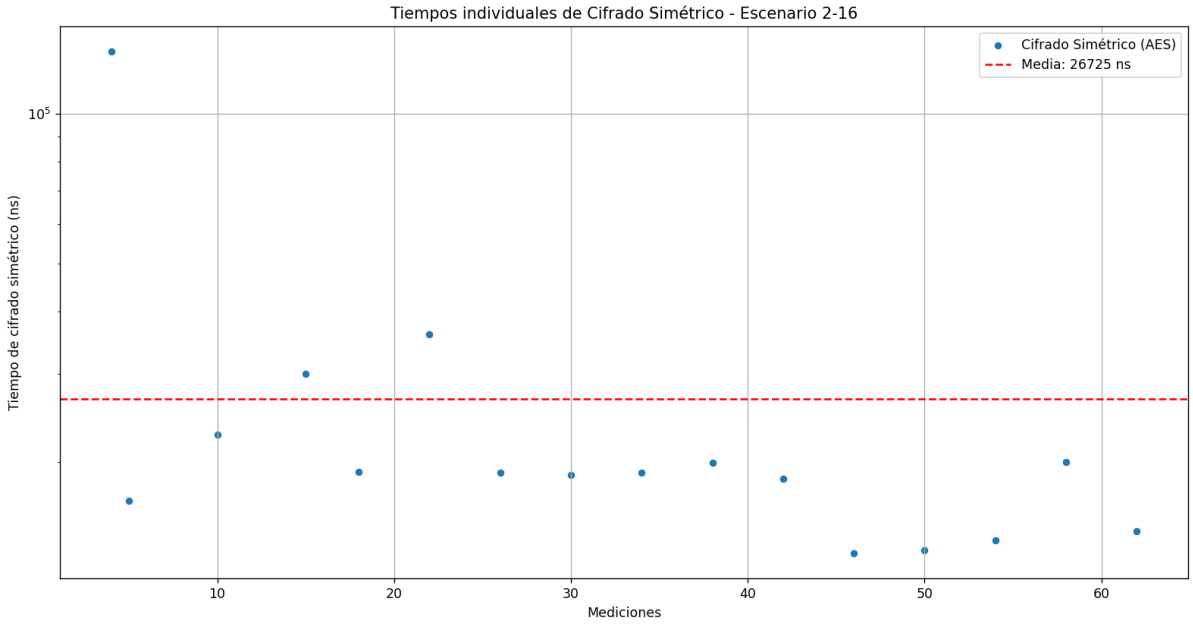
En el caso de la verificación, los tiempos se distribuyeron de manera relativamente equilibrada alrededor de la media de 254625 ns. Aunque hubo una ligera dispersión en los valores, el proceso de validación de HMACs continuó siendo eficiente y no mostró grandes variaciones bajo esta carga moderada.

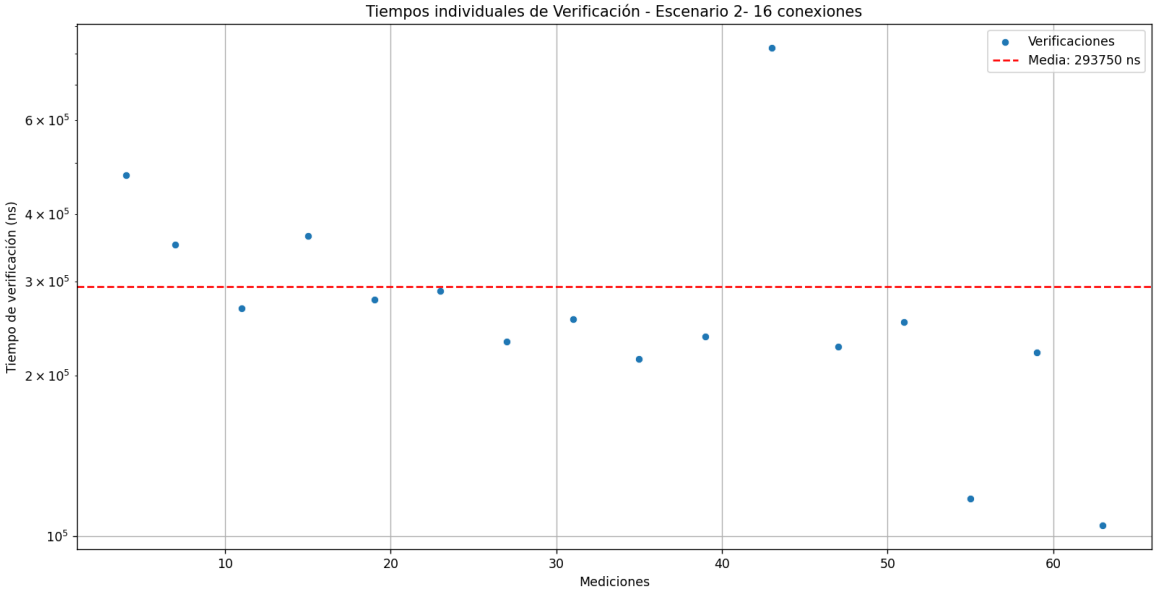
Comparando el cifrado simétrico y el asimétrico, se identificó que el tiempo promedio del cifrado asimétrico fue mayor. El cifrado simétrico mantuvo sus mediciones bastante cercanas entre sí, mientras que el cifrado asimétrico mostró una mayor estabilidad alrededor de su media, aunque con tiempos más altos en promedio. Esto era de esperarse, dado que las operaciones asimétricas suelen ser más costosas computacionalmente, y la presencia de múltiples conexiones incrementa aún más su impacto.

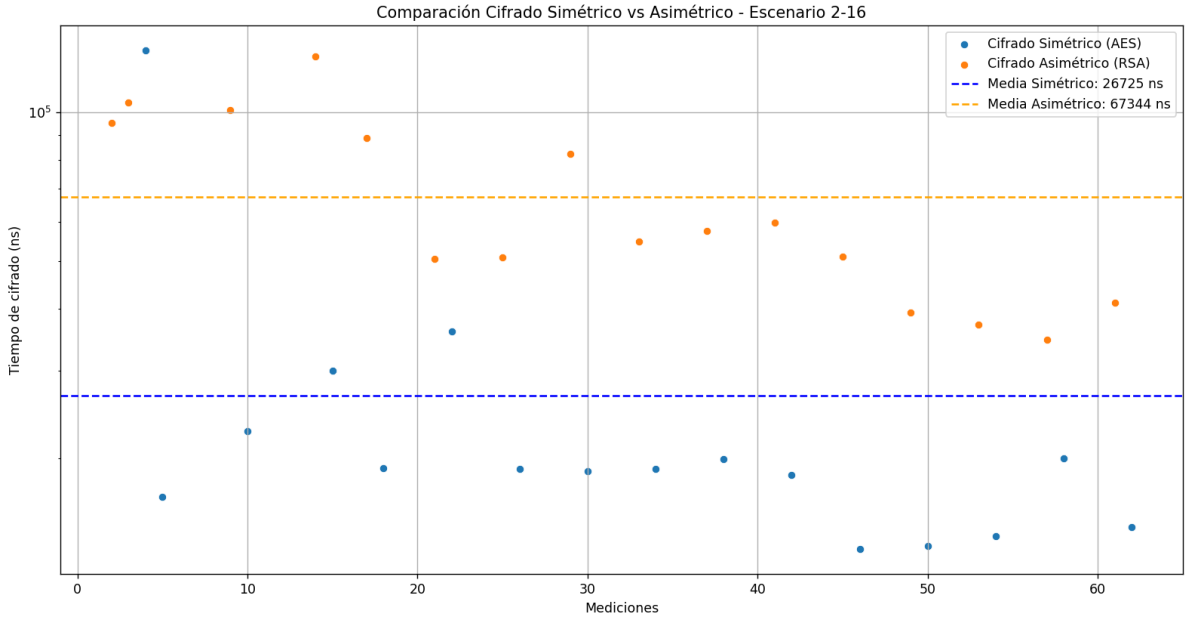
En cuanto al orden de duración de las operaciones, firmar fue la acción más costosa en tiempo, seguida por la verificación, luego el cifrado asimétrico, y finalmente el cifrado simétrico, que resultó ser la operación más rápida en este escenario.

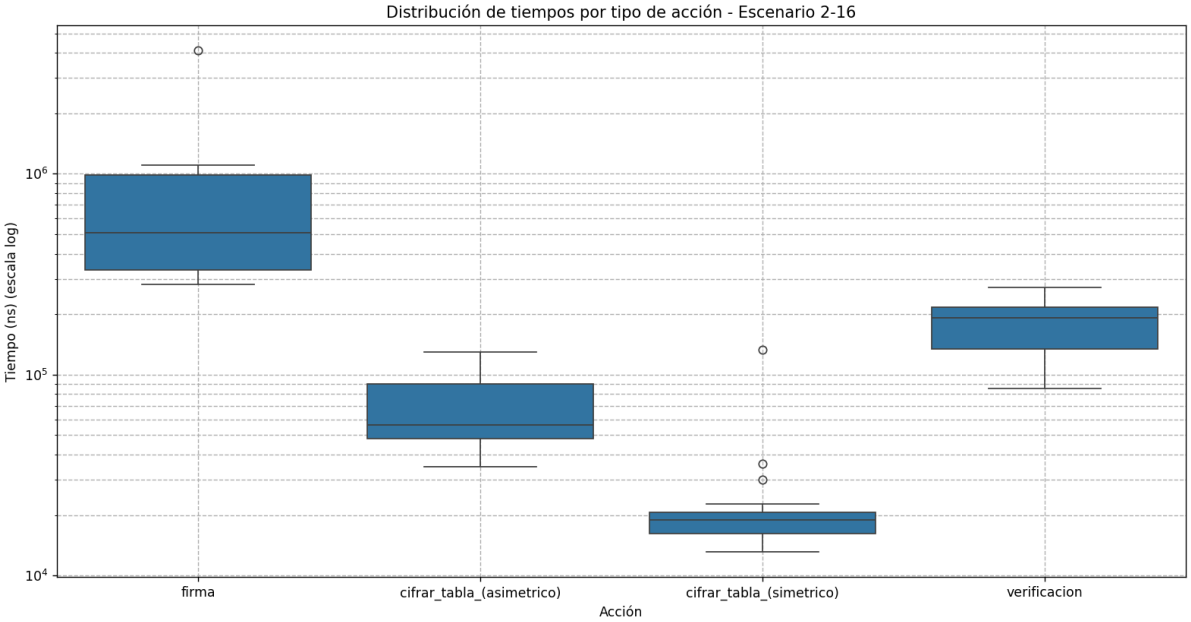
Graficas escenario 2 – 16 conexiones:






Tiempos individuales de Verificación - Escenario 2- 16 conexiones
Verificaciones
Media: 293750 ns
Tiempo de verificación (ns)
6×10^5
4×10^5
3×10^5
2×10^5
10^5
10
20
30
40
50
60
Mediciones


Comparación Cifrado Simétrico vs Asimétrico - Escenario 2-16
Cifrado Simétrico (AES)
Cifrado Asimétrico (RSA)
Media Simétrico: 26725 ns
Media Asimétrico: 67344 ns
Tiempo de cifrado (ns)
10^5
0
10
20
30
40
50
60
Mediciones



Análisis:

En el escenario de 16 conexiones concurrentes, los tiempos de firma se mantuvieron bastante estables, con valores cercanos a la media de 1162319 ns. Esto indica que, a pesar de que el servidor ya manejaba un volumen más alto de solicitudes en paralelo, el comportamiento de la operación de firma no se vio afectado de manera significativa.

Para el cifrado simétrico, la mayoría de las mediciones se ubicaron por debajo de la media de 26725 ns, mostrando una ejecución estable en general. Aunque se presentó un valor algo más elevado respecto a las demás mediciones, la dispersión fue baja, reflejando que el proceso de cifrado se mantuvo eficiente incluso bajo una carga más alta.

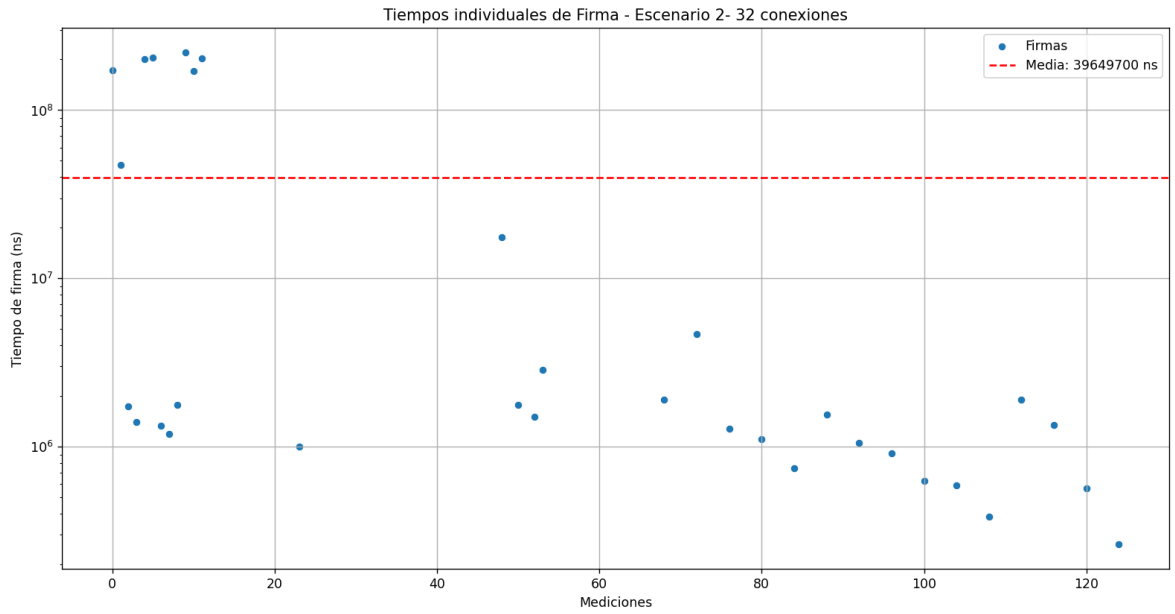
En el caso de la verificación, los tiempos oscilaron alrededor de la media de 293750 ns, pero se identificaron algunos valores atípicos que estuvieron considerablemente por encima o por debajo de esta media. Esto sugiere que, aunque el proceso de validación de consultas es generalmente rápido, pueden producirse pequeñas inestabilidades cuando se incrementa la concurrencia.

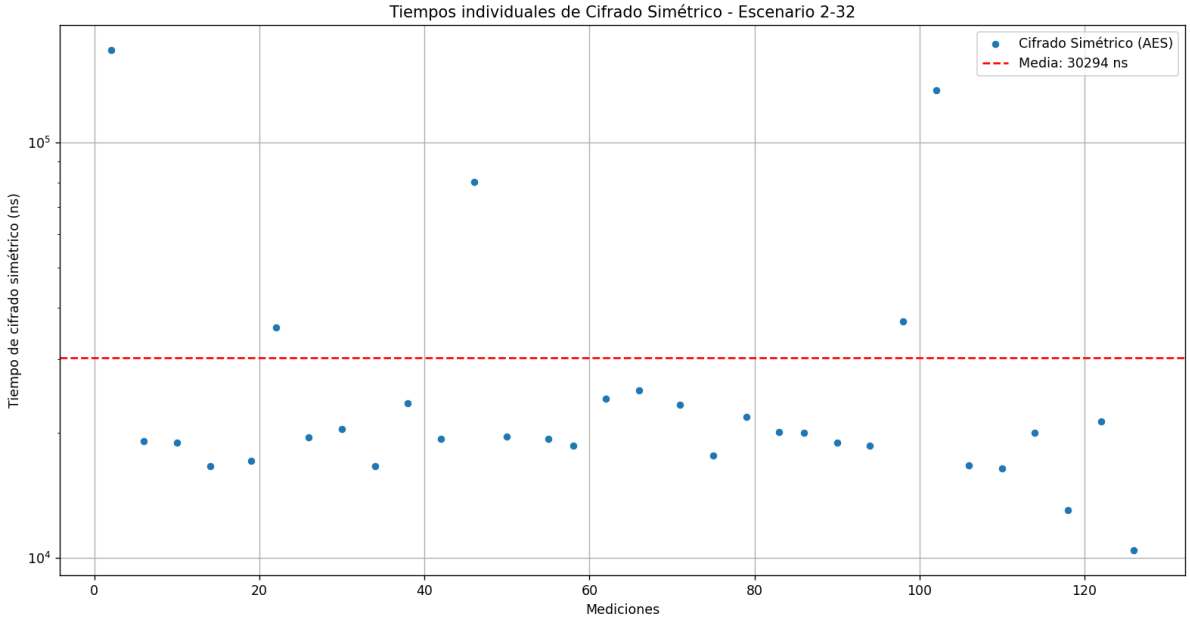
Comparando los tiempos de cifrado simétrico contra los de cifrado asimétrico, se observa que ambos tipos de cifrado mostraron comportamientos relativamente estables, con tiempos no muy alejados de sus respectivas medias (26725 ns para el simétrico y 67344 ns para el asimétrico). Aunque en algunas mediciones puntuales el

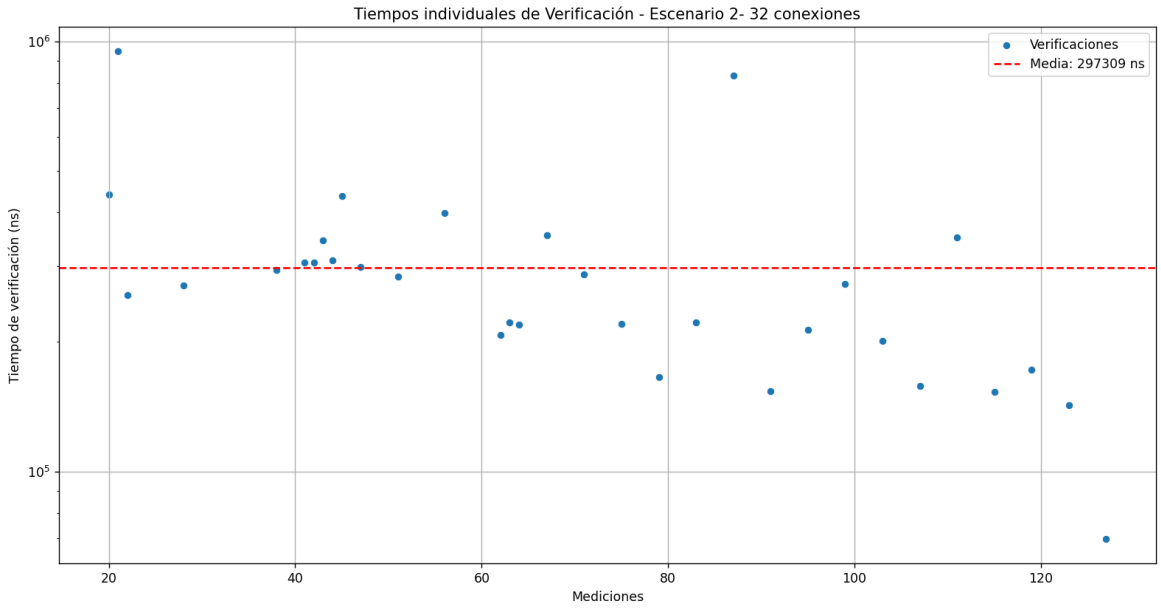
cifrado asimétrico tardó más, no fue lo habitual, y en general la media del cifrado simétrico permaneció inferior, aunque ahora las diferencias entre ambos tipos de cifrado fueron más pequeñas en comparación con los escenarios anteriores.

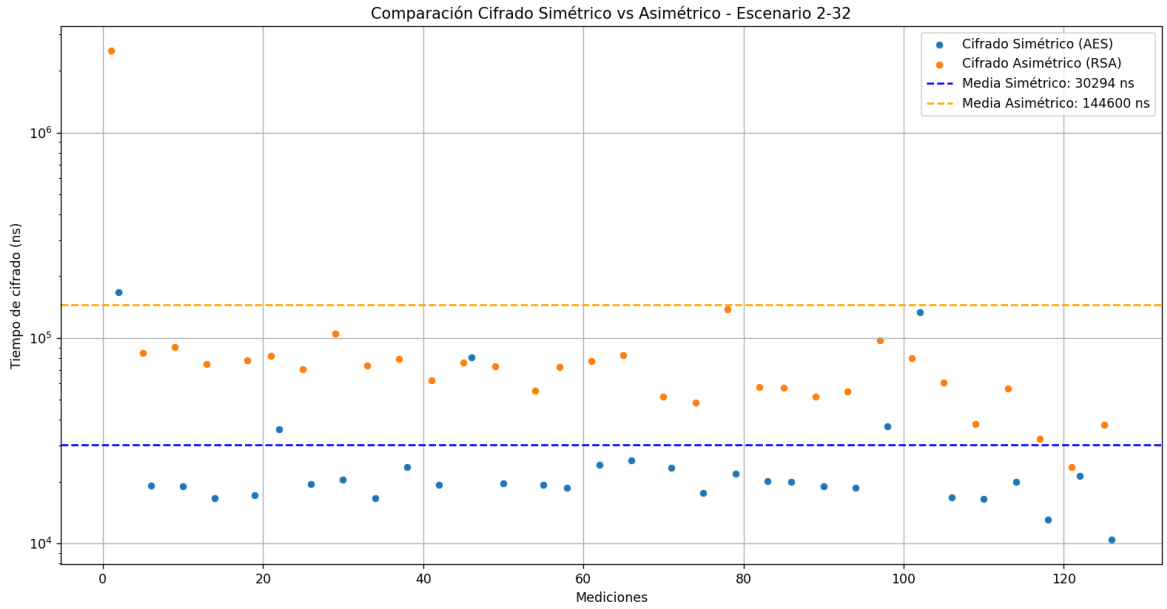
Finalmente, el análisis del diagrama de caja mostró que la firma sigue siendo la operación que más tiempo consume, seguida por la verificación, luego el cifrado simétrico y finalmente el cifrado asimétrico. Además, se puede notar que en este escenario las diferencias de tiempo entre cifrado simétrico y asimétrico se empiezan a marcar más que en escenarios pasados.

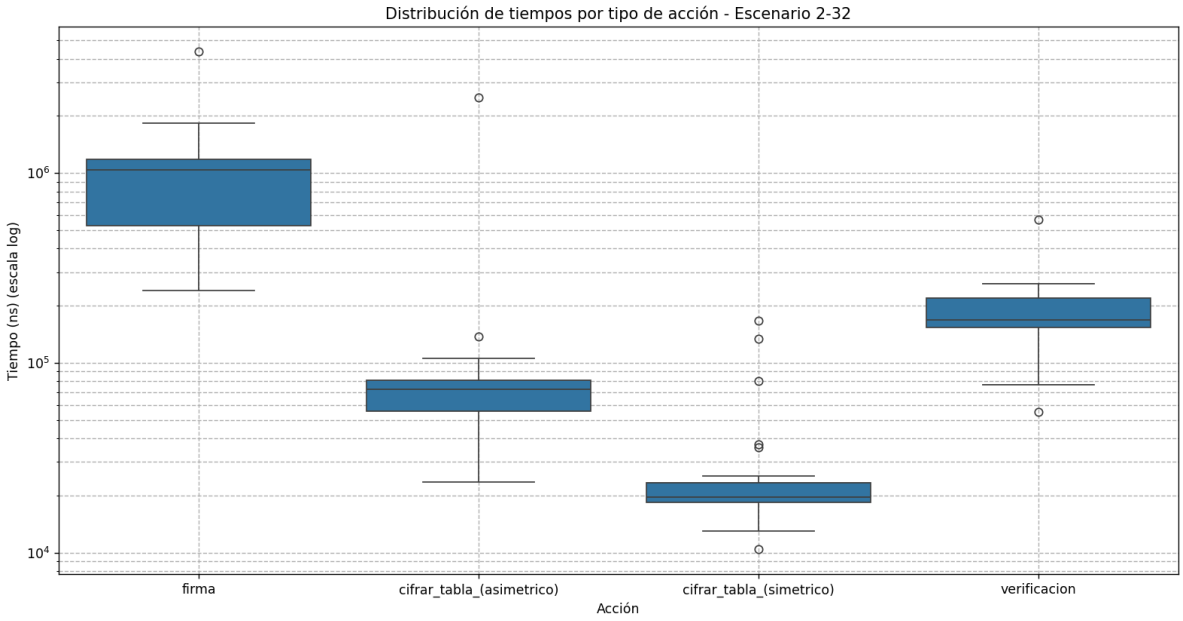
Graficas escenario 2 – 32 conexiones




Tiempos individuales de Cifrado Simétrico - Escenario 2-32
Cifrado Simétrico (AES)
Media: 30294 ns
Tiempo de cifrado simétrico (ns)
10^5
10^4
0
20
40
60
80
100
120
Mediciones


Tiempos individuales de Verificación - Escenario 2- 32 conexiones
Verificaciones
Media: 297309 ns
Tiempo de verificación (ns)
10^6
10^5
20
40
60
80
100
120
Mediciones





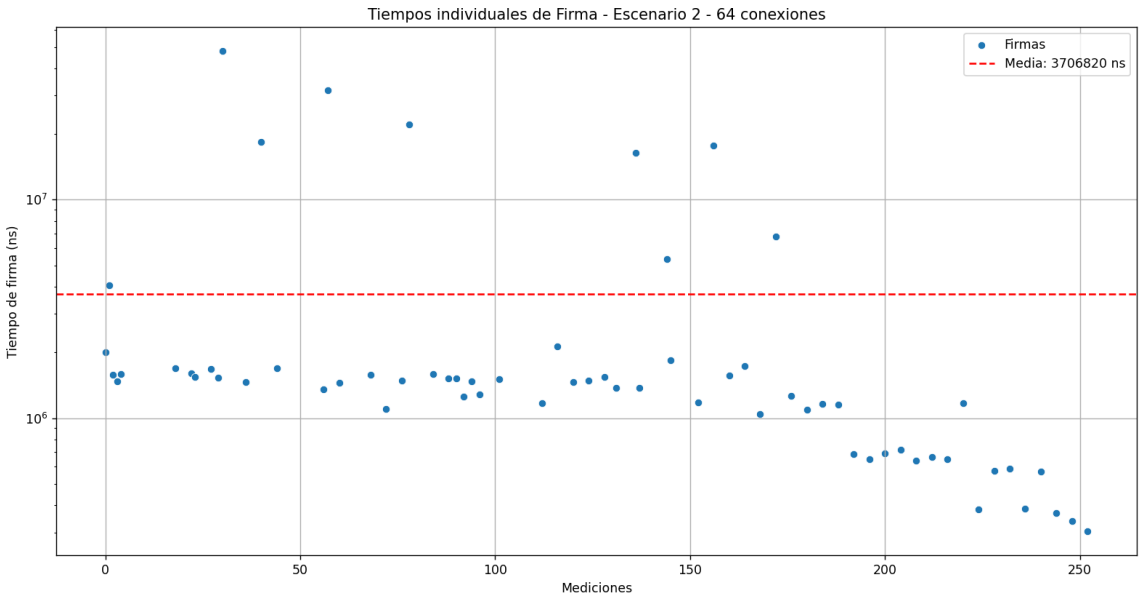
En el escenario de 32 conexiones concurrentes, los tiempos de firma mostraron que la mayoría de las mediciones se ubicaron por debajo de la media de 39649700 ns, aunque se identificó un grupo inicial de valores que estuvo por encima. Esto sugiere que al inicio de la carga concurrente hubo una mayor saturación, que luego se estabilizó conforme avanzaron las solicitudes.

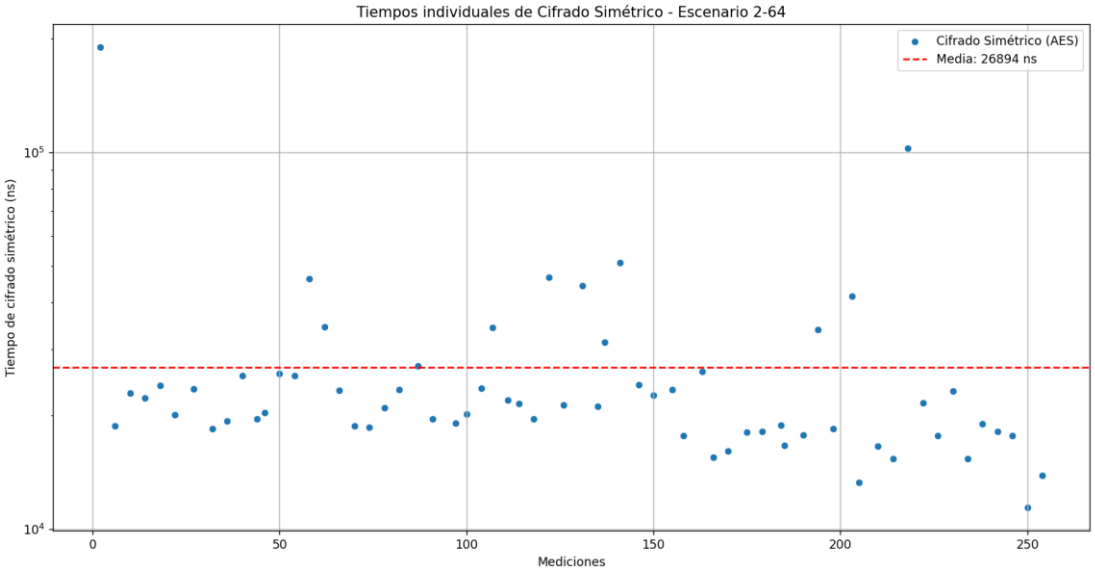
El cifrado simétrico, con una media de 302294 ns, presentó un comportamiento muy similar al de la firma, mostrando al principio algunas mediciones más elevadas pero estabilizándose rápidamente. La tendencia general fue hacia tiempos consistentes y cercanos a la media.

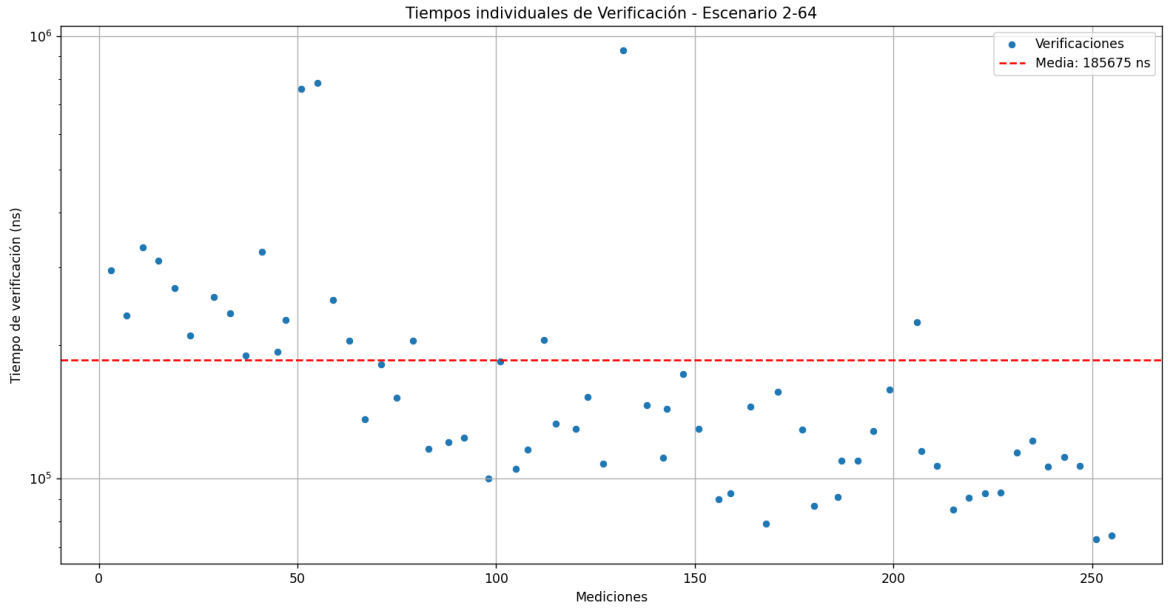
En cuanto a la verificación, los tiempos fueron más regulares desde el inicio, con valores muy cercanos a la media de 297309 ns y una variabilidad menor en comparación con las otras operaciones, lo cual demuestra que el proceso de validación de consultas se mantuvo eficiente incluso bajo esta carga de conexiones.

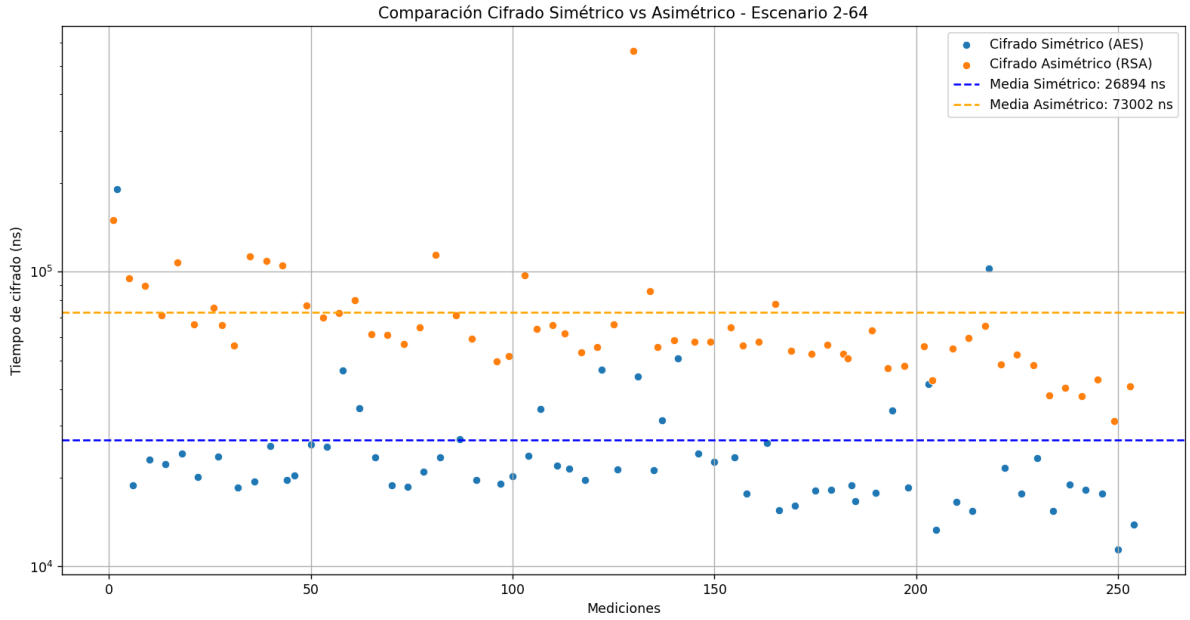
Comparando el cifrado simétrico con el cifrado asimétrico, se observa que en la gran mayoría de los casos el cifrado asimétrico fue más costoso en tiempo, con una media de 144600 ns. Ambos tipos de cifrado mostraron comportamientos bastante estables, con la mayoría de las mediciones ubicándose por debajo de sus respectivas medias y solo unos pocos casos atípicos por encima. Esto indica que, a pesar de la alta concurrencia, los procesos de cifrado se mantuvieron relativamente predecibles, aunque el cifrado asimétrico empezó a mostrar un mayor impacto en el desempeño general del sistema. El orden que sugiere el diagrama de caja sigue siendo el mismo que en escenarios anteriores, siendo la acción de firmar la más costosa, seguida de la verificación y por último el cifrado asimétrico y simétrico respectivamente.

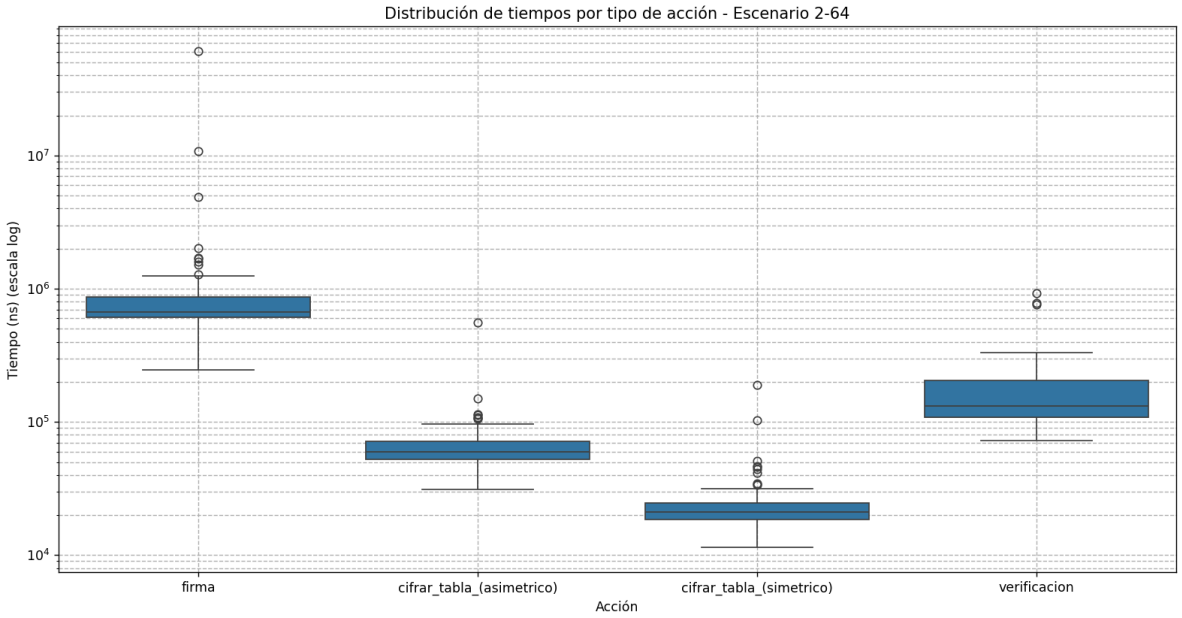
Graficas escenario 2 – 64 conexiones:




Tiempos individuales de Cifrado Simétrico - Escenario 2-64
Cifrado Simétrico (AES)
Media: 26894 ns
Tiempo de cifrado simétrico (ns)
10^5
10^4
0
50
100
150
200
250
Mediciones


Tiempos individuales de Verificación - Escenario 2-64
Verificaciones
Media: 185675 ns
Tiempo de verificación (ns)
Mediciones


Comparación Cifrado Simétrico vs Asimétrico - Escenario 2-64
Cifrado Simétrico (AES)
Cifrado Asimétrico (RSA)
Media Simétrico: 26894 ns
Media Asimétrico: 73002 ns
Tiempo de cifrado (ns)
Mediciones



En el escenario de 64 conexiones concurrentes, los tiempos de firma se mantuvieron mayoritariamente por debajo de la media de 3706820 ns, con valores bastante parecidos entre sí y una tendencia a disminuir a medida que avanzaban las mediciones. Esto sugiere que, aunque la carga inicial pudo afectar ligeramente los tiempos, el sistema logró estabilizarse rápidamente.

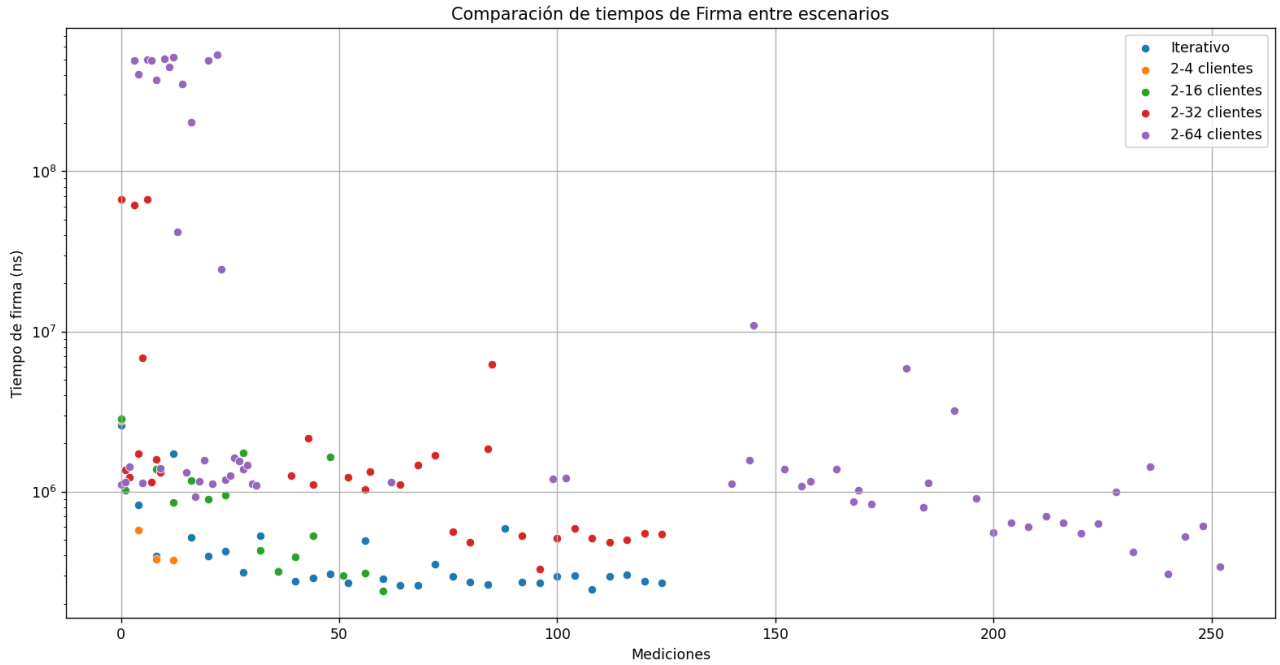
El cifrado simétrico, con una media de 26894 ns, mostró un comportamiento muy estable, con la mayoría de los valores concentrados cerca de la media y con pocas anomalías. Esto evidencia que el proceso de cifrado simétrico, incluso bajo una carga alta, mantiene un buen desempeño y resistencia a la variabilidad.

En cuanto a la verificación, los tiempos también fueron consistentes, manteniéndose alrededor de la media de 185675 ns, con pequeñas variaciones. Esto confirma que la validación de consultas a través de HMAC se comporta de manera eficiente y estable, incluso bajo escenarios de alta concurrencia.

Al comparar los tiempos de cifrado simétrico y asimétrico, se evidenció un cambio claro respecto a escenarios anteriores. En este caso, el cifrado asimétrico resultó ser en casi todas las mediciones mucho más costoso que el simétrico, con una media de 73002 ns. Aunque en algunos casos la diferencia fue menor, en la mayoría de los casos el tiempo del asimétrico fue considerablemente superior, lo cual es coherente con las expectativas, dado que el cifrado RSA es más pesado computacionalmente y sufre más bajo condiciones de alta carga.

Finalmente, en el análisis del diagrama de caja, se observa que firmar sigue siendo la operación más costosa en tiempo, seguida por la verificación, luego el cifrado asimétrico y finalmente el cifrado simétrico. Aunque las medias de verificación, cifrado asimétrico y cifrado simétrico son relativamente cercanas, se mantienen en ese orden.

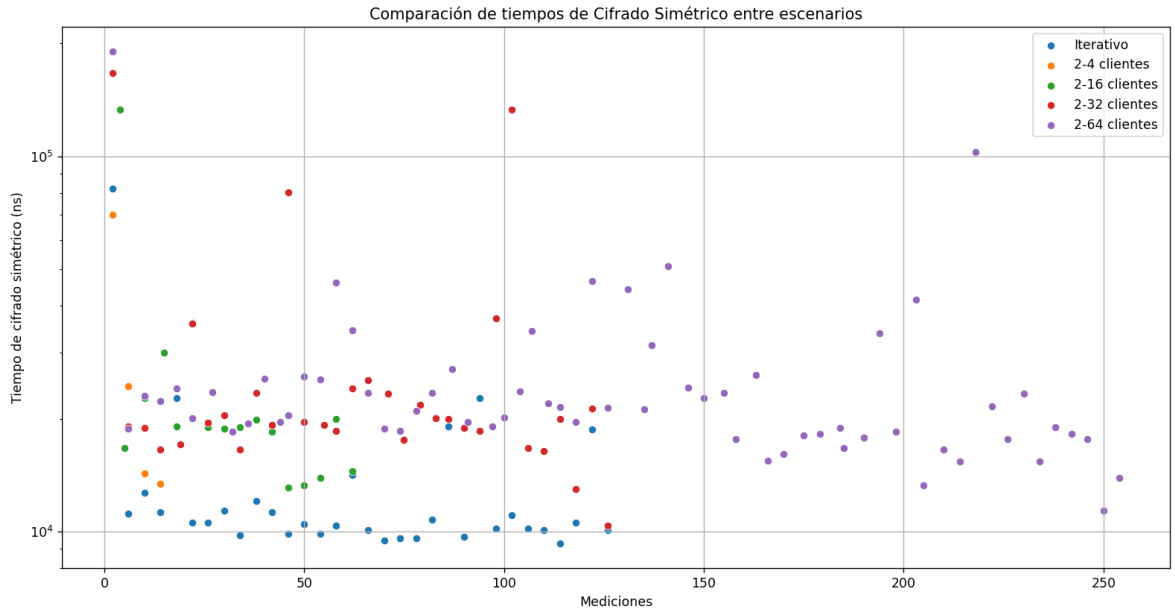
Comparativa de tiempos de firma



Análisis:

Al comparar los tiempos de firma entre los diferentes escenarios, se puede ver que el escenario de 64 conexiones es el que presenta los tiempos más altos de forma general, seguido del de 32 conexiones. Los escenarios de 16, 4 y el iterativo tienen tiempos más bajos y similares entre sí, aunque en general el de 16 conexiones resulta un poco más elevado que los otros dos. El escenario iterativo se destaca por mostrar el comportamiento más estable y rápido de todos, lo cual tiene sentido si se considera que en este caso solo se atiende una solicitud a la vez, sin competencia por recursos del servidor. A medida que el número de conexiones concurrentes aumenta, los tiempos de firma también tienden a crecer, lo que refleja el impacto que tiene la carga en el procesamiento de operaciones criptográficas en el servidor. Esto confirma que, aunque la firma es relativamente eficiente, su desempeño sí se ve afectado cuando hay alta concurrencia.

Comparativa de tiempos para cifrar la tabla de servicios



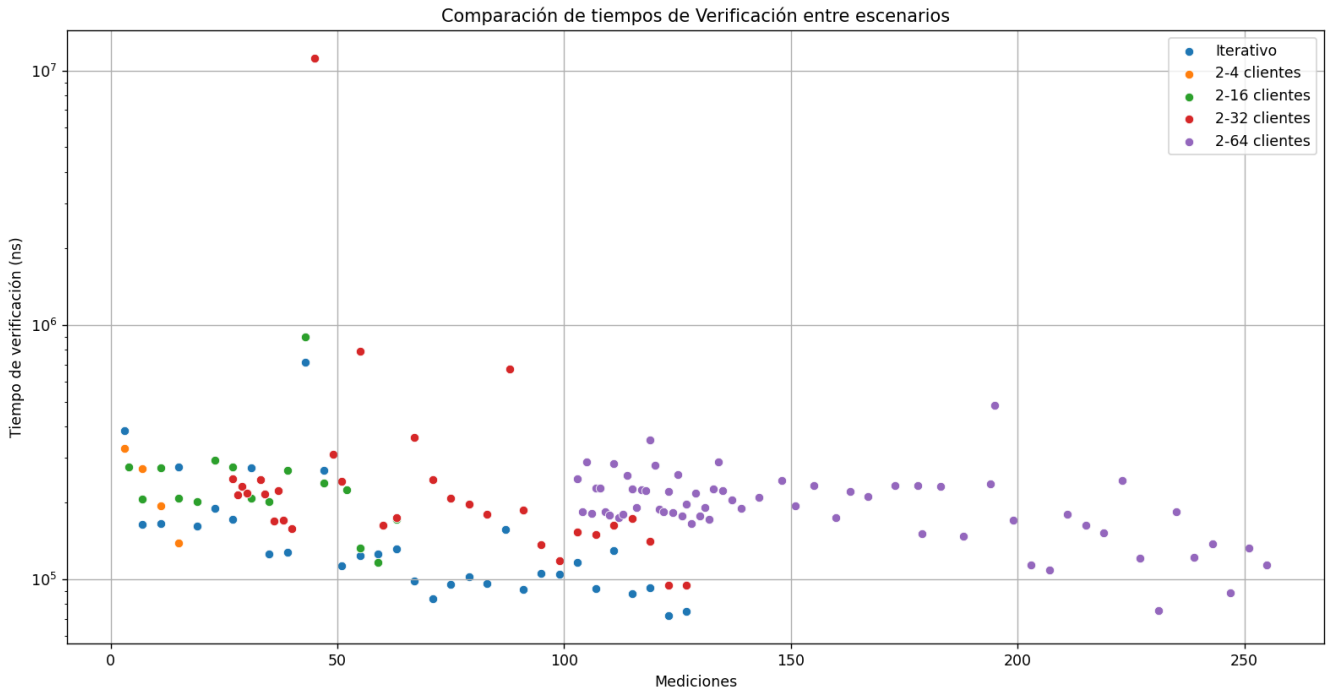
Análisis:

Se puede observar que, en general, los tiempos de ejecución se mantuvieron dentro de un rango relativamente estable. La mayoría de las mediciones, sin importar el nivel de concurrencia, se agruparon alrededor de valores cercanos entre sí, lo cual evidencia que AES es un algoritmo eficiente y confiable incluso cuando aumenta la carga sobre el servidor.

Sin embargo, también es evidente que a medida que la concurrencia incrementa, comienzan a aparecer algunas anomalías. Estas se presentan con más frecuencia en los escenarios de mayor número de conexiones (como los de 32 y 64 clientes concurrentes), donde algunos tiempos de cifrado se disparan respecto al promedio. Aunque no son la mayoría de los casos, sí muestran que el sistema empieza a experimentar cierta presión en condiciones de carga alta, lo cual puede deberse a la competencia por recursos de procesamiento o a pequeñas saturaciones.

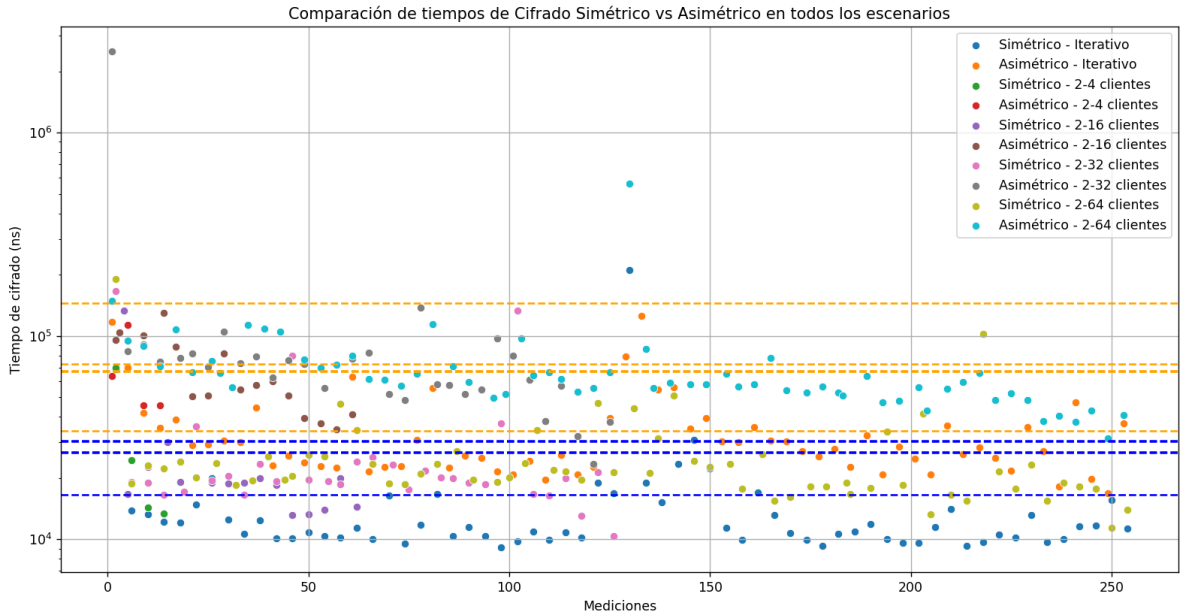
Por otro lado, el escenario iterativo donde solo una solicitud es atendida a la vez presentó los tiempos de cifrado más bajos y constantes, tal como era de esperarse. Al no haber competencia por recursos ni múltiples procesos ejecutándose en paralelo, el rendimiento del cifrado se mantiene, funcionando con total estabilidad.

Comparativa de tiempos para verificar la consulta



Al analizar los tiempos de verificación en los diferentes escenarios, se observa que la mayoría de las mediciones se mantienen dentro de un mismo rango de valores, siguiendo una tendencia bastante horizontal. A pesar de que aparecen algunas anomalías puntuales, en general los resultados son muy consistentes entre escenarios, mostrando tiempos similares tanto en el escenario iterativo como en los escenarios concurrentes. Esto indica que la operación de verificación, basada en códigos HMAC, es poco sensible al aumento en la cantidad de conexiones concurrentes, lo cual era de esperarse teniendo en cuenta que el proceso de calcular y validar un HMAC es ligero y eficiente. Incluso en los escenarios de mayor carga, como 32 o 64 conexiones, no se evidencia un aumento significativo en los tiempos de verificación, lo que demuestra que esta operación se mantiene estable aun en condiciones de alta concurrencia.

Comparativa de tiempos de los tiempos para el caso simétrico y asimétrico



Análisis:

Al observar la gráfica comparativa entre los tiempos promedio de cifrado simétrico (AES) y cifrado asimétrico (RSA) en los diferentes escenarios evaluados, se nota una tendencia clara, que nos dice que en todos los casos, los tiempos de cifrado asimétrico son superiores a los de cifrado simétrico. Esta diferencia se mantiene consistente incluso cuando se incrementa la cantidad de conexiones concurrentes.

Pudimos observar que, aún en el escenario de mayor carga (64 conexiones simultáneas), el tiempo promedio del cifrado simétrico se mantiene inferior al del cifrado asimétrico en escenarios de baja carga, como el iterativo o el de 4 conexiones. Esto refuerza la eficiencia del algoritmo simétrico frente al asimétrico, no solo en términos absolutos sino también en escenarios de alta concurrencia.

En la gráfica, la línea azul representa las medias obtenidas para el cifrado simétrico en cada escenario, mientras que la línea amarilla representa las medias del cifrado asimétrico. Se puede ver que la línea amarilla se mantiene por encima de la azul en todos los casos, indicando que el costo computacional de RSA es considerablemente mayor que el de AES.

En cuanto al rango de valores, se observa que los tiempos para el cifrado simétrico están más concentrados, especialmente en los escenarios con menor concurrencia. A medida que el número de conexiones aumenta, el rango de valores tiende a ampliarse levemente, pero aun así el rendimiento general del cifrado simétrico sigue siendo notablemente superior en comparación con el cifrado asimétrico.

Estimación de la velocidad del procesador mediante operaciones de cifrado

Para estimar la velocidad del procesador en el contexto de operaciones de cifrado, se utilizó como escenario las mediciones realizadas sobre los tiempos promedio de cifrado simétrico (AES) y asimétrico (RSA) bajo los diferentes niveles de concurrencia evaluados (1, 4, 16, 32 y 64 conexiones).

Como referencia, se usaron los tiempos promedio obtenidos en cada caso:

Escenario	Tipo de Cifrado	Tiempo Promedio de Cifrado (ns)
1	Simétrico (AES)	16706,25
1	Asimétrico (RSA)	33958,59375
2	Simétrico (AES)	57106,25
2	Asimétrico (RSA)	80937,5
2	Simétrico (AES)	29782,8125
2	Asimétrico (RSA)	73940,625
2	Asimétrico (RSA)	32043,75
2	Simétrico (AES)	276988,28
2	Asimétrico (RSA)	34344,141
2	Simétrico (AES)	282441,797

Para realizar el cálculo de operaciones por segundo, se utilizó la siguiente fórmula:

$$Operaciones\ por\ segundo = \frac{1000000000s}{tiempo\ promedio\ de\ cifrado\ (ns)}$$

Se tomaron los valores promedio más representativos, en este caso los del escenario de 1 conexión (iterativo), para hacer los cálculos:

- **Cifrado simétrico (AES)**:

$$Operaciones\ por\ segundo = \frac{1000000000}{16706{,}25} \approx 59857{,}83764\,\frac{operaciones}{segundo}$$

- **Cifrado asimétrico (RSA)**:

$$Operaciones\ por\ segundo = \frac{1000000000}{33958{,}59375} \approx 29447{,}62694\,\frac{operaciones}{segundo}$$

Resultados:

- El procesador puede realizar aproximadamente 59857 operaciones de cifrado simétrico por segundo.
- El procesador puede realizar aproximadamente 29447 operaciones de cifrado asimétrico por segundo.

Consideraciones:

Para estimar la velocidad de operaciones, se utilizaron los tiempos promedio de las mediciones del escenario 1 (una conexión iterativa). Este escenario fue elegido porque representa una situación sin concurrencia ni saturación del servidor, permitiendo medir el desempeño puro de las operaciones de cifrado en condiciones ideales. De esta manera, se evita que factores como la competencia por recursos o la carga simultánea de procesos alteren los resultados. Además, es importante tener en cuenta que el tamaño del mensaje cifrado en las pruebas fue pequeño, lo cual puede afectar la comparación de tiempos entre los métodos de cifrado simétrico y asimétrico, favoreciendo en algunos casos al cifrado asimétrico debido a la menor sobrecarga de inicialización en mensajes reducidos.

Conclusiones:

Con base en las mediciones realizadas, se puede concluir que el procesador de la máquina utilizada es capaz de realizar aproximadamente 6032 operaciones de cifrado simétrico por segundo y alrededor de 11249 operaciones de cifrado asimétrico por segundo, bajo condiciones ideales de baja carga y con mensajes de tamaño reducido (en nuestro caso una tabla así: “S1 S2 S3”).

Estimación velocidad del procesador.

Para estimar la velocidad del procesador se implementó un programa en Java que realiza mil millones de sumas simples (operaciones aritméticas básicas). Estas operaciones se ejecutan de forma continua y se mide el tiempo total usando System.nanoTime().

Consideraciones

Se usaron sumas porque son operaciones simples y rápidas.

Se ejecutaron mil millones para obtener una medición representativa.

La prueba se hizo bajo condiciones normales del sistema, sin forzar rendimiento.

System.nanoTime() permitió medir con buena precisión.

System.nanoTime() permitió medir con buena precisión.A partir del tiempo, se calcula cuántas operaciones por segundo se lograron, lo que permite estimar la velocidad del procesador en GHz. Esta aproximación es válida porque refleja cuántas instrucciones sencillas puede procesar la CPU en un segundo.

Consideraciones

Se usaron sumas porque son operaciones simples y rápidas.

Se ejecutaron mil millones para obtener una medición representativa.

La prueba se hizo bajo condiciones normales del sistema, sin forzar rendimiento.

System.nanoTime() permitió medir con buena precisión.

Se usaron sumas porque son operaciones simples y rápidas.

Se ejecutaron mil millones para obtener una medición representativa.

La prueba se hizo bajo condiciones normales del sistema, sin forzar rendimiento.

System.nanoTime() permitió medir con buena precisión.

Resultados obtenidos:

Tiempo total (s): 0.2397984

Operaciones por segundo: 4.170169609138343E9

Velocidad aproximada de CPU (GHz): 4.170169609138343 - 4,17 GHz

Conclusión

El procesador logró ejecutar más de 4 mil millones de operaciones por segundo, lo que da una velocidad aproximada de 4,17 GHz. Esta estimación es coherente con lo esperado para una máquina moderna lo que indica que está bien preparado para manejar tareas de cifrado y concurrencia como las planteadas en este proyecto.

Conclusión