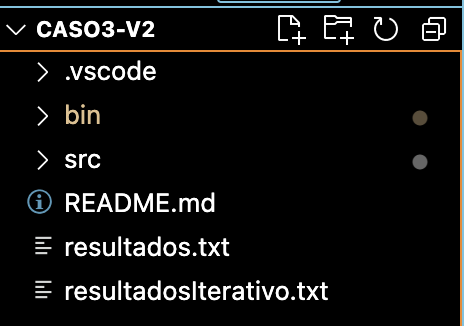
**Caso 3**

Angélica Ortiz - 202222480  
María José Amorocho - 202220179

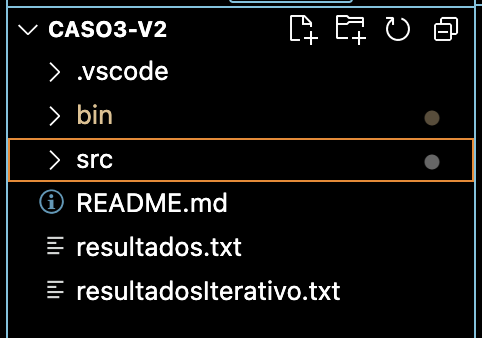
<https://docs.google.com/spreadsheets/d/1JGPCRV4mHZUg4pZ6gEsYoBeRlOh8wcyLk-krlDe4KH0/edit?usp=sharing>

# Descripción de la organización de los archivos en el zip









# Instrucciones para correr servidor y cliente

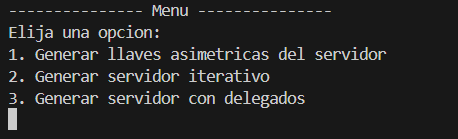
El código se corre desde la clase Main. Al ejecutarlo, lo primero que aparece es el siguiente mensaje



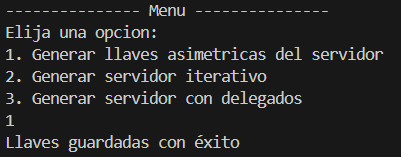
Aquí el usuario debe ingresar la ruta completa de la carpeta que contiene la aplicación de OpenSSL. Por ejemplo:

C:\Users\majoa\Downloads\OpenSSL-1.1.1h\_win32\OpenSSL-1.1.1h\_win32

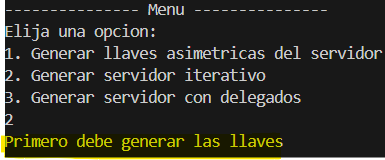
Después de ingresar la ruta, se muestra el menú de la aplicación.



Lo primero que debería hacer es ejecutar la opción 1. Al seleccionar esta opción se generan las llaves simétricas del servidor. Estas llaves quedan guardadas en la ruta src\Llaves. En el archivo LlavePrivadaServidor.txt queda guardada la llave privada del servidor y en el archivo LlavePublicaServidor.txt queda guardada la llave privada de este. Si todo se generó correctamente debería aparecer el siguiente mensaje

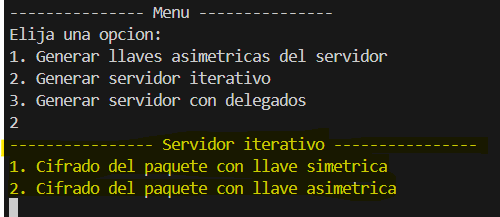


Es importante recalcar que no se pueden ejecutar las opciones 2 y 3 del menú si primero no se ejecutó la opción 1. Si el usuario intenta ejecutar la opción 2 o 3 sin haber ejecutado la primera, el programa muestra el siguiente mensaje

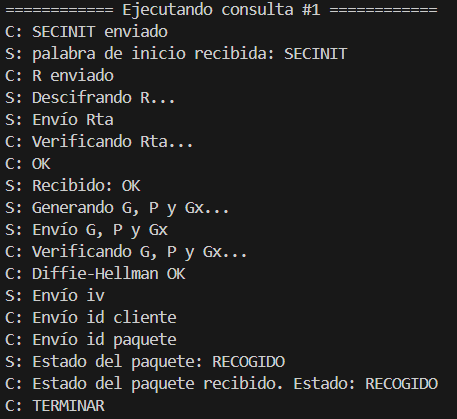


Una vez generadas las llaves, vuelve a aparecer el mismo menú y el usuario tiene la opción entre generar un servidor iterativo o un servidor con delegados.

Para iniciar el **servidor iterativo**, el usuario debe elegir la opción 2. A continuación se mostrarán las siguiente opciones

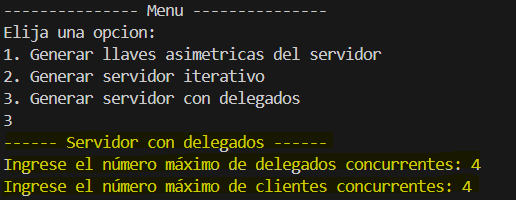


El usuario debe **ingresar el número** de la opción que desea. Una vez realizada esta acción el programa creará el servidor y el cliente, que automáticamente realizará las 32 consultas de manera iterativa. Cada consulta se imprime de la siguiente manera:

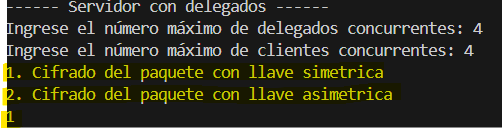


S corresponde a un mensaje que envía el servidor y C a un mensaje que envía el cliente. Lo mismo se muestra con la opción de cifrado asimétrico del paquete.

Para el servidor concurrente, la dinámica es similar. Al presionar la opción 3 del menú se muestra lo siguiente:



Aquí el usuario debe colocar el número de delegados y de cliente que desee crear. En el ejemplo de la imagen, se crearon 4 clientes con 4 delegados. A continuación el usuario debe seleccionar si quiere cifrar el paquete con llave simétrica (opción 1) o con llave asimétrica (opción 2), como se muestra a continuación



En el ejemplo de la imágen, se usó el cifrado del paquete con la llave simétrica.

Una vez insertada la opción, el programa creará el número de clientes y delegados elegidos y comenzará a ejecutar el protocolo de comunicación por cada consulta.

Cabe resaltar que los tiempos no son impresos por consola en ningún caso. Estos quedan almacenados en dos archivos: resultados.txt, que almacena los tiempos de las consultas hechas en el caso concurrente y resultadosIterativo.txt, que almacena los tiempos de las consultas hechas en el caso iterativo.

# Tablas de datos

## Cifrado simetrico

### Servidor iterativo

| **Cifrado simétrico** | | | | |
| --- | --- | --- | --- | --- |
| # Consulta | Tiempo para descifrar el reto (ms) | Tiempo para generar G, P y Gx (ms) | Tiempo para verificar consulta (ms) | Tiempo para cifrar paquete (ms) |
| 1 | 7.5622 | 346.54 | 39.0447 | 0.3241 |
| 2 | 0.459 | 1284.4946 | 2.9449 | 0.4235 |
| 3 | 1.0932 | 1236.8588 | 8.2319 | 0.3867 |
| 4 | 0.424 | 4075.4608 | 5.228 | 0.7356 |
| 5 | 0.4752 | 3913.6156 | 1.8572 | 0.2124 |
| 6 | 0.8186 | 382.5876 | 2.9113 | 0.3023 |
| 7 | 0.5132 | 6515.781 | 2.1751 | 0.2986 |
| 8 | 0.8889 | 15921.0654 | 11.2207 | 0.2861 |
| 9 | 0.4895 | 1884.1163 | 2.3352 | 0.2805 |
| 10 | 0.3713 | 2155.8291 | 1.6166 | 0.3634 |
| 11 | 0.386 | 8781.0259 | 6.0924 | 0.2617 |
| 12 | 0.3392 | 4398.4611 | 1.1803 | 0.2902 |
| 13 | 0.5229 | 2430.5987 | 2.6187 | 0.3379 |
| 14 | 0.5903 | 5263.7611 | 2.742 | 0.2836 |
| 15 | 0.5137 | 13489.2064 | 6.6835 | 0.2893 |
| 16 | 0.8032 | 1774.3739 | 3.3495 | 0.3029 |
| 17 | 0.6258 | 139.0836 | 2.1747 | 0.2902 |
| 18 | 0.5541 | 10547.196 | 1.384 | 0.3067 |
| 19 | 0.5746 | 3751.489 | 2.7224 | 0.296 |
| 20 | 0.6507 | 13396.2494 | 2.2417 | 0.3236 |
| 21 | 0.4004 | 9710.8256 | 1.2369 | 0.381 |
| 22 | 0.4957 | 1160.509552 | 2.9732 | 0.4006 |
| 23 | 1.6007 | 721.988433 | 2.6901 | 0.2001 |
| 24 | 0.392 | 1020.297227 | 4.16858 | 0.2199 |
| 25 | 0.769 | 468.871349 | 5.4764 | 0.2459 |
| 26 | 0.9334 | 448.59641 | 2.8907 | 0.2566 |
| 27 | 1.0418 | 681.54256 | 2.2584 | 0.3853 |
| 28 | 0.645 | 612.284961 | 4.0962 | 0.2314 |
| 29 | 0.665 | 577.275679 | 6.2094 | 0.258 |
| 30 | 0.5819 | 681.648059 | 4.6328 | 0.2767 |
| 31 | 0.593 | 649.404156 | 2.0147 | 0.2613 |
| 32 | 1.1901 | 857.089393 | 2.9764 | 0.2876 |

| Tiempo promedio para descifrar el reto (ms) | Tiempo promedio para generar G, P y Gx (ms) | Tiempo promedio para verificar consulta (ms) | Tiempo promedio para cifrar paquete (ms) |
| --- | --- | --- | --- |
|  |  |  |  |

### Servidor concurrente

## Cifrado asimétrico

### Servidor iterativo

| **Cifrado asimétrico** | | | | |
| --- | --- | --- | --- | --- |
| # Consulta | Tiempo para descifrar el reto (ms) | Tiempo para generar G, P y Gx (ms) | Tiempo para verificar consulta (ms) | Tiempo para cifrar paquete (ms) |
| 1 | 3.5914 | 6231.896579 | 46.4828 | 0.4088 |
| 2 | 0.9947 | 11106.5369 | 5.0492 | 0.2651 |
| 3 | 0.6612 | 6421.068562 | 5.2927 | 0.596 |
| 4 | 0.7956 | 10936.19869 | 4.5852 | 0.4352 |
| 5 | 0.4438 | 4141.832178 | 2.7533 | 0.151 |
| 6 | 0.8303 | 14822.20582 | 3.6934 | 0.2693 |
| 7 | 0.7727 | 14729.04907 | 3.6253 | 0.1559 |
| 8 | 1.0294 | 9706.899054 | 3.5882 | 0.709 |
| 9 | 0.8716 | 1853.197163 | 4.2206 | 0.2483 |
| 10 | 0.957 | 7872.605362 | 4.073 | 0.1262 |
| 11 | 1.0607 | 8657.162578 | 5.0739 | 3.7066 |
| 12 | 0.773 | 8329.65177 | 6.6107 | 0.0961 |
| 13 | 1.3931 | 11537.33983 | 5.1795 | 0.2746 |
| 14 | 0.7317 | 1268.935734 | 3.3687 | 0.2505 |
| 15 | 1.1859 | 6693.767442 | 5.0016 | 0.2564 |
| 16 | 1.2269 | 14368.17317 | 5.4324 | 0.2951 |
| 17 | 1.3165 | 14219.24146 | 3.9885 | 0.1723 |
| 18 | 1.3431 | 6259.283981 | 4.257 | 0.1279 |
| 19 | 1.0066 | 443.602954 | 4.5479 | 0.1959 |
| 20 | 1.4232 | 8649.177434 | 4.1473 | 0.2107 |
| 21 | 0.8091 | 569.508026 | 5.6475 | 0.1259 |
| 22 | 1.4238 | 14031.09166 | 8.9425 | 0.261 |
| 23 | 0.8263 | 8692.455973 | 3.4896 | 0.3036 |
| 24 | 1.23 | 8140.568462 | 3.1782 | 0.2059 |
| 25 | 0.7918 | 14558.74831 | 3.2906 | 0.2759 |
| 26 | 1.1245 | 12548.76732 | 3.2214 | 0.2078 |
| 27 | 1.2026 | 1579.518746 | 6.7817 | 0.1919 |
| 28 | 1.0557 | 1555.568331 | 3.4824 | 0.2963 |
| 29 | 0.8025 | 8708.84082 | 3.6626 | 0.2743 |
| 30 | 0.6941 | 12848.74325 | 3.2405 | 0.2382 |
| 31 | 1.0223 | 14407.1804 | 3.7294 | 0.2047 |
| 32 | 1.1008 | 8570.927905 | 3.3543 | 0.2398 |

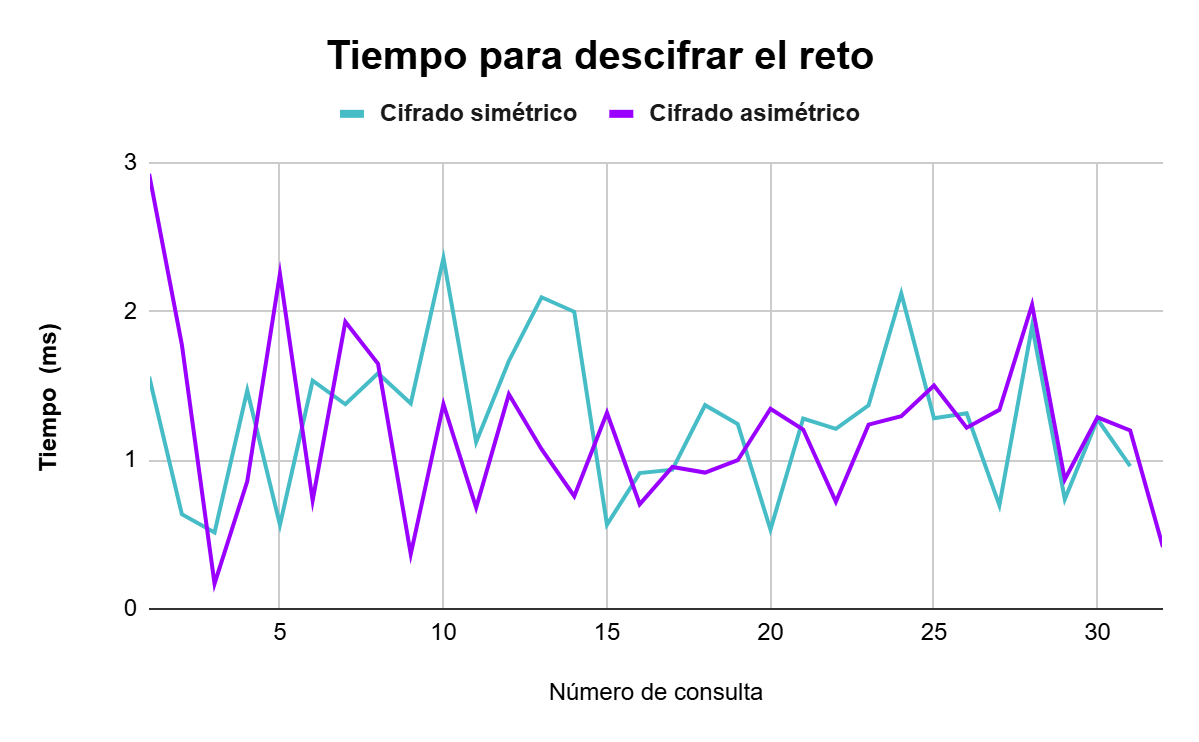
| Tiempo promedio para descifrar el reto (ms) | Tiempo promedio para generar G, P y Gx (ms) | Tiempo promedio para verificar consulta (ms) | Tiempo promedio para cifrar paquete (ms) |
| --- | --- | --- | --- |
|  |  |  |  |

### Servidor concurrente

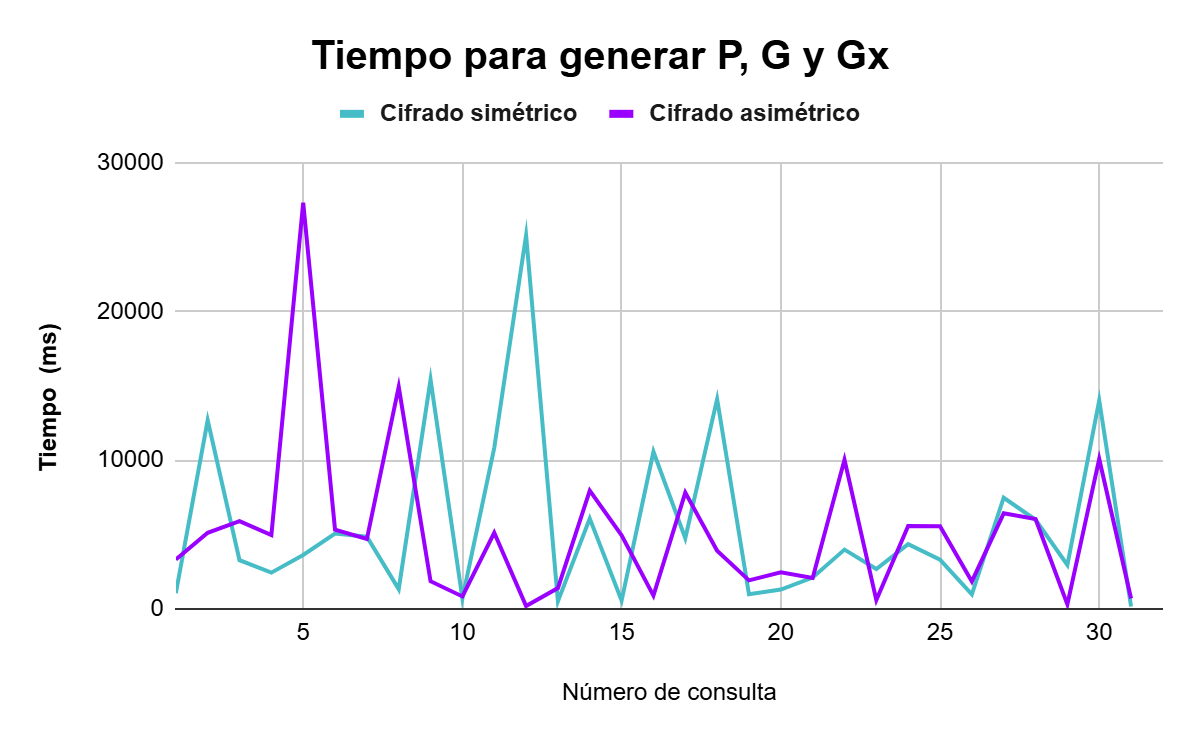
### 

# Gráficas y análisis de resultados

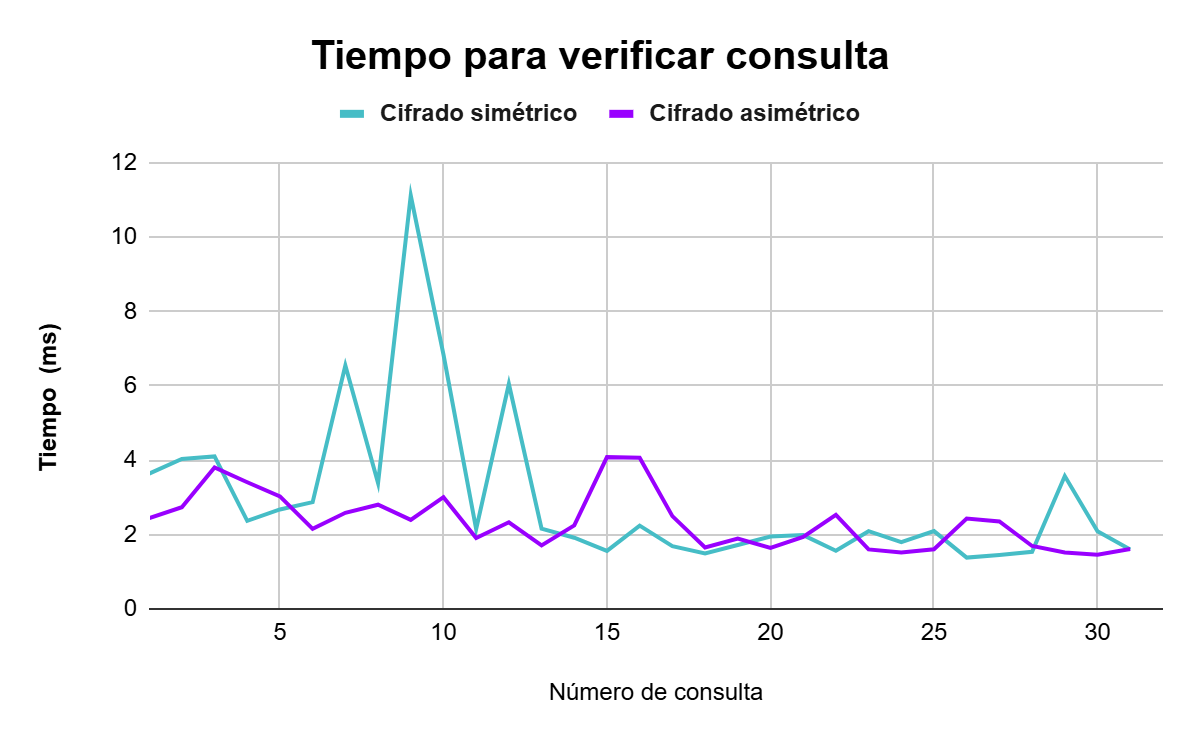
## Cifrado simétrico vs cifrado asimétrico en servidor iterativo



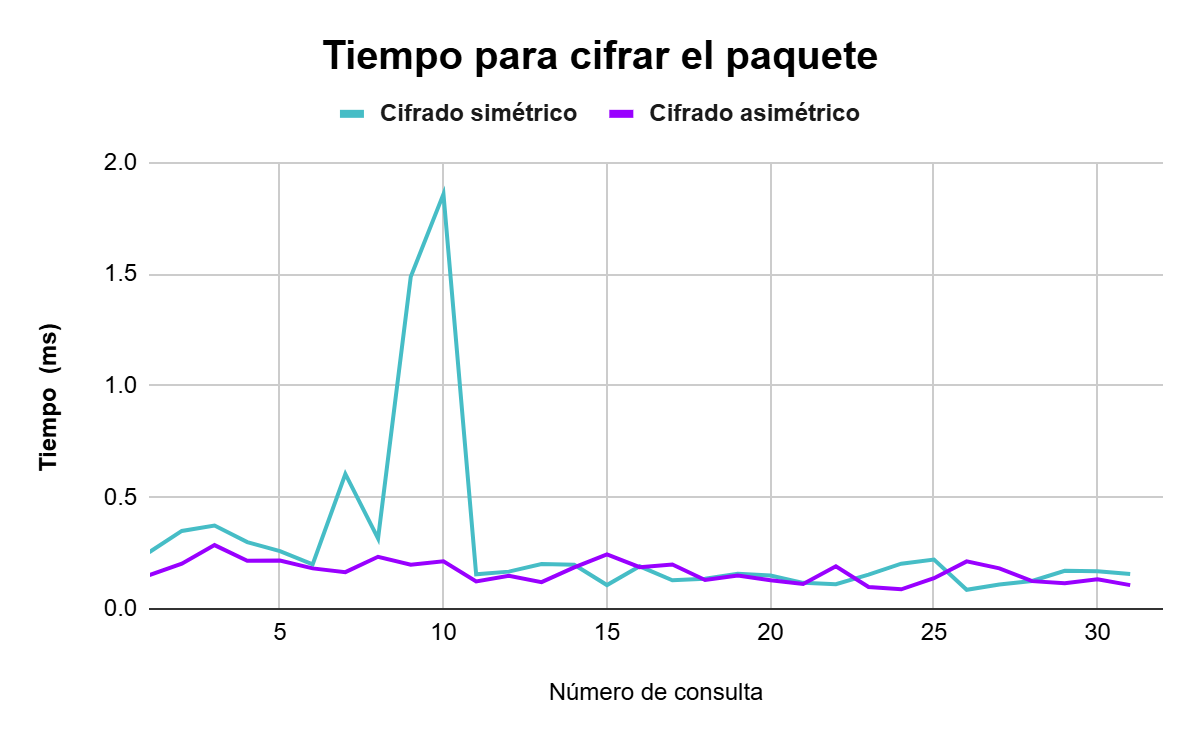
Al observar la gráfica, se puede evidenciar que el tiempo de descifrado con cifrado asimétrico es un poco más constante en comparación con el cifrado simétrico. No obstante, el cifrado asimétrico, presenta un pico muy pronunciado al inicio, indicando un tiempo alto en la primera consulta. Después de este inicio elevado, los tiempos del cifrado asimétrico se estabilizan, aunque siguen variabilidad, al igual que el estado simétrico.

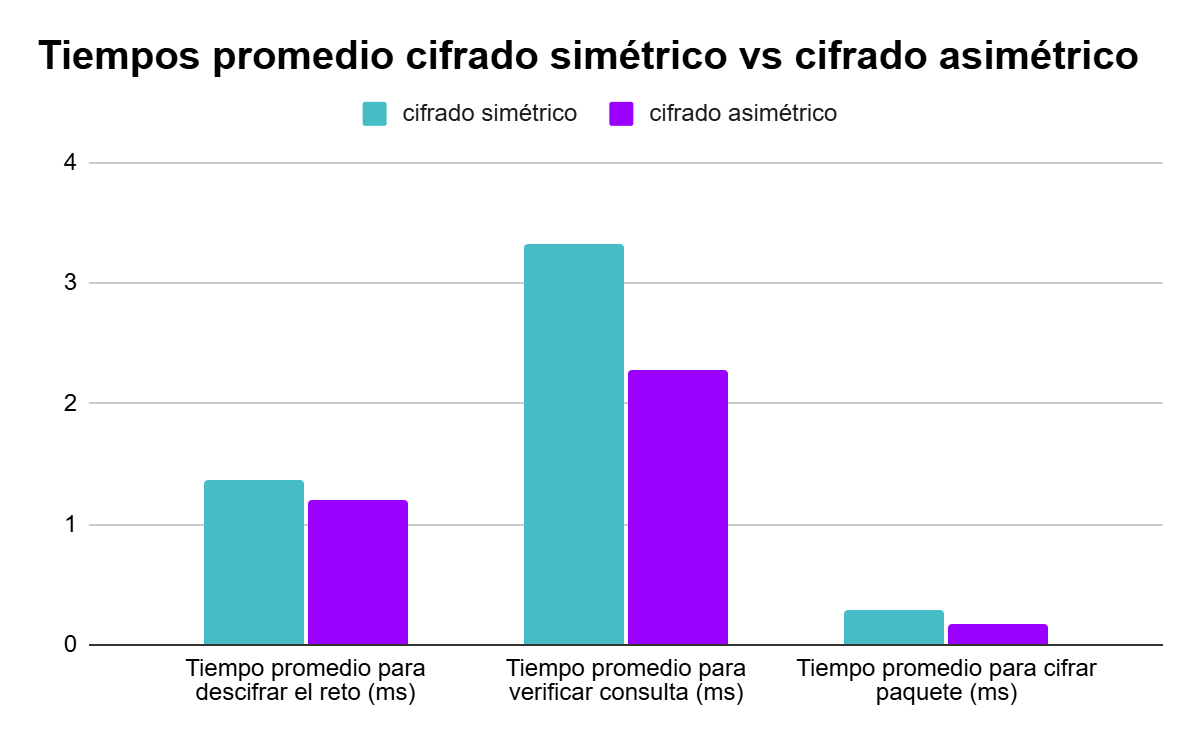


Al observar la gráfica, se puede evidenciar que el tiempo de ambos cifrados, tanto el cifrado simétrico como el asimétrico, presentan una alta variabilidad en los tiempos para generar los parámetros .



Al observar la gráfica, se puede evidenciar que el cifrado asimétrico presenta tiempos generalmente menores en comparación con el cifrado simétrico

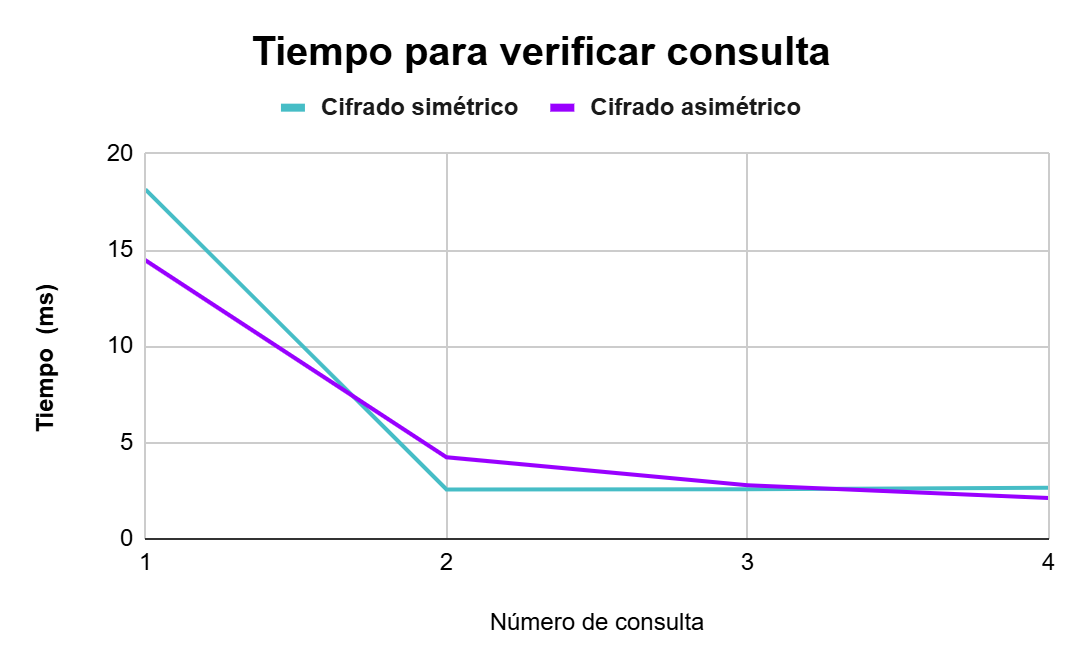


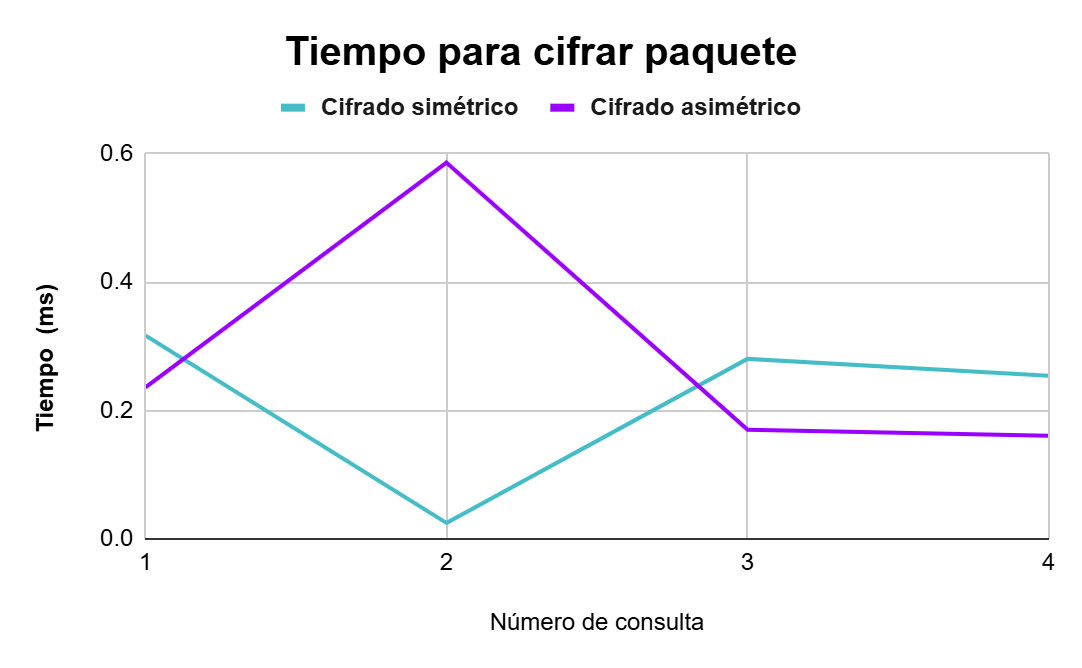


## Cifrado simétrico vs cifrado asimétrico en servidor concurrente

### Con 4 delegados

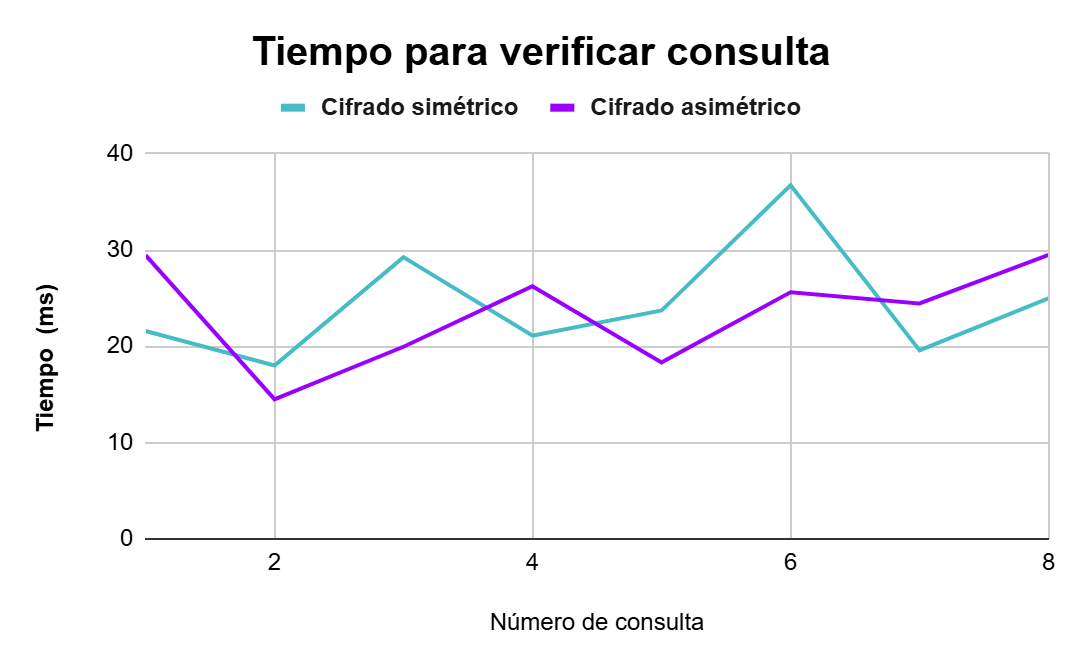
### 

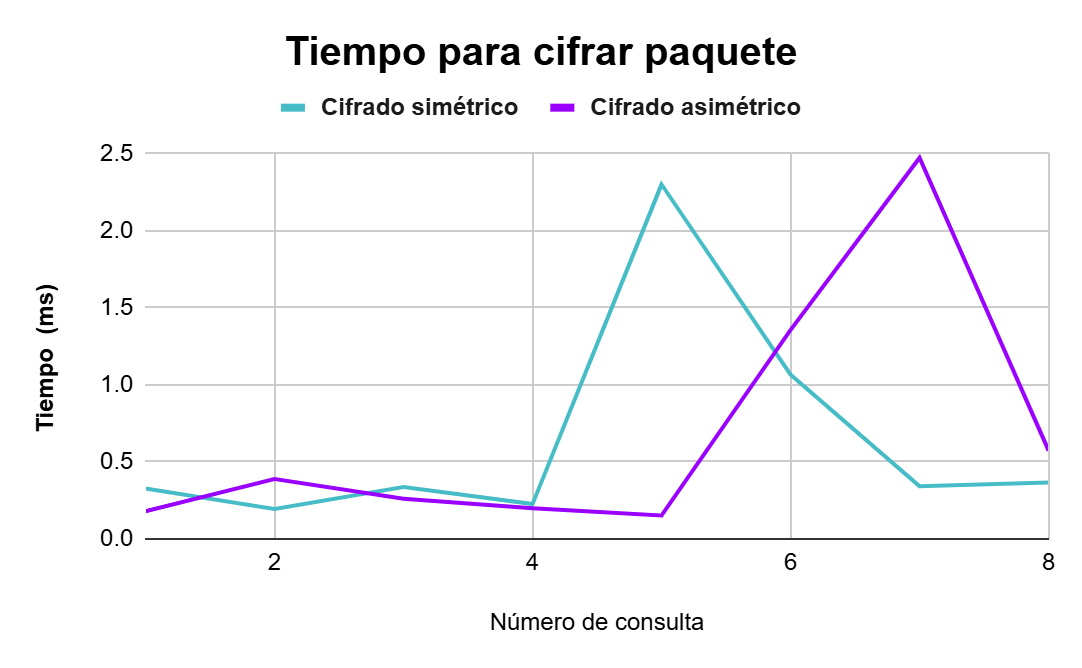




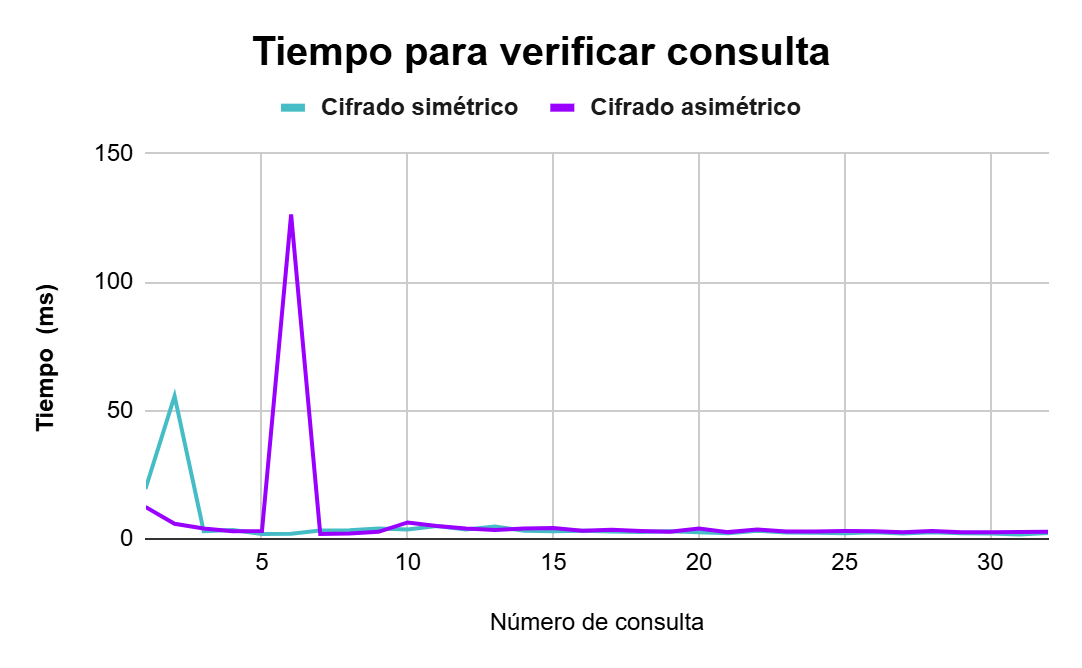
### Con 8 delegados

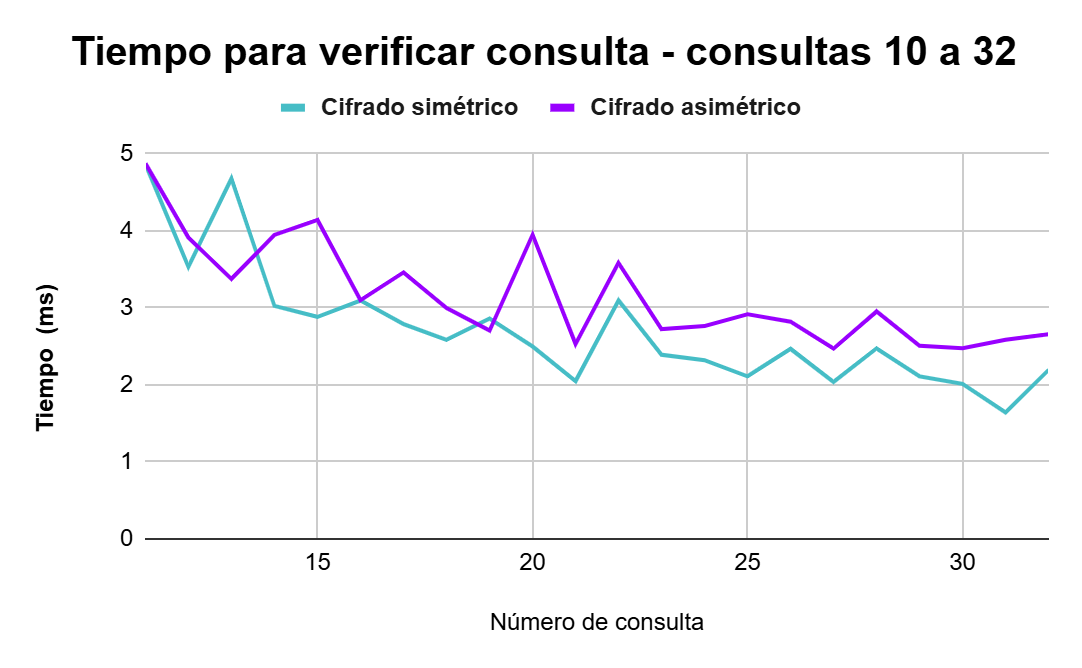
### 

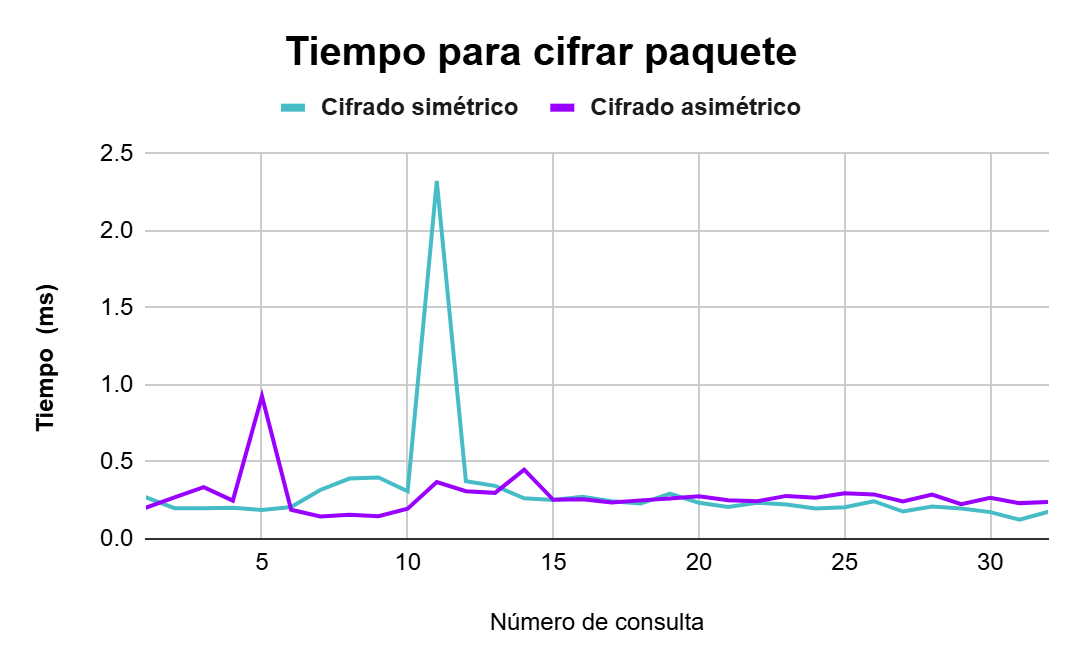


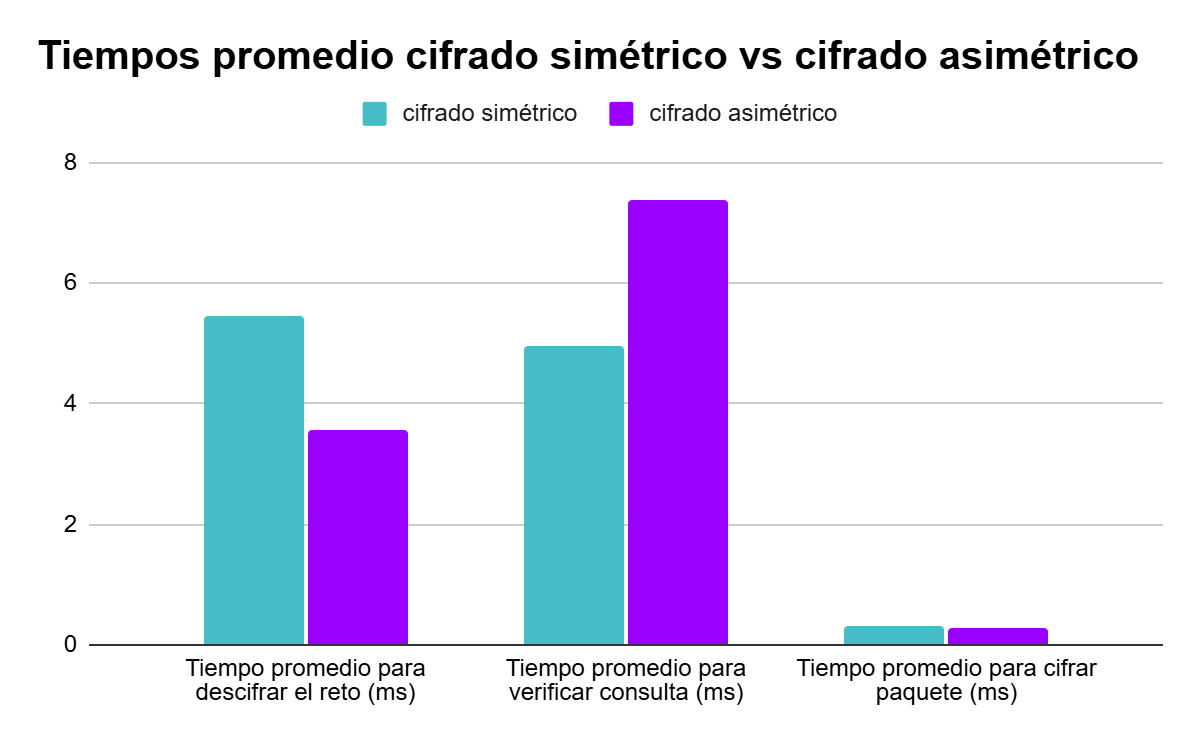


### Con 32 delegados



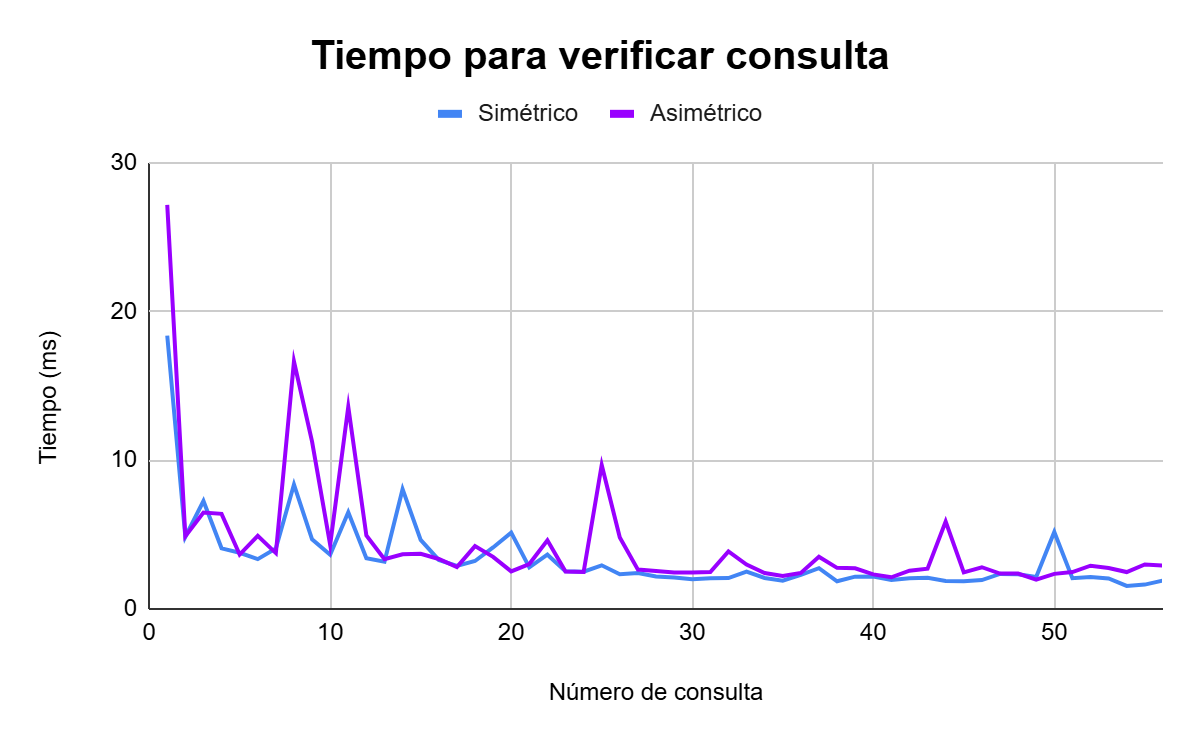


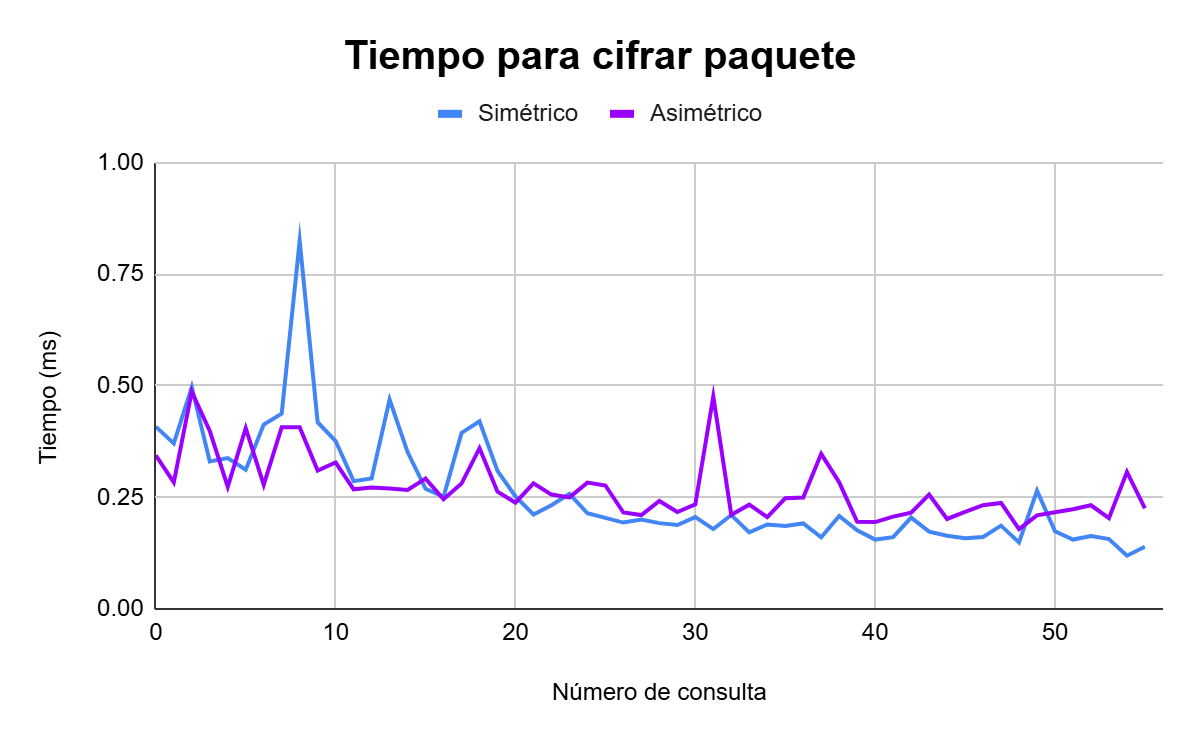




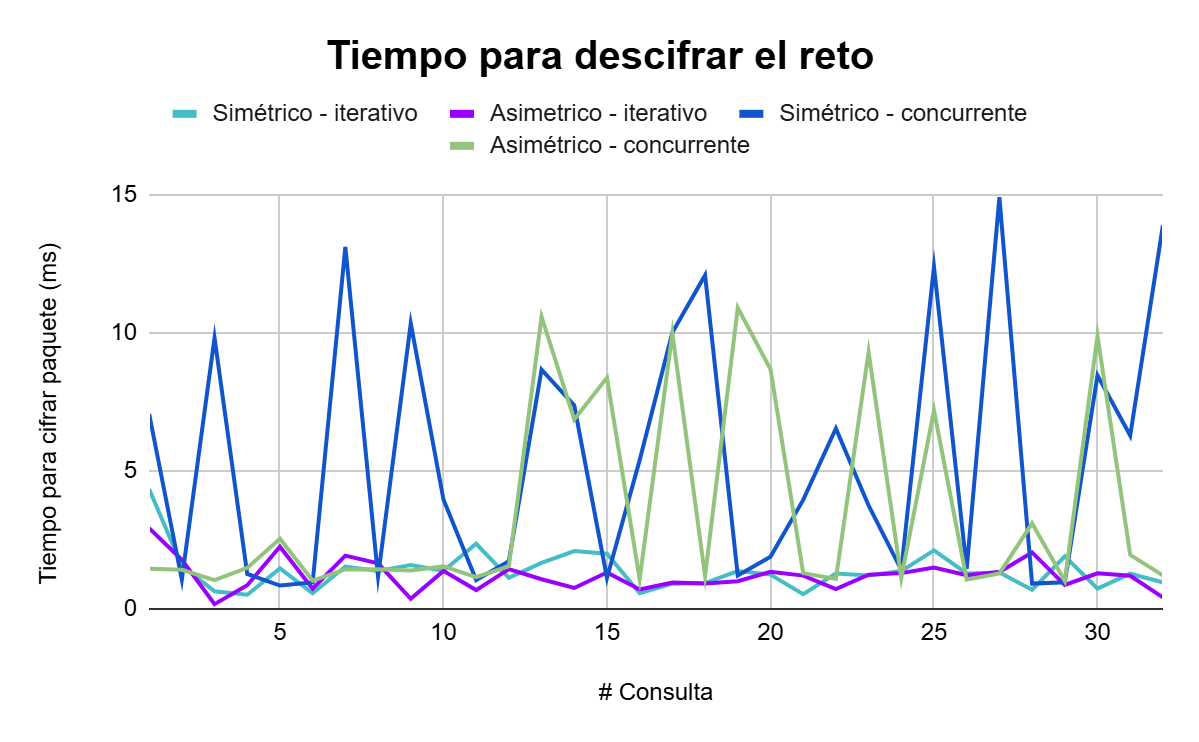
### Caso adicional: mayor número de clientes concurrentes

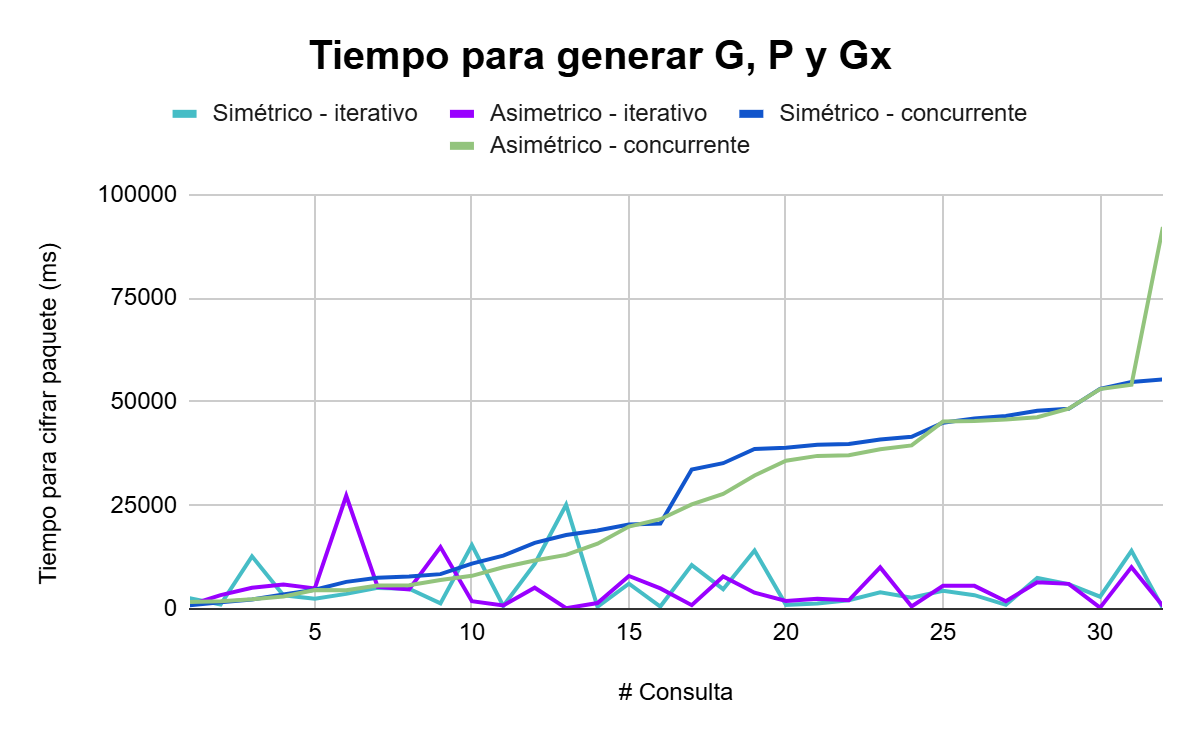
Para este caso, se hizo la prueba con 56 clientes y 56 delegados. A continuación se muestran los resultados

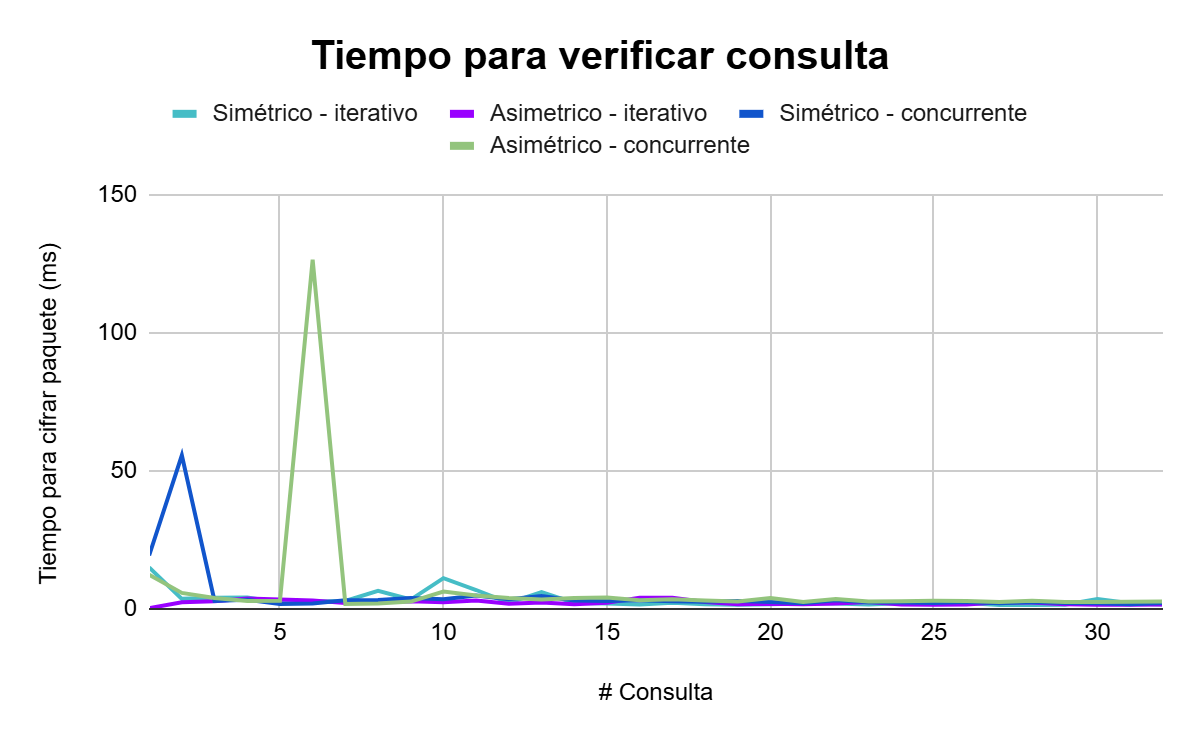


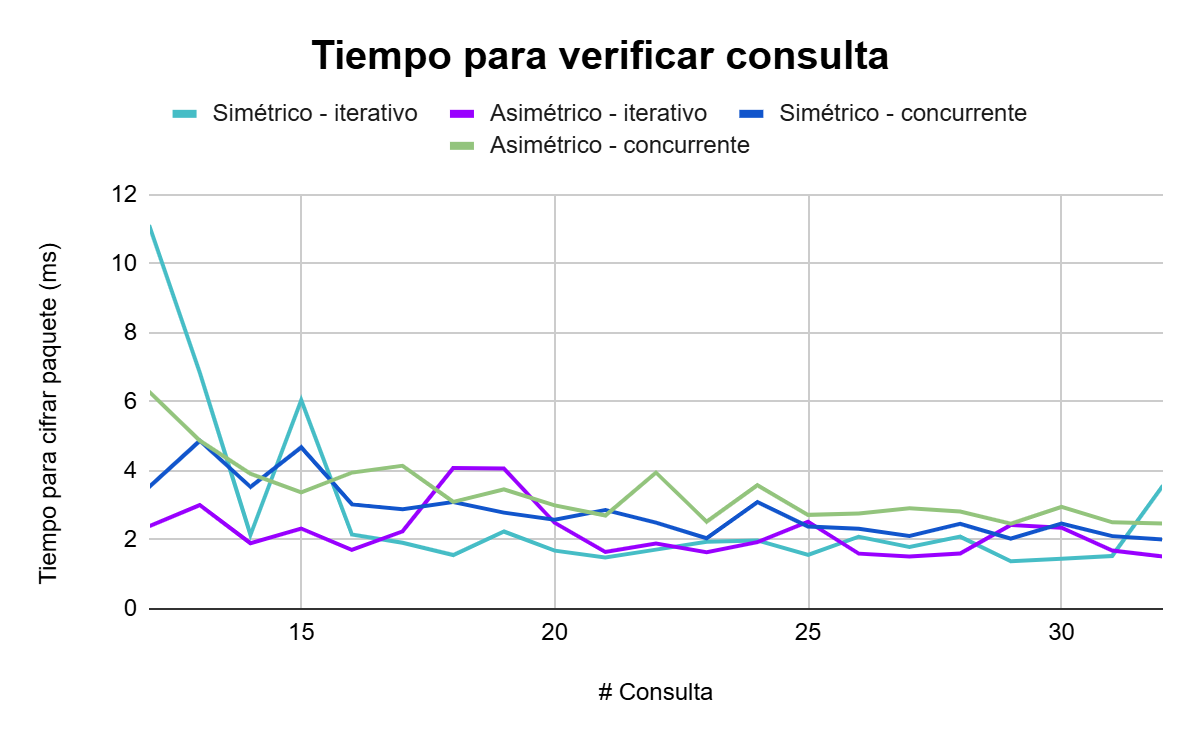


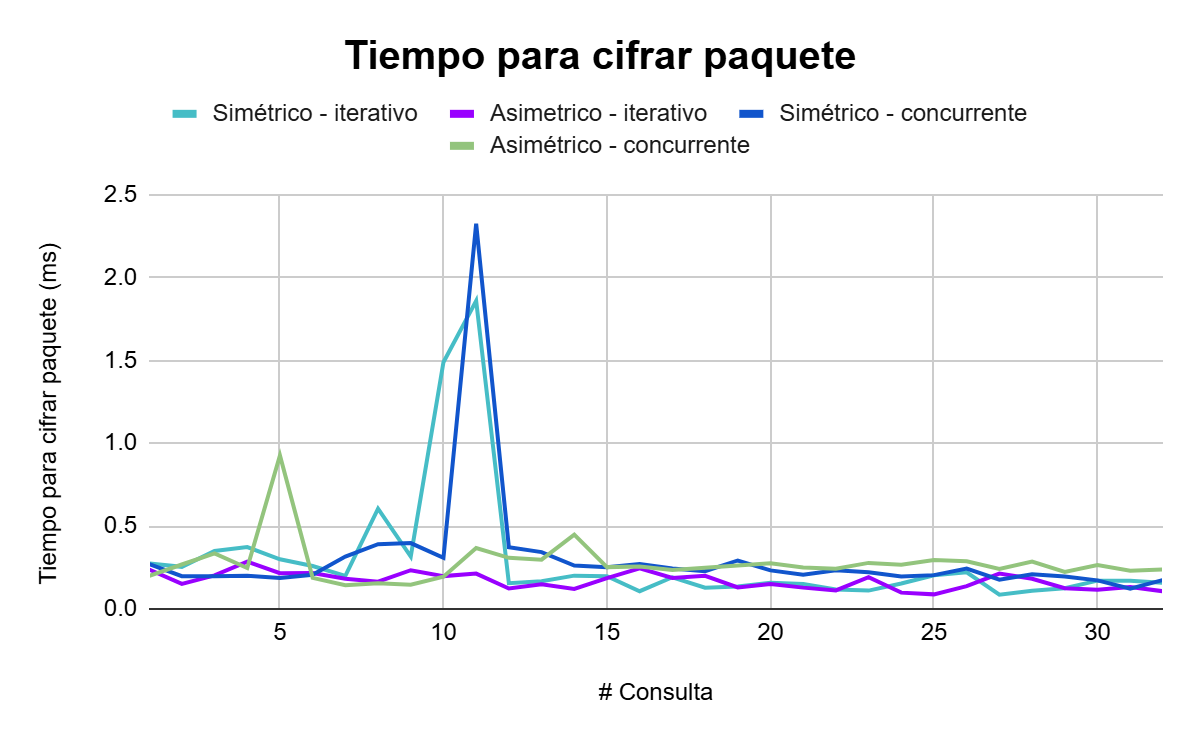
## Servidor concurrente vs servidor iterativo

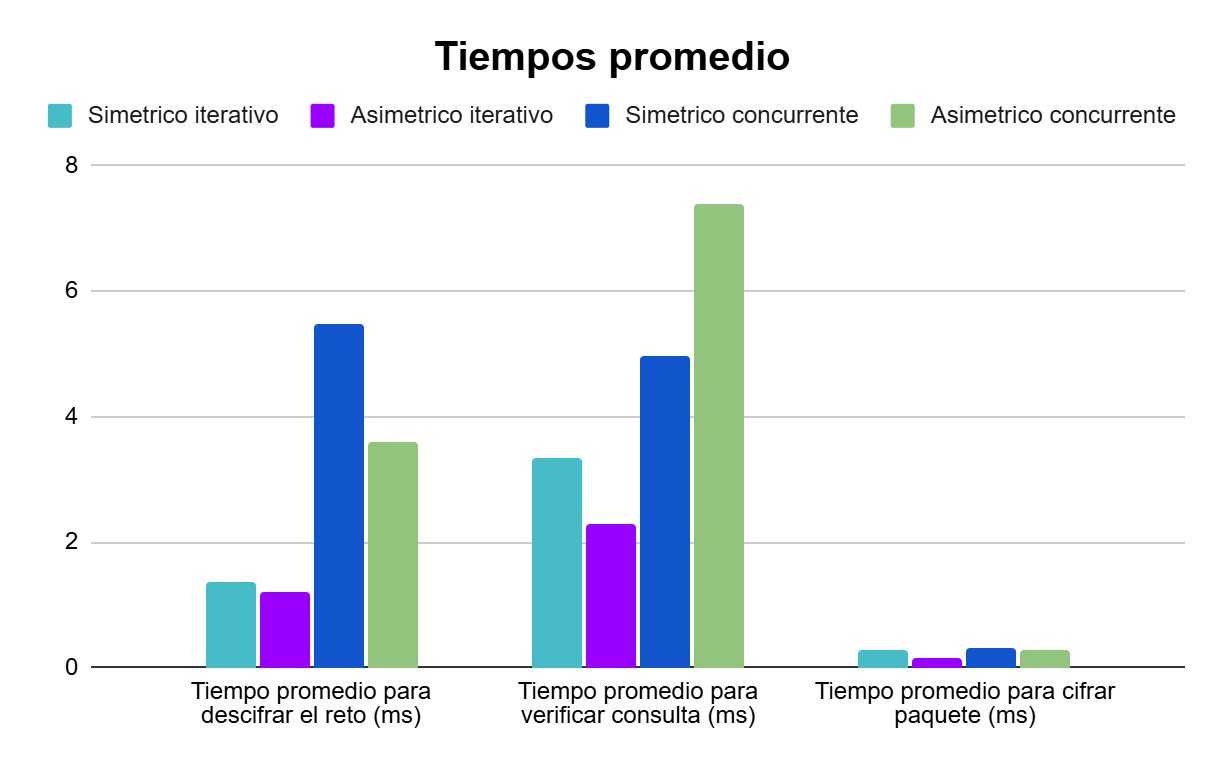












# Respuestas a las preguntas planteadas

## Estimación de velocidad del procesador

## Estimación de cantidad de operaciones por segundo

### Caso simétrico

Con las pruebas hechas, puede obtenerse un valor aproximado del promedio de todos los tiempos que se demora el equipo para realizar una operación de cifrado simétrico.

Este promedio corresponde a la suma del tiempo promedio que se demora en cifrar el estado del paquete con la llave simétrica en el caso iterativo y el tiempo promedio que se demora en cifrar el estado del paquete con la llave simétrica en el caso concurrente, dividido entre 2. De esta manera:

Ahora bien, sabiendo que el equipo es capaz de hacer un cifrado simétrico en aproximadamente ms entonces, el número de operaciones de cifrado que puede realizar en 1 segundo puede encontrarse mediante la siguiente expresión

Así, se puede decir que el equipo puede ejecutar aproximadamente 3312 operaciones de cifrado simétrico en 1 segundo.

### Caso asimétrico

Con las pruebas hechas, puede obtenerse un valor aproximado del promedio de todos los tiempos que se demora el equipo para realizar una operación de cifrado asimétrico.

Este promedio corresponde a la suma del tiempo promedio que se demora en cifrar el estado del paquete con la llave asimétrica en el caso iterativo y el tiempo promedio que se demora en cifrar el estado del paquete con la llave asimétrica en el caso concurrente, dividido entre 2. De esta manera:

Ahora bien, sabiendo que el equipo es capaz de hacer un cifrado asimétrico en aproximadamente ms entonces, el número de operaciones de cifrado que puede realizar en 1 segundo puede encontrarse mediante la siguiente expresión

Así, se puede decir que el equipo puede ejecutar aproximadamente 4486 operaciones de cifrado asimétrico en 1 segundo.