Reto 3 - Doc

1. Corra su programa en diferentes escenarios y mida el tiempo que el servidor requiere para:
   Responder el reto, (ii) generar G, P y Gx , (iii) verificar la consulta. Los escenarios son:
   i)Un servidor y un cliente iterativos. El cliente genera 32 consultas.
   (ii) Un servidor y un cliente que implementen delegados. El número de delegados, tanto servidores como clientes, debe variar entre 4, 8, y 32 delegados concurrentes. Cada cliente genera una sola solicitud.

2. Construya una tabla con los datos recopilados. Tenga en cuenta que necesitará correr cada escenario en más de una ocasión para validar los resultados.

Tiempo en segundos Servidor y cliente iterativos			
Responder el Reto	Generar G, P Gx	Verificar la consulta	Numero de consultas
0.011	43.5	0.001	1
0.78	6.99	0.01	2
0.007	16.56	0.002	3
0.005	14.96	0.002	4
0.006	53.30	0.001	5
0.01	10.91	0.007	6
0.006	20.15	0.001	7
0.004	14.66	0.001	8
0.004	9.01	0.0007	9
0.004	11.41	0.001	10
0.007	14.68	0.001	11
0.006	10.44	0.001	12
0.005	14.41	0.0009	13
0.003	14.64	0.001	14
0.004	14.89	0.0009	15
0.004	12.73	0.001	16
0.007	5.54	0.001	17
0.006	24.76	0.0009	18
0.010	2.96	0.0008	19
0.003	4.42	0.003	20
0.005	16.53	0.001	21
0.007	5.09	0.001	22
0.003	35.09	0.0006	23
0.003	15.97	0.001	24
0.004	11.32	0.0009	25
0.003	13.05	0.0008	26
0.004	9.9	0.001	27
0.005	2.19	0.0008	28
0.009	3.62	0.001	29
0.004	2.61	0.0007	30
0.003	13.52	0.0007	31
0.004	17.97	0.002	32

Tiempo Total en segundos Servidor y Cliente Iterativos, 32 consultas	
Responder el reto	0.9656
P , G ,Gx	467.97
Verificar consulta	0.05997

Tiempo total en segundos Servidor y cliente con delegados, 4 delegados	
Responder el reto	2.81
P , G ,Gx	144.02
Verificar consulta	0.0098

Tiempo total en segundos Servidor y cliente con delegados, 8 delegados	
Responder el reto	7.74
P , G ,Gx	224.85
Verificar consulta	0.0195

Tiempo total en segundos Servidor y cliente con delegados, 32 delegados	
Responder el reto	34.33
P , G ,Gx	2988.93
Verificar consulta	0.0612

Promedio en segundos Servidor y Cliente Iterativos, 32 consultas	
Responder el reto	0.0302
P , G ,Gx	146.241
Verificar consulta	0.0019

Promedio en segundos Servidor y Cliente delegados , 4 delegados	
Responder el reto	0.3919
P , G ,Gx	51.394
Verificar consulta	0.0009

Promedio en segundos Servidor y Cliente delegados , 8 delegados	
Responder el reto	0.4325
P , G ,Gx	126.914
Verificar consulta	0.0013

Promedio en segundos Servidor y Cliente delegados , 32 delegados	
Responder el reto	0.5780
P , G ,Gx	354.167
Verificar consulta	0.0008

3. Mida el tiempo que el servidor requiere para cifrar el estado del paquete con cifrado simétrico y con cifrado asimétrico. Observe que el cifrado asimétrico de este valor no se usa en el protocolo, solo se calculará para posteriormente comparar los tiempos.

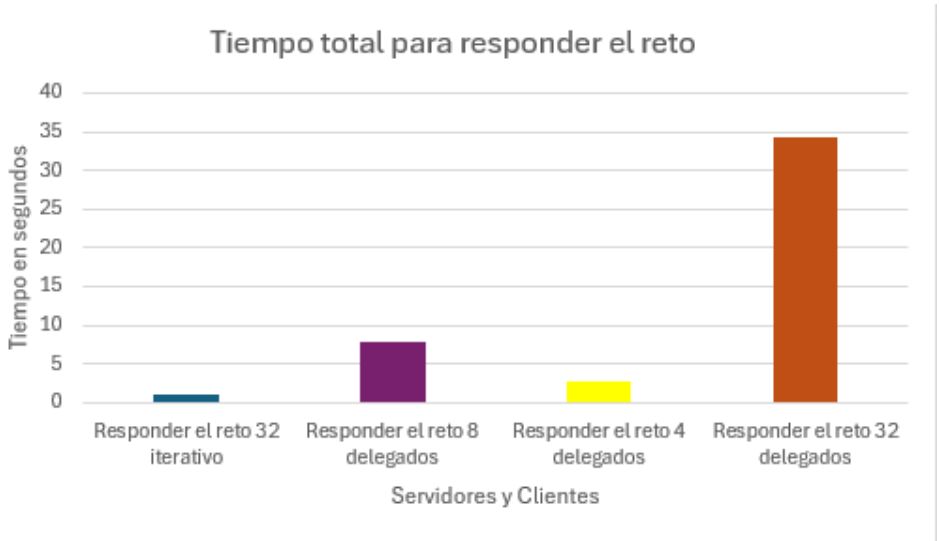
Iterativo 5 consultas	
Tiempo consulta simetrico	Tiempo consulta asimetrico
0,00027	0,00052

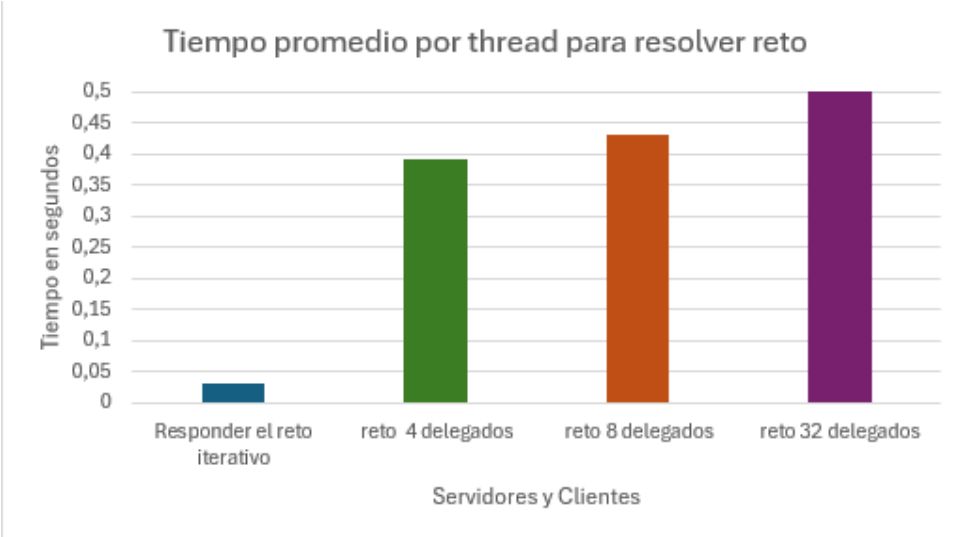
Con delegados 5 delegados	
Tiempo consulta simetrico	Tiempo de consulta asimetrico
0.00027	0.00075

Tipo de cifrado	32 consultas iterativo	4 delegados	8 delegados	32 delegados
Asimetrico	0.00052	0.00129	0.00085	0.00043
Simetrico	0.00022	0.00043	0.00029	0.00023

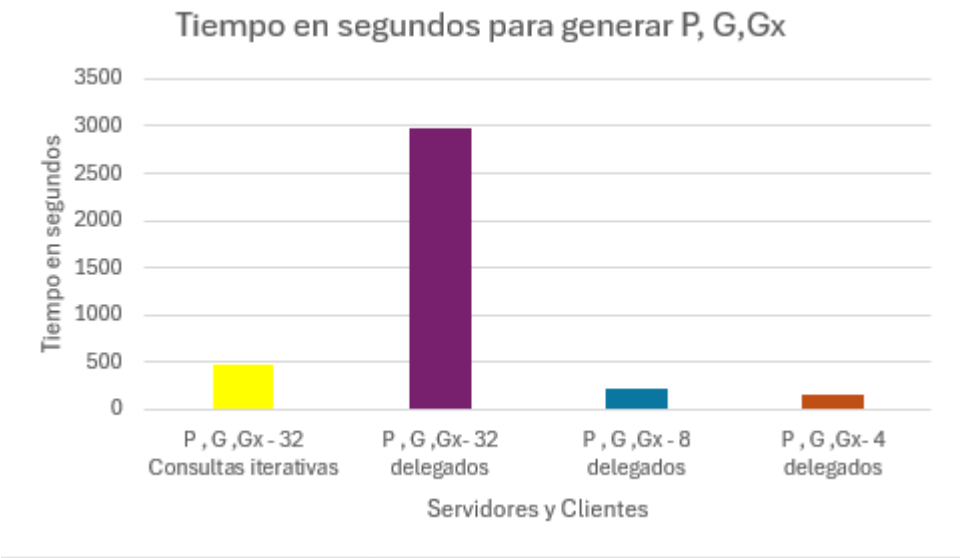
4. Construya las siguientes gráficas:

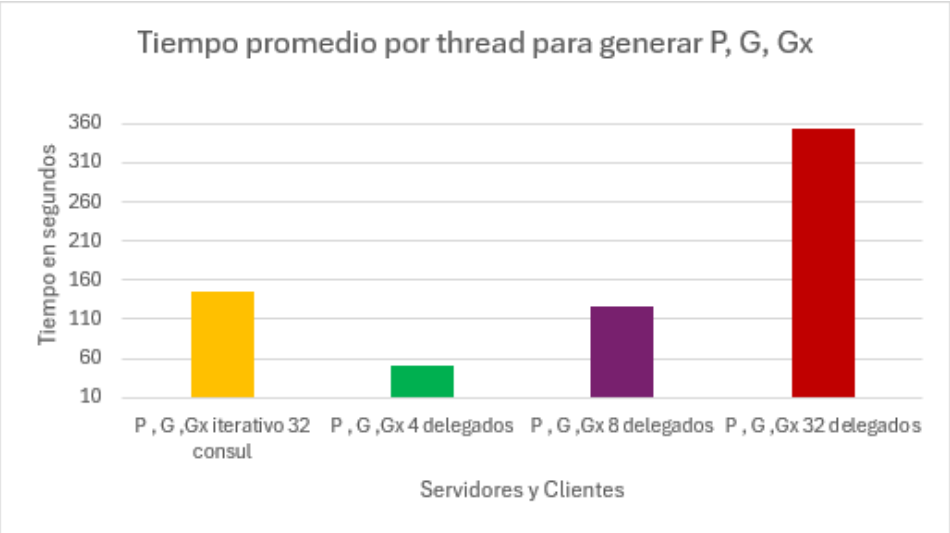
(i) Una que compare los tiempos para descifrar el reto en los diferentes escenarios



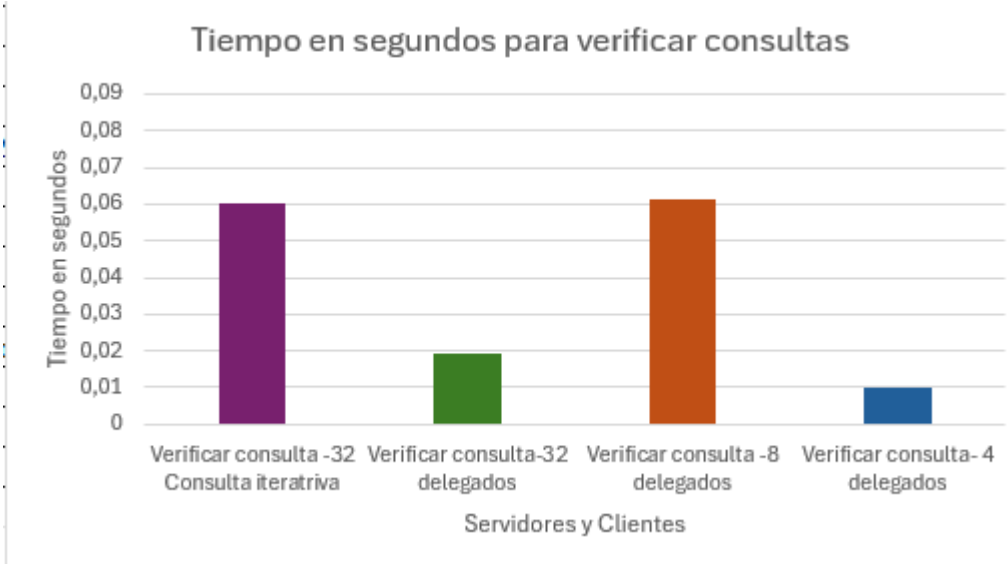


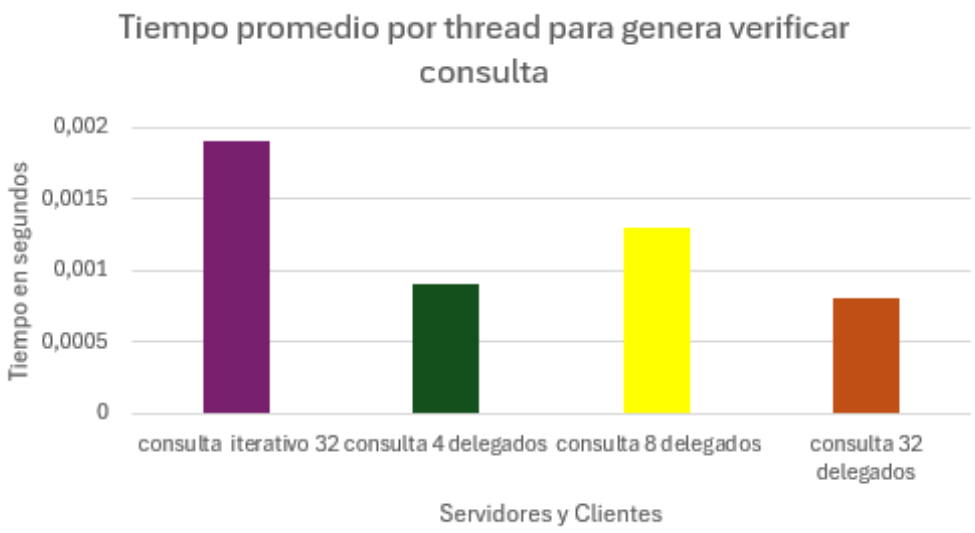
(ii) Una que compare los tiempos para generar G, P y Gx en los diferentes escenarios



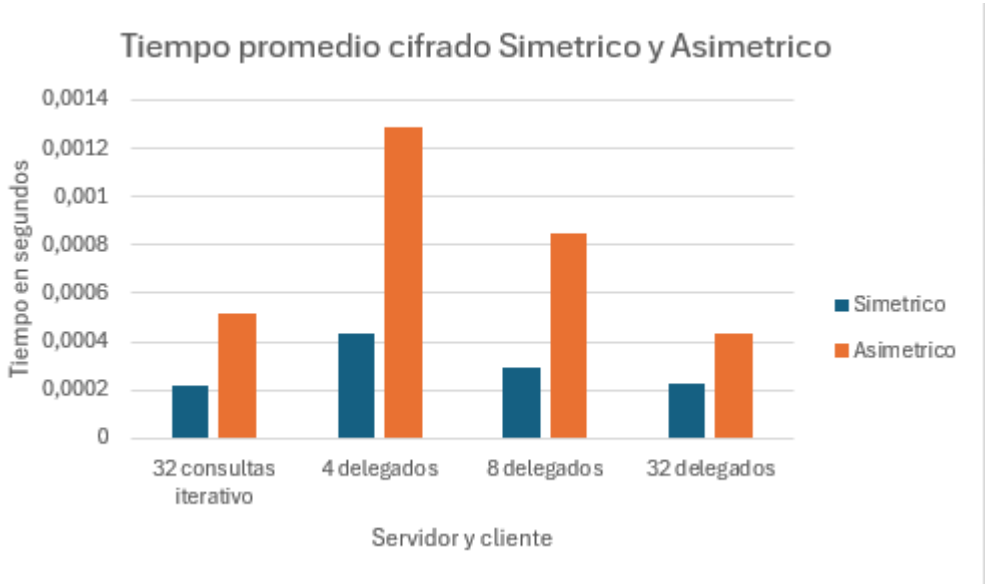


(iii) Una que muestre los tiempos para verificar la consulta en los diferentes escenarios





(iv) Una que muestre los tiempos para el caso simétrico y el caso asimétrico en los diferentes escenarios



5. Escriba sus comentarios sobre las gráficas, explicando los comportamientos observados.

Análisis tiempo para responder reto: Se observa que 32 delegados utilizan el mayor tiempo en promedio, pero 32 consultas iterativas consumen menos tiempo total y promedio lo que sugiere que es mejor evitar el paralelismo en esta consulta, con 4 y 8 delegados el tiempo es menor.
El tiempo promedio por thread aumenta con el número de delegados, alcanzando el máximo con 32 delegados. Esto refleja que a medida que se incrementa la cantidad de

threads, cada uno se vuelve menos eficiente, posiblemente debido a la mayor carga de coordinación y el acceso compartido a los recursos.

Análisis tiempo para generar P, G y Gx: La configuración de 32 delegados presenta el tiempo total más alto, lo que sugiere una significativa sobrecarga al coordinar tantos threads. Las configuraciones de 4 y 8 delegados tienen tiempos considerablemente menores en comparación con la de 32 delegados, lo que indica una mejora en la eficiencia al reducir el número de threads. La configuración de consultas iterativas de 32 también muestra un tiempo total bajo, destacándose como una alternativa eficiente sin paralelismo. La configuración iterativa de 32 consultas y la configuración de 4 delegados tienen el menor tiempo promedio por thread, lo que indica una mayor eficiencia en comparación con configuraciones con más threads.
La configuración de 32 delegados presenta el tiempo promedio por thread más alto, lo cual indica que, aunque haya más threads, cada uno se vuelve menos eficiente debido a la sobrecarga adicional.

Análisis tiempo para verificar consulta: La configuración iterativa de 32 consultas y la de 8 delegados muestran tiempos relativamente altos, con la configuración de 8 delegados siendo la más alta. La configuración con 32 delegados tiene el tiempo total más bajo, lo que implica que, en este caso, dividir la tarea en más threads parece beneficiar el rendimiento general al reducir el tiempo total de verificación. La configuración iterativa y la de 8 delegados muestran el tiempo promedio por thread más alto, lo que indica una baja eficiencia en comparación con otras configuraciones.
La configuración de 32 delegados tiene el menor tiempo promedio por thread, lo cual sugiere que con más threads, cada uno tiene una carga menor y logra ejecutar la tarea de verificación de manera más rápida.

Análisis tiempo cifrado asimétrico y cifrado simétrico: En todas las configuraciones, el tiempo promedio para el cifrado asimétrico es consistentemente mayor que el del cifrado simétrico. Esto es esperable, ya que el cifrado asimétrico, generalmente, requiere más tiempo de procesamiento debido a su complejidad y al manejo de claves públicas y privadas.

6. Identifique la velocidad de su procesador, y estime cuántas operaciones de cifrado puede realizar su máquina por segundo, en el caso evaluado de cifrado simétrico y cifrado asimétrico. Escriba todos sus cálculos.

Procesador Core i7vPro

Velocidad de procesamiento = 4.80 GHz

F = 4.80 x 10 a la 9ciclos por segundo

Operaciones por segundo = 1 / T

Tiempo promedio cifrado asimétrico: 0.00043

Tiempo promedio cifrado simétrico: 0.00023

Operación de cifrado Simétrico: 1 /Tsimetrico = (1/0.00023) = 4347.83

Operación de cifrado Asimétrico: 1 /TAsimetrico = (1/0.00043) = 2325.58

4348 operaciones de cifrado simétrico por segundo.

2326 operaciones de cifrado asimétrico por segundo.