Iván Arturo Ávila - 202216280

Juan David Roa Moyano - 202211446

**Informe caso 3**

**Descripción de la organización de los archivos**

En el archivo zip se va encontrar los siguientes archivos importantes:

* OpenSSL-1.1.1h\_win32: este archivo contiene la aplicación para correr Openssl la cual genera las llaves del algoritmo de DH.
* Src: esta carpeta contiene las siguientes clases:
  + Cliente: Este archivo contiene el código para ejecutar el cliente, el cual se conecta al servidor y realiza consultas específicas en función de la configuración del servidor. El cliente envía solicitudes al servidor para ejecutar operaciones de cifrado y verificar el tiempo de respuesta.
  + ClienteHandler: Este archivo define el manejador de clientes del servidor. Es utilizado por el servidor para gestionar cada conexión individual de los clientes, proporcionando la lógica de cifrado y autenticación de cada solicitud recibida.
  + Servidor: Este archivo contiene el código principal para iniciar el servidor. Permite gestionar las conexiones de los clientes y responder a sus solicitudes de manera concurrente. Al ejecutarse, el servidor solicita al usuario seleccionar la opción deseada para la cantidad de delegados, lo cual determina el número de conexiones concurrentes permitidas.
* Documento de Word que contiene el informe.

**Instrucciones para correr servidor y cliente**

Este proyecto es compatible únicamente con el sistema operativo Windows. Con OpenSSL y Java Development Kit .

Requisitos Previos

* Java Development Kit

Ejecución Paso a Paso

1. Ejecuta el servidor:
   1. Compila Servidor.java si es necesario, usando el comando en la terminal del proyecto o mediante la interfaz gráfica del IDE.
2. Selecciona la opción deseada en el servidor:
   1. Una vez que el servidor esté en ejecución, se te pedirá seleccionar una opción en la consola de Windows. Escoge la opción deseada según los requerimientos de la prueba o el escenario.
3. Ejecuta el cliente:
   1. Compila y ejecuta Cliente.java.

Notas Importantes

* Orden de Ejecución: Asegúrate de que el servidor esté iniciado y configurado antes de ejecutar el cliente.
* Múltiples Clientes: Para pruebas de concurrencia con varios clientes, abre varias instancias de la terminal de Windows y ejecuta el cliente en cada una.
* Compatibilidad con Windows: Este proyecto ha sido diseñado específicamente para Windows, por lo que podría no funcionar correctamente en otros sistemas operativos.
* OpenSSL: Este proyecto depende de OpenSSL para manejar operaciones criptográficas. OpenSSL debe estar instalado y configurado en el PATH del sistema.

**Tablas de datos**

**Escenario 1**

Un servidor y un cliente iterativos. El cliente genera 32 consultas.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Consulta** | **Reto(ns)** | **DH(ns)** | **Consulta(ns)** | **Simétrico(ns)** | **Asimétrico(ns)** |
| 1 | 919720 | 3238712900 | 530920 | 37400 | 275699 |
| 2 | 1246800 | 3413068000 | 455700 | 24400 | 255000 |
| 3 | 991000 | 3664565900 | 385900 | 20000 | 249900 |
| 4 | 1003400 | 410253900 | 444000 | 24200 | 675300 |
| 5 | 1060900 | 241431100 | 362600 | 19800 | 242100 |
| 6 | 912100 | 2013256100 | 727900 | 22900 | 227500 |
| 7 | 824100 | 1634218200 | 232000 | 19000 | 237400 |
| 8 | 1327000 | 1624583700 | 376900 | 21200 | 233800 |
| 9 | 825000 | 5662710300 | 215200 | 20600 | 229100 |
| 10 | 839000 | 1621799900 | 329600 | 26700 | 366000 |
| 11 | 918100 | 472788800 | 216000 | 19500 | 220600 |
| 12 | 875700 | 1002034200 | 219400 | 19300 | 222300 |
| 13 | 837000 | 3512787200 | 209900 | 21600 | 218800 |
| 14 | 908200 | 819433600 | 217400 | 19500 | 229300 |
| 15 | 834300 | 3708397100 | 224100 | 21100 | 224800 |
| 16 | 774800 | 531227800 | 206700 | 20500 | 228200 |
| 17 | 1040900 | 1735687600 | 202300 | 28800 | 215400 |
| 18 | 850300 | 3618610300 | 245800 | 43800 | 236400 |
| 19 | 819900 | 4347187800 | 203500 | 20300 | 225500 |
| 20 | 933400 | 341580500 | 202500 | 19800 | 230600 |
| 21 | 1387200 | 2552815300 | 424300 | 22900 | 273100 |
| 22 | 995700 | 764896600 | 381900 | 19900 | 277800 |
| 23 | 1166900 | 1384569400 | 363700 | 20600 | 542500 |
| 24 | 1039000 | 1695134900 | 362900 | 22400 | 283000 |
| 25 | 1001800 | 1357368300 | 667500 | 22200 | 256200 |
| 26 | 829000 | 251970300 | 238600 | 20100 | 264300 |
| 27 | 1338200 | 2776083400 | 382800 | 22200 | 252900 |
| 28 | 926500 | 856291500 | 213700 | 21100 | 257300 |
| 29 | 959800 | 2655240000 | 222300 | 21800 | 237600 |
| 30 | 918200 | 425019100 | 212900 | 20100 | 231800 |
| 31 | 838900 | 4833802000 | 210800 | 20400 | 239300 |
| 32 | 827400 | 4635329000 | 323900 | 22000 | 236800 |

**Escenario 2**

Datos 4 servidores delegados y 4 clientes delegados

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tiempo de Reto (ns)** | **Tiempo DH (ns)** | **Tiempo Consulta (ns)** | **Tiempo Simétrico (ns)** | **Tiempo Asimétrico (ns)** |
| 116959000 | 429953500 | 8810400 | 60800 | 570000 |
| 116731500 | 1356838800 | 636400 | 41800 | 836300 |
| 116965000 | 2949936700 | 495700 | 55600 | 527100 |
| 116904400 | 5910815800 | 625200 | 26300 | 416200 |

Datos 8 servidores delegados y 8 clientes delegados

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tiempo de Reto (ns)** | **Tiempo DH (ns)** | **Tiempo Consulta (ns)** | **Tiempo Simétrico (ns)** | **Tiempo Asimétrico (ns)** |
| 116299200 | 765261100 | 9708400 | 95200 | 1102400 |
| 115529000 | 1933511000 | 531000 | 23000 | 411100 |
| 116338800 | 2098924900 | 548600 | 21100 | 419700 |
| 117132300 | 3367445000 | 629100 | 39700 | 458100 |
| 115401100 | 3368494200 | 729000 | 59200 | 485600 |
| 116534500 | 3429150700 | 1151300 | 46400 | 310900 |
| 114112000 | 4701381100 | 596800 | 35700 | 452000 |
| 76603400 | 8365888700 | 245600 | 18000 | 290900 |

32 servidores delegados y 32 Clientes delegados

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tiempo de Reto (ns)** | **Tiempo DH (ns)** | **Tiempo Consulta (ns)** | **Tiempo Simétrico (ns)** | **Tiempo Asimétrico (ns)** |
| 158809200 | 820661900 | 8626800 | 51300 | 652400 |
| 161041500 | 979093200 | 614900 | 26500 | 553300 |
| 162685100 | 2916720600 | 608000 | 35600 | 448100 |
| 166279800 | 3251687300 | 505100 | 22800 | 382900 |
| 163193500 | 3752805600 | 811800 | 47600 | 477300 |
| 155241400 | 5542881300 | 1210000 | 62000 | 506000 |
| 153041700 | 5701668200 | 356100 | 23700 | 385300 |
| 156679500 | 6012167500 | 648200 | 23100 | 396200 |
| 164016600 | 6153533700 | 380000 | 24000 | 413000 |
| 158118400 | 6434756600 | 367900 | 33400 | 408500 |
| 154849000 | 6461142900 | 345200 | 19900 | 354000 |
| 154317200 | 7027617800 | 365700 | 22600 | 421800 |
| 162451600 | 7380126200 | 311600 | 24700 | 442300 |
| 157867600 | 7450717300 | 332500 | 23700 | 379100 |
| 162241800 | 7873617500 | 411400 | 26600 | 420100 |
| 154500100 | 8118146800 | 275600 | 35500 | 390400 |
| 166064700 | 9805189100 | 305200 | 20500 | 420200 |
| 157071300 | 9886303100 | 262700 | 21500 | 386800 |
| 154104100 | 1,0589E+10 | 347800 | 24900 | 408500 |
| 157449300 | 1,0619E+10 | 289500 | 30300 | 386500 |
| 160207900 | 1,0639E+10 | 296500 | 21300 | 689300 |
| 154775400 | 1,0748E+10 | 303800 | 26500 | 441800 |
| 164273500 | 1,2392E+10 | 249000 | 18000 | 374500 |
| 155565000 | 1,2776E+10 | 311100 | 24500 | 371300 |
| 157797400 | 1,3271E+10 | 256800 | 19300 | 278800 |
| 163072100 | 1,3368E+10 | 244400 | 18800 | 259100 |
| 155972100 | 1,376E+10 | 265100 | 19100 | 290200 |
| 159756700 | 1,3553E+10 | 306100 | 21800 | 382900 |
| 146581400 | 1,3862E+10 | 258300 | 19800 | 296700 |
| 154770100 | 1,4124E+10 | 262900 | 17300 | 279200 |
| 152218700 | 1,4865E+10 | 222500 | 18800 | 271700 |
| 150442800 | 1,5018E+10 | 199400 | 16800 | 254100 |

4 servidores y 8 clientes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tiempo de Reto (ns)** | **Tiempo DH (ns)** | **Tiempo Consulta (ns)** | **Tiempo Simétrico (ns)** | **Tiempo Asimétrico (ns)** |
| 106933500 | 461045500 | 7643700 | 18900 | 937900 |
| 107328200 | 466340200 | 7550200 | 45000 | 945700 |
| 1876500 | 2847810800 | 606700 | 28800 | 791500 |
| 107114400 | 3767606100 | 418100 | 18500 | 293300 |
| 1597400 | 1545124000 | 742800 | 49700 | 461900 |
| 1808200 | 2493707500 | 1209400 | 32500 | 334400 |
| 107531600 | 6467713900 | 294700 | 18600 | 294700 |
| 2310800 | 7194010600 | 335900 | 20500 | 289700 |

**Gráficas**

**Escenario 1**

La gráfica presentada muestra los tiempos de procesamiento del reto en el servidor, medidos en nanosegundos (ns) a lo largo de 32 pruebas consecutivas. En el eje horizontal se observan las pruebas individuales, numeradas del 1 al 32, mientras que el eje vertical indica el tiempo requerido para cada procesamiento del reto. La altura de cada barra representa el tiempo en nanosegundos que tomó el servidor para responder al reto en esa prueba específica. En general, la gráfica evidencia cierta variabilidad en los tiempos de respuesta, lo cual indica que, aunque el proceso es en promedio rápido, existen fluctuaciones en el rendimiento del servidor. Estas variaciones pueden deberse a factores como la carga de trabajo en el servidor en el momento de la prueba, la concurrencia de solicitudes, o la disponibilidad de recursos de sistema en cada instancia de procesamiento.

En cuanto a los valores extremos, se observan algunos picos en las pruebas 7, 21 y 27, donde el tiempo de procesamiento alcanza entre 1,200,000 y 1,500,000 ns, considerablemente más alto que en las otras pruebas. Estos picos representan momentos en los que el servidor tarda más en procesar el reto, posiblemente debido a factores temporales como una mayor carga en el sistema o la ejecución de otras tareas que limitan la capacidad de respuesta del servidor en esos instantes específicos. Por otro lado, los tiempos de procesamiento en la mayoría de las pruebas se encuentran en un rango más consistente, entre 700,000 y 1,000,000 ns. Esto sugiere que, aunque el servidor presenta algunos casos atípicos de tiempos elevados, en general el cálculo del reto es rápido y muestra un comportamiento bastante estable.

La tendencia general de la gráfica indica que el servidor es capaz de manejar el cálculo del reto en un tiempo relativamente corto, con ligeras variaciones que reflejan un rendimiento adecuado. Sin embargo, los picos elevados revelan áreas de oportunidad para optimización, pues la reducción de estas variaciones podría mejorar la eficiencia del servidor. En conclusión, la gráfica sugiere que el servidor mantiene un buen rendimiento en el cálculo del reto, pero la presencia de algunos picos en los tiempos de procesamiento muestra que el sistema podría beneficiarse de ajustes para reducir el impacto de esos casos atípicos.

La gráfica muestra los tiempos de procesamiento para el cálculo de los valores de Diffie-Hellman (DH) en el servidor, expresados en nanosegundos (ns) a través de 32 pruebas consecutivas. En el eje horizontal, se encuentran las pruebas individuales numeradas del 1 al 32, mientras que el eje vertical representa el tiempo necesario para realizar los cálculos de los parámetros GGG, PPP y GxG^xGx en cada prueba. La altura de cada barra indica el tiempo en nanosegundos que tomó el servidor para completar esta parte del protocolo de establecimiento de clave en esa prueba en particular.

Observamos una notable variabilidad en los tiempos de cálculo de Diffie-Hellman. La mayoría de las pruebas muestran tiempos en el rango de 1x10^9 a 3x10^9 ns, lo que indica una tendencia general en cuanto a los recursos de tiempo que requiere el servidor para ejecutar estos cálculos. Sin embargo, existen ciertos picos significativos que superan considerablemente este rango. En particular, en las pruebas 9 y 31, el tiempo de cálculo de DH alcanza valores alrededor de 5x10^9 y 6x10^9 ns, respectivamente. Estos valores representan los tiempos más elevados de toda la serie y sugieren que el servidor experimentó una carga adicional o una limitación de recursos durante estas pruebas en particular. Este tipo de picos puede deberse a factores como la carga concurrente en el sistema, procesos en segundo plano o posibles variaciones en la asignación de recursos computacionales en el momento del cálculo.

En contraposición a estos picos, algunas pruebas muestran tiempos de cálculo mucho más bajos, incluso cercanos a 0.5x10^9 ns, como ocurre en las pruebas 5, 7, y 12. Estos resultados representan los tiempos más eficientes dentro de la serie y podrían estar asociados con un estado del sistema más óptimo, con menos interferencias o mayor disponibilidad de recursos. La disparidad entre estos tiempos altos y bajos indica que el proceso de cálculo de los parámetros de DH no es completamente constante y que el rendimiento del servidor está sujeto a fluctuaciones significativas.

En general, la gráfica sugiere que el cálculo de los parámetros de Diffie-Hellman es un proceso relativamente intensivo en tiempo, pero con variaciones considerables de una prueba a otra. La presencia de algunos valores extremadamente altos sugiere que el sistema podría beneficiarse de una revisión para optimizar los tiempos de procesamiento y reducir la variabilidad, lo que ayudaría a mejorar la eficiencia y confiabilidad del servidor en el cálculo de claves compartidas. La reducción de estos tiempos y la estabilidad en el cálculo de DH serían particularmente beneficiosas en escenarios con alta concurrencia o demandas de tiempo real.

La gráfica presentada muestra los tiempos de verificación de la respuesta enviada por el cliente, expresados en nanosegundos (ns), a través de 32 pruebas consecutivas realizadas en el servidor. En el eje horizontal se encuentran las pruebas individuales numeradas del 1 al 32, mientras que en el eje vertical se representa el tiempo necesario para completar el proceso de verificación en cada prueba. La altura de cada barra indica el tiempo que tomó el servidor para verificar correctamente la respuesta del cliente en esa prueba en particular.

Observamos que los tiempos de verificación varían, con una tendencia general que oscila entre los 100,000 y 300,000 ns, lo que representa el rango promedio de duración de este proceso de verificación en la mayoría de las pruebas. Sin embargo, hay ciertos picos notables que se destacan significativamente por encima de este rango promedio. La prueba 1, por ejemplo, presenta un valor cercano a los 500,000 ns, mientras que la prueba 6 alcanza aproximadamente los 750,000 ns, que es el valor más alto registrado en esta serie. Estas variaciones, donde el tiempo de verificación es marcadamente mayor que el promedio, sugieren que el servidor podría haber enfrentado condiciones especiales de carga o limitaciones en los recursos disponibles durante estas pruebas específicas, o posiblemente una interferencia de otros procesos concurrentes que afectaron la eficiencia de verificación.

Aparte de estos picos aislados, también se observan varias pruebas con tiempos mucho más bajos, algunos cercanos a los 100,000 ns, como en las pruebas 10 a 19, lo cual indica que el servidor pudo verificar las respuestas de forma mucho más eficiente en estos casos. La presencia de estos tiempos bajos en las pruebas consecutivas puede estar asociada a condiciones óptimas en el sistema, donde el servidor tuvo acceso a suficientes recursos de procesamiento y menos interferencias de otros procesos. Estos tiempos más bajos son deseables, ya que representan una verificación rápida y eficiente que podría contribuir a un desempeño más fluido en escenarios de alta demanda.

En términos generales, la gráfica sugiere que el tiempo de verificación de la respuesta del cliente en el servidor presenta una cierta variabilidad, aunque con una tendencia estable en el rango de los 100,000 a 300,000 ns. Los picos aislados y elevados indican que existe una potencial área de mejora en términos de estabilidad y consistencia en la respuesta del servidor. Minimizar estos tiempos de verificación más largos podría ser beneficioso para garantizar un desempeño más constante y mejorar la eficiencia del servidor en entornos con múltiples solicitudes simultáneas. Una verificación rápida y constante también sería clave para mejorar la experiencia del usuario en aplicaciones que requieren respuestas en tiempo real o con baja latencia.

La gráfica presentada compara los tiempos de cifrado de mensajes utilizando algoritmos simétricos y asimétrico expresados en nanosegundos (ns), a través de 32 pruebas consecutivas realizadas en el servidor.

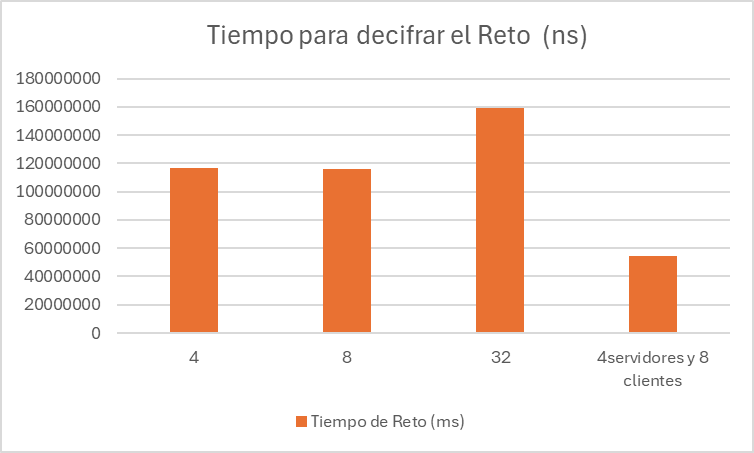
A primera vista, es evidente que el cifrado simétrico es significativamente más rápido que el cifrado asimétrico para todos los conjuntos de datos evaluados. Los tiempos de cifrado simétrico alcanzan picos de varios cientos de miles de nanosegundos, mientras que los tiempos de cifrado asimétrico se mantienen consistentemente en el rango de decenas de miles de nanosegundos, lo que representa una diferencia de varias órdenes de magnitud.

Este resultado es coherente con las características inherentes de ambos tipos de cifrado. Los algoritmos simétricos utilizan una única clave tanto para cifrar como para descifrar los datos, lo que los hace más eficientes en términos de cálculo. Por otro lado, los algoritmos asimétricos emplean un par de claves (pública y privada), lo que implica operaciones matemáticas más complejas y, por consiguiente, tiempos de procesamiento más largos.

La variabilidad en los tiempos de cifrado dentro de cada categoría puede atribuirse a diversos factores, como el tamaño de los mensajes, la complejidad de los algoritmos utilizados, la capacidad de procesamiento del servidor y las condiciones de carga del sistema en el momento de las pruebas.

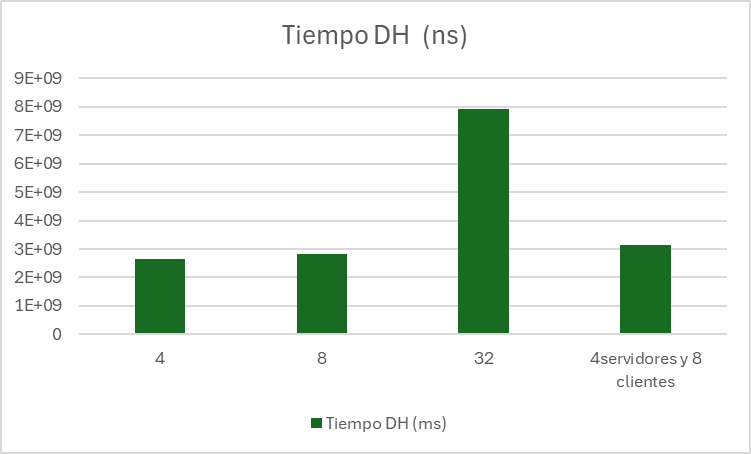
En conclusión, los resultados de esta gráfica confirman la superioridad del cifrado simétrico en términos de velocidad de cifrado. Sin embargo, es importante destacar que la elección entre cifrado simétrico y asimétrico depende de factores adicionales, como los requisitos de seguridad, la gestión de claves y la arquitectura general del sistema. El cifrado asimétrico, a pesar de ser más lento, ofrece ventajas en términos de autenticación y distribución de claves, lo que lo hace ideal para ciertas aplicaciones.

**Escenario 2**



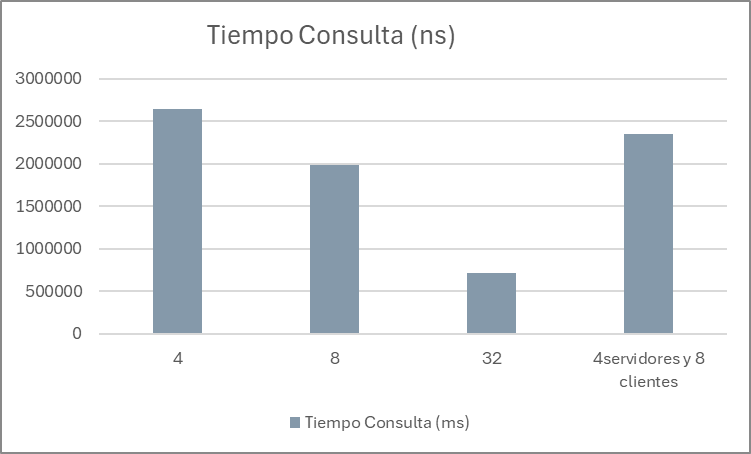
La gráfica muestra el tiempo en nanosegundos que toma descifrar el reto en distintos escenarios, donde varía el número de servidores y clientes delegados: 4, 8, y 32 delegados.

* A medida que aumenta el número de delegados, el tiempo para descifrar el reto también aumenta, alcanzando su punto máximo con 32 delegados. Sin embargo, cuando se utiliza una configuración de 4 servidores y 8 clientes, el tiempo es significativamente menor.
* El aumento del tiempo con más delegados podría deberse a una mayor carga de procesamiento y sincronización entre ellos. La configuración de 4 servidores y 8 clientes parece ser óptima para descifrar el reto, posiblemente porque reduce la sobrecarga de comunicación y manejo de múltiples instancias en el sistema.



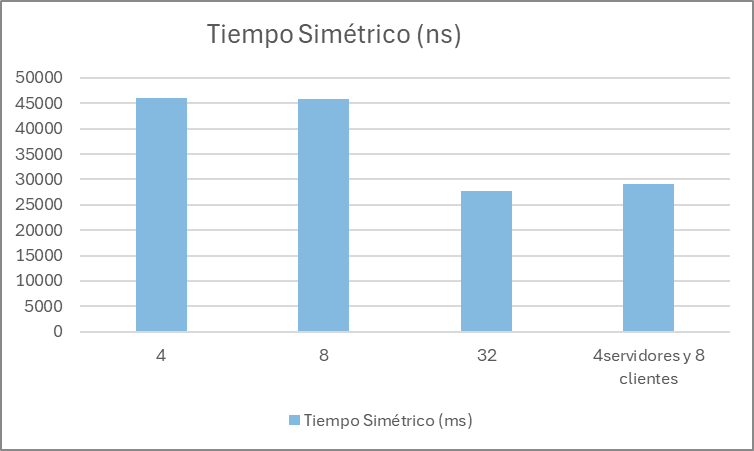
Esta gráfica muestra el tiempo en nanosegundos para generar los parámetros de Diffie-Hellman (DH) en los distintos escenarios.

* Se observa un incremento marcado en el tiempo de generación de los parámetros DH cuando se utilizan 32 delegados. La configuración de 4 servidores y 8 clientes muestra un tiempo más moderado, similar al de los escenarios de 4 y 8 delegados.
* La generación de parámetros DH parece volverse menos eficiente con un mayor número de delegados, probablemente debido a la complejidad adicional de manejo concurrente en el sistema. La configuración de 4 servidores y 8 clientes optimiza el tiempo, posiblemente por una mejor distribución de la carga sin demasiada comunicación concurrente.



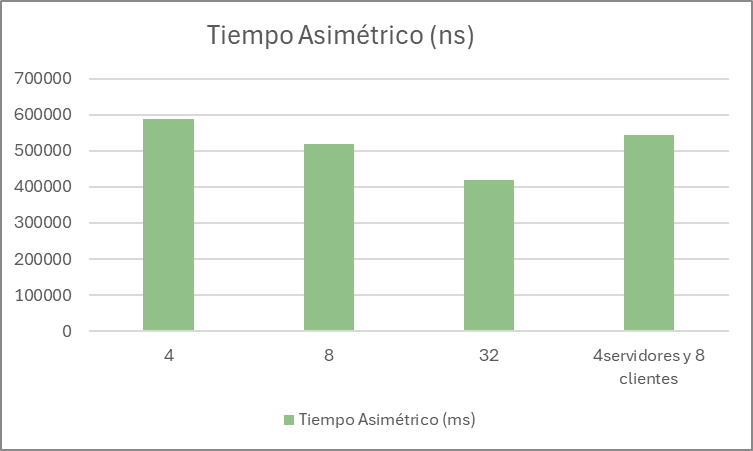
La gráfica compara el tiempo requerido para verificar la consulta en los mismos escenarios.

* El tiempo de consulta es considerablemente más alto para 4 delegados, luego disminuye para 8 y 32 delegados. Para la configuración de 4 servidores y 8 clientes, el tiempo de consulta es similar al de 4 delegados.
* La disminución en el tiempo de consulta al incrementar el número de delegados sugiere que, en este caso, más delegados distribuyen la carga de verificación eficientemente. Sin embargo, la configuración de 4 servidores y 8 clientes no presenta mejoras significativas sobre el escenario de 4 delegados, lo cual puede indicar que la capacidad de procesamiento ya es suficiente en el caso de menos delegados.



Esta gráfica muestra el tiempo necesario para realizar el cifrado simétrico en cada escenario.

* El tiempo es bastante uniforme en todos los escenarios, aunque se observa una ligera disminución conforme aumenta el número de delegados. La configuración de 4 servidores y 8 clientes mantiene un tiempo relativamente bajo.
* Dado que el cifrado simétrico es menos costoso computacionalmente, los tiempos bajos y uniformes indican que el sistema puede manejar esta operación de forma eficiente incluso con múltiples delegados. La ligera reducción con más delegados puede deberse a una distribución más eficiente de la tarea.



Esta gráfica compara el tiempo necesario para realizar el cifrado asimétrico en cada escenario.

* Similar al cifrado simétrico, el tiempo de cifrado asimétrico disminuye con un mayor número de delegados, siendo menor en la configuración de 32 delegados. La configuración de 4 servidores y 8 clientes también muestra un tiempo relativamente bajo.
* El cifrado asimétrico, aunque más costoso que el simétrico, se beneficia de la distribución en múltiples delegados. La mejora en tiempos con 32 delegados indica que el sistema distribuye eficientemente la tarea, reduciendo la carga en cada delegado.

las configuraciones con mayor número de delegados tienden a mejorar los tiempos en tareas menos intensivas como la consulta y los cifrados (simétrico y asimétrico). Sin embargo, el tiempo para descifrar el reto y para generar los parámetros de Diffie-Hellman es mejor en configuraciones moderadas, como la de 4 servidores y 8 clientes, sugiriendo que este equilibrio permite manejar la carga sin introducir una complejidad excesiva en el manejo concurrente.

**Respuestas a preguntas planteadas**

**Calculo de operaciones de cifrado**

**Procesador:** AMD Ryzen 5 5600G tiene una frecuencia base de 3.9 GHz.

**Operaciones de cifrado simétrico y asimétrico**: Los algoritmos de cifrado simétrico, como AES, requieren menos ciclos de reloj por operación en comparación con los algoritmos de cifrado asimétrico, como RSA. En general:

* Cifrado **simétrico** (AES-256) puede realizarse en alrededor de **20 ciclos por byte**.
* Cifrado **asimétrico** (RSA-2048) toma aproximadamente **100,000 ciclos** por operación de cifrado.

Dado que la velocidad base del procesador es de **3.9 GHz**, esto significa que ejecuta:

**Cifrado simétrico (AES-256)**

Si asumimos que cada operación de cifrado simétrico requiere **20 ciclos por byte**, entonces el número de bytes que pueden cifrarse por segundo es:

Esto equivale a **195 MB/s** de datos cifrados por segundo usando AES-256 en este procesador.

**Cifrado asimétrico (RSA-2048)**

Para RSA-2048, donde cada operación de cifrado toma aproximadamente **100,000 ciclos**:

Por lo tanto, el procesador podría realizar **aproximadamente 39,000 operaciones de cifrado RSA-2048 por segundo**.