Documentación.

Carlos Figueredo – 201813445

Erik Nielsen – 201913493

Descripción de organización de archivos

src: Este directorio contiene los .java para las funciones principales del caso.

llavesAsimetricas: Contiene las llaves públicas y privadas de cada cliente, repartidor y servidor.

llavesSimetricas: Contiene las llaves secretas de cada cliente, repartidor y servidor.

docs: Contiene documentos descriptivos

Instrucciones para ejecutar:

Empiece modificando el archivo escenario.txt el cual especifica cuántos clientes quiere ejecutar y si quiere que sea con cifrado simétrico (1) o asimétrico (2). Posteriormente, ejecute el archivo main.java dentro del directorio src.

Generación de llaves:

Las llaves secretas (cifrado simétrico) se generaron con algoritmo AES, modo ECB, esquema de relleno PKCS5 y un tamaño de 128 bits. Se generaron con la clase GenerarLLaveSimetrica.java, que está contenida en el paquete Auxiliares. Las llaves se guardaron en la carpeta llavesSimetricas, siguen un esquema para las llaves entre cliente y repetidor, id indica el número de identificación del cliente, que es el mismo que el del repetidor delegado. Las llaves entre repetidor y servidor siguen el esquema, donde id es el identificador del repetidor delegado, que es el mismo que el del servidor delegado.

Las llaves públicas y privadas (cifrado asimétrico) se generaron con algoritmo RSA y tamaño de 1024 bits. Se generaron con la clase GenerarLLavesAsimetricas.java, que está contenida en el paquete Auxiliares. Las llaves se guardan en la carpeta llavesAsimetricas, siguen un esquema para la llave pública del cliente con identificación “id”, para la llave privada del cliente con identificación “id”. Lo mismo ocurre con los repetidores y servidores delegados, pero cambian la C por la R o por la S, respectivamente.

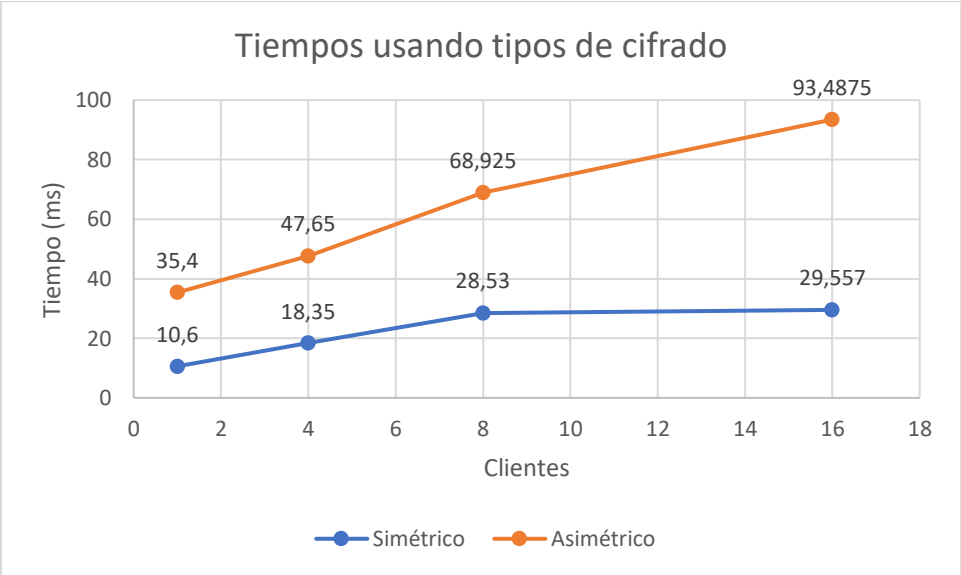
Desarrollo de tareas:

1. Para obtener unos tiempos mas concisos, se realizaron5 iteraciones en ambos algoritmos, los tiempos están detallados en la siguiente tabla:

		Tiempo en repetidor (ms)					
Cifrado	Clientes	Iteración 1	Iteración 2	Iteración 3	Iteración 4	Iteración 5	Promedio
Simétrico	1	11	13	12	8	9	10,6
	4	22,5	17	18,25	15,75	18,25	18,35
	8	32	21,65	22,875	33,125	33	28,53
	16	21,875	34,75	23,93	30,56	36,67	29,557
Asimétrico	1	32	40	44	31	30	35,4
	4	41,75	40,75	51,25	54,25	50,25	47,65
	8	90	58,75	52,25	67	76,625	68,925
	16	102,25	107,1875	69,6875	92,5	95,8125	93,4875

2.

Con base en los datos obtenidos en la tabla anterior, se obtiene la siguiente grafica con 2 series, la primera serie corresponde al algoritmo de cifrado simétrico y la segunda al algoritmo de cifrado asimétrico con sus respectivos numero de clientes y tiempos.



3.

Como podemos ver en el grafico obtenido, el algoritmo de cifrado asimétrico se demoro mas tiempo, independientemente del numero de clientes. Este resultado era de esperarse, debido a que algoritmo de cifrado asimétrico es mucho mas seguro, pero a su vez es mas costos en tiempo. Adicionalmente, con ayuda de la grafica se puede evidenciar que los tiempos son directamente proporcionales al número de clientes, con la diferencia que en el algoritmo de cifrado asimétrico el tiempo aumenta de manera exponencial cuando aumenta el número de clientes.

4.

Si se tiene un procesador de 3,7 GHZ, este podrá realizar $3{,}7 * 10^9 \frac{ciclos}{segundo}$, basado en estos datos se calcula el numero promedio de ciclos con :

$$Promedio\ Ciclos = \frac{3{,}7*10^9 \frac{ciclos}{segundo} * tiempo\ promedio\ en\ seg}{número\ de\ clientes}$$

El promedio de ciclos se halla para los dos algoritmos de cifrado, dándonos como resultado la siguiente tabla:

Cifrado	Clientes	Ciclos que toma:	Promedio de ciclos
Simétrico	1	39220000	19055982,81
	4	16973750	
	8	13195125	
	16	6835056,25	
Asimétrico	1	130980000	57138261,72
	4	44076250	
	8	31877812,5	
	16	21618984,38	

Finalmente, dentro del directorio se anexa el archivo de Excel que se utilizó para realizar los cálculos respectivos.