Documentación Caso 3 InfraComp
Juan Pablo Reyes Romero
Juan Sebastián Maldonado

1. Organización de los Archivos en Zip

Los archivos dentro del zip de entrega son los siguientes:

- ClientePrincipal.java
- ServidorPrincipal.java
- CryptoUtils.java
- Private.key
- Public.key
- Docs – *subdirectorio del informe*

La lógica del caso y los involucrados en su funcionamiento son los tres primeros archivos en la lista, estos hacen uso de los dos archivos .key, generados para simular los procesos llevados a cabo. Adicionalmente, cabe destacar que se encuentra la carpeta docs, en donde se encontrará el archivo pdf el informe (archivo está siendo leído). Igualmente, estos son los archivos que se solicitan para la entrega, ya que se excluye a los .class, que, por instrucciones en el enunciado, no se tienen en cuenta para la entrega, a pesar de tener que ser generados posteriormente.

2. Instrucciones para Ejecución del Caso

Para poder llevar a cabo la ejecución del caso, se requiere la descarga del zip enviado, así como su descompresión. Posteriormente, teniendo en un editor de código todos los archivos previamente mencionados, se debe de ejecutar el siguiente comando:

```
javac CryptoUtils.java ServidorPrincipal.java ClientePrincipal.java
```

Lo que se hace con el anterior comando es la generación de los archivos .class, que son necesarios para la ejecución del programa.

Ahora bien, se requiere la apertura de dos terminales diferentes, para poder llevar a cabo los procesos designados. En caso general, e independientemente del escenario que se desee correr, se inicializa el servidor a través del siguiente comando:

```
java ServidorPrincipal
```

En caso de que se genere algún error, se podría probar el siguiente comando:

```
java ServidorPrincipal.java
```

Lo anterior es por razones desconocidas, ya que, para el caso de este caso, un integrante usó Windows, y el otro MacOS, en donde el primer comando funcionó para la primera máquina, y el segundo para la segunda, respectivamente. Si todo sale en orden, debería de aparecer el siguiente mensaje, que indica el funcionamiento correcto del programa:

```
Servidor Principal iniciado en el puerto 9000
```

Habiendo hecho la anterior salvedad, luego lo que se lleva a cabo es la apertura de la segunda terminal, en donde dependiendo del escenario que se quiera correr, variará el comando. En caso de que se quiera correr el escenario 1, el comando debe ser el siguiente (**reiterando la situación expuesta previamente sobre las máquinas, en caso de que solamente incluyendo el nombre del archivo genere error, agregue por favor "*.java*" al final**):

```
java ClientePrincipal iterative 32
```

Lo anterior ejecutará el escenario 1, cabe destacar que el número al final del comando "iterative", hace alusión al número de consultas que se quieren llevar a cabo, si es sólo 1, entonces el comando debe ser "`iterative 1`", si se quieren 13 consultas, debe ser "`iterative 13`", si se quieren 32, debe ser "`iterative 32`", y así…

Se podrán visualizar los resultados de los tiempos solicitados en el enunciado en la otra terminal (en donde se inicializó ServidorPrincipal).

Ahora bien, para la ejecución del escenario 2, se debe ejecutar el siguiente comando:

```
java ClientePrincipal concurrent 4
```

Cabe destacar que, para poder variar el número de delegados y clientes, se debe modificar el número luego de "`concurrent`". Para este caso tener presente el espacio entre concurrent y el número, es decir, si se quieren 16 delegados y clientes, utilizar "`concurrent 16`", si se quieren 32, usar "`concurrent 32`", y así…

Los resultados como se mencionó anteriormente se visualizan en la terminal donde se ejecutó ServidorPrincipal.

3. Recopilación de Datos Solicitados en los dos Escenarios

Las siguientes son las tablas de los dos escenarios del caso, anexas a cada una se encuentran datos estadísticos que brindan un poco de claridad sobre cada uno de los tiempos e información recopilada. Igualmente, para mayor claridad, se emplearán algunos detalles y consideraciones sobre los mismos más adelante en el análisis, ya que brindan apoyo y comprensión frente a los datos recolectados.

- ESCENARIO 1:

ESCENARIO 1					
Consulta	*Tiempo Firma (ms)*	*Tiempo cifrar (ms)*	*Tiempo Verificacion (ms)*	*Tiempo simetrico (ms)*	*Tiempo asimetrico (ms)*
1	4590459	1108625	98250	63583	369167
2	462334	90292	93625	67583	107375
3	340875	90500	85417	61917	86459
4	387417	93458	67417	45792	63042
5	242167	81041	86875	55583	58834
6	256667	86708	72917	46541	77625
7	234500	70250	82000	45792	62042
8	220958	60792	29250	42917	49000
9	214292	84709	26000	45291	51208
10	207458	70291	25334	40584	46583
11	210875	70791	31083	42041	79000
12	205250	61708	23375	43917	44458
13	222917	62958	42000	38625	62375
14	202500	63959	21459	37125	46333
15	228375	72834	29750	50375	41833
16	208542	66709	29250	51166	52792
17	231875	122625	27459	38625	48916
18	213000	58209	21542	37459	40500
19	212708	84125	28208	46833	48250
20	217333	63125	22542	38875	46708
21	199333	62917	25166	52417	65417
22	231958	80875	23667	38416	44708
23	223125	81167	23333	36375	42875
24	198834	63709	14750	34834	47583
25	202542	64667	21750	37000	44542
26	216834	66834	20292	36500	51417
27	211792	69792	21500	33542	45583
28	231167	54083	36083	38292	55667
29	209041	55875	24750	40958	42667
30	199542	55875	14500	30167	36167
31	190417	39125	13958	29250	33750
32	210084	46708	21459	312958	37417
Media	369849,0938	103291,75	37655,03125	51916,65625	63446,65625
Desviacion	772304,3841	184146,5535	25859,84648	48507,59568	57966,75897
Mediana	215563	68313	25667	41499,5	48583
Varianza	5,96454E+11	33909953160	668731660,1	2352986839	3360145146

- ESCENARIO 2:

ESCENARIO 2 - 4 DELEGADOS Y CLIENTES						
Delegados	*Cliente*	*Tiempo Firma (ms)*	*Tiempo cifrar (ms)*	*Tiempo Verificacion (ms)*	*Tiempo simetrico (ms)*	*Tiempo asimetrico (ms)*
4	1	4985708	3267584	466542	107333	128041
4	2	1788666	2102542	509875	132583	686250
4	3	806000	175417	84000	55125	71542
4	4	260541	93625	79167	51666	69875
Media		1960228,75	1409792	284896	86676,75	238927
Desviacion		2113775,526	1547823,299	235438,9121	39813,43993	299438,301
Mediana		1297333	1138979,5	275271	81229	99791,5
Varianza		4,46805E+12	2,39576E+12	55431481338	1585109999	89663296085

ESCENARIO 2 - 16 DELEGADOS Y CLIENTES						
Delegados	*Cliente*	*Tiempo Firma (ms)*	*Tiempo cifrar (ms)*	*Tiempo Verificacion (ms)*	*Tiempo simetrico (ms)*	*Tiempo asimetrico (ms)*
16	1	20090292	2129208	180283	63583	389750
16	2	20099000	2179209	177041	137291	202209
16	3	1300500	209333	155833	108334	160208
16	4	939334	230208	136292	177292	151417
16	5	504167	162250	143417	110417	133792
16	6	963834	156791	83375	50250	71500
16	7	487250	139625	76625	47625	57708
16	8	935833	139792	59958	120750	123917
16	9	678875	154208	73917	134875	146583
16	10	489250	158083	88125	131791	160417
16	11	221709	69792	37000	44916	52917
16	12	461750	155708	55458	127333	136583
16	13	215667	68792	35292	43208	66959
16	14	216084	60833	19125	41709	50000
16	15	227375	76875	19417	50875	50083
16	16	204625	77125	23292	49542	46125
Media		3002221,563	385489,5	85278,125	89986,9375	125010,5
Desviacion		6680297,746	692328,5743	56295,94804	45095,55984	86924,51965
Mediana		496708,5	154958	75271	85958,5	128854,5
Varianza		4,46264E+13	4,49361E+11	2971156656	1906508922	7083630109

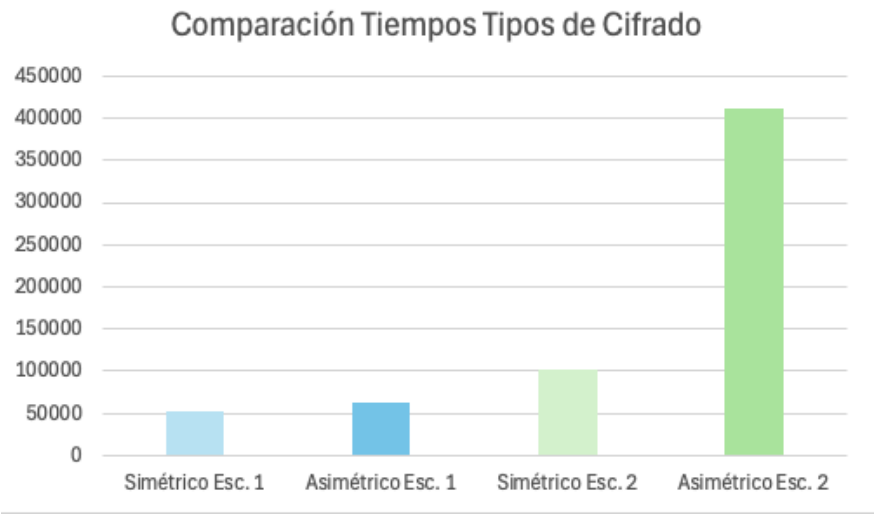
ESCENARIO 2 - 32 DELEGADOS Y CLIENTES						
Delegados	*Cliente*	*Tiempo Firma (ms)*	*Tiempo cifrar (ms)*	*Tiempo Verificacion (ms)*	*Tiempo simetrico (ms)*	*Tiempo asimetrico (ms)*
32	1	66950709	2601959	213333	60875	180458
32	2	67154792	2425208	201041	56542	725125
32	3	644000	77834	80250	52333	91167
32	4	927416	149583	169625	125375	148792
32	5	1286167	142208	69292	47333	65000
32	6	511750	63250	75000	49292	62250
32	7	442000	60167	80125	46417	62791
32	8	443583	150291	68292	138625	148209
32	9	692708	148416	54625	112542	136500
32	10	474000	71250	57250	105375	709375
32	11	437625	139250	53625	97459	134334
32	12	443417	208375	50209	118500	137875
32	13	692708	151125	67917	161291	135916
32	14	474000	160875	50834	92417	108792
32	15	437625	149417	28667	47584	63541
32	16	443417	720042	61125	129500	190125
32	17	692708	139958	45667	105625	119959
32	18	474000	158375	46125	92000	136833
32	19	437625	162792	55625	117709	178167
32	20	443417	109334	48083	110375	106166
32	21	692708	114250	43125	91916	104167
32	22	474000	174709	28750	46416	62666
32	23	437625	126750	42083	88542	106208
32	24	443417	126875	42167	86542	106125
32	25	692708	134333	41667	105792	106250
32	26	474000	145791	58333	86584	97500
32	27	437625	112167	45583	111000	124250
32	28	443417	71000	20667	38959	44958
32	29	412375	56292	69250	119458	107458
32	30	217000	55958	33125	38667	46916
32	31	208916	72584	19167	45000	44917
32	32	207667	74041	20458	290250	47333
Media		4676410,156	289201,8438	63783,90625	94259,21875	145003,8438
Desviacion		16364509,01	594776,7487	46159,92649	48904,92645	155449,2361
Mediana		458791,5	139604	52229,5	92208,5	106854
Varianza		2,67797E+14	3,53759E+11	2130738813	2391691831	24164465002

ESCENARIO 2 - 64 DELEGADOS Y CLIENTES						
Delegados	*Cliente*	*Tiempo Firma (ms)*	*Tiempo cifrar (ms)*	*Tiempo Verificacion (ms)*	*Tiempo simetrico (ms)*	*Tiempo asimetrico (ms)*
64	1	86291458	2774958	186084	67167	573542
64	2	2732167	174083	183708	1070833	146208
64	3	2479875	167167	150375	104334	211625
64	4	2907542	170625	191834	103333	234666
64	5	2387458	190708	157333	119625	271334
64	6	2464750	157250	148333	94458	207583
64	7	1019208	73625	162666	89917	219750
64	8	2176083	161417	57458	124167	190125
64	9	2041958	141625	75000	135459	303625
64	10	2071917	174416	48459	97875	202750
64	11	977667	64667	62875	122375	193000
64	12	979250	59833	46833	98416	178125
64	13	2037541	166666	60042	143375	204042
64	14	976209	68792	64000	105458	193333
64	15	3863042	74584	38584	87625	169875
64	16	1903167	127833	61625	57250	18371417
64	17	1932208	129666	58834	121750	176833
64	18	1914500	136166	43458	91375	164333
64	19	1924750	152041	100833	105208	225959
64	20	955792	59917	59334	96625	180292
64	21	1905708	146917	65708	91750	170916
64	22	470125	180875	27334	44917	78709
64	23	414958	166875	56625	44208	43250
64	24	1977041	191625	47667	89958	115958
64	25	425708	116917	289458	98042	128709
64	26	219667	70833	60208	130542	117167
64	27	205333	57583	17709	35167	63708
64	28	547000	2247208	46666	73791	95333
64	29	413083	115375	20042	37375	47958
64	30	425333	98083	36250	79083	94709
64	31	476416	118333	29375	37958	51458
64	32	209875	37125	55417	809292	113125
64	33	467750	115916	111500	69584	92750

64	34	518958	90458	41667	72583	156458
64	35	449000	110583	41792	69167	104459
64	36	824125	131125	41958	90666	118125
64	37	462875	226250	90667	146000	119084
64	38	247625	55750	65959	75375	99583
64	39	491791	240666	35625	90250	116791
64	40	527792	120125	35875	65958	95708
64	41	437166	86709	37792	65167	77250
64	42	429541	146458	223666	78042	386667
64	43	438750	114208	446667	148791	146000
64	44	461084	166750	34417	85125	98833
64	45	483625	108958	46917	93458	98542
64	46	440959	111917	36916	65167	99875
64	47	435541	111000	38417	68125	101000
64	48	218750	53625	44083	73917	104750
64	49	305250	44459	27167	36166	40167
64	50	213084	46417	16458	33709	41292
64	51	198291	44042	12250	40333	39417
64	52	195791	57862	30534	41875	37625
64	53	193418	82347	28415	41292	36917
64	54	192568	49321	22518	40817	36000
64	55	191250	14688	51379	40333	35291
64	56	191198	38217	15603	39750	34625
64	57	188750	87219	41502	39208	34125
64	58	187422	12453	60244	38667	33292
64	59	186237	94510	31345	37958	32625
64	60	185982	27654	19870	37334	31917
64	61	183761	15523	43718	36792	31292
64	62	182544	76342	27410	36250	30667
64	63	181368	119872	58531	35667	30125
64	64	180789	45839	14902	34625	29625
Media		2222184,75	181578,9219	71654,54688	102763,4219	411098,3438
Desviacion		10712115,46	427644,7031	73377,94115	156809,4813	2282677,186
Mediana		461979,5	111458,5	46875	74646	104604,5
Varianza		1,14749E+14	1,8288E+11	5384322247	24589213428	5,21062E+12

4. Cifrado Simétrico vs Asimétrico

COMPARACION CIFRADO SIMÉTRICO Y ASIMÉTRICO (ms)				
Metrica	*Simétrico Esc. 1*	*Asimétrico Esc. 1*	*Simétrico Esc. 2*	*Asimétrico Esc. 2*
Media	51916,65625	63446,65625	102763,4219	411098,3438
Mediana	41499,5	48583	83510,5	110026,125
Desviacion Estd.	48507,59568	57966,75897	72655,85188	706122,3107
Varianza	2352986839	3360145146	7618131045	1,33288E+12



A simple vista, es posible revisar que los tiempos del Cifrado Simétrico son **claramente menores** en comparación con el Cifrado Asimétrico, véase en ambos casos. Ahora bien, hay una particularidad dentro de los tiempos del escenario 2, ya que para el cifrado simétrico son casi el doble que en el escenario 1, y lo mismo sucede con el cifrado asimétrico, en donde el tiempo aumenta casi 6.5 veces, esto se da debido al cambio de un proceso iterativo a un concurrente. Lo cual es bastante particular como fue mencionado, por el hecho de que la concurrencia se lleva a cabo en pro de la ejecución de múltiples procesos.

Ahora bien, en referencia a la Mediana extraída de ambos casos, es evidente que esta aumenta en el segundo escenario, siendo muy superior a los demás valores, sobre todo para el cifrado asimétrico. Lo anterior puede llevarnos a realizar una conclusión algo precipitada pero correcta de acuerdo con la estadística, y es que el cifrado asimétrico no solamente tiene más promedio en tiempo, sino que constantemente tiene operaciones mucho más lentas.

Por otro lado, en lo que respecta la desviación estándar, se muestra que para el escenario 1 hay desviaciones moderadas: (48,507 ms en cifrado simétrico y 57,966 ms en cifrado asimétrico). Ahora, en el escenario 2, el simétrico aumenta su variabilidad, lo que indica que sus valores son menos consistentes (72,655 ms), y para el asimétrico el aumento es realmente grande (706,122 ms). En conclusión, se puede decir que la desviación en el cifrado asimétrico es muy inestable en el escenario 2, mostrando que algunas operaciones pueden ser o muy rápidas o lentas, y, por el contrario, en general los tiempos de cifrado simétrico muestran que siempre se es mucho más predecible y estable.

Finalmente, la varianza se incluyó por formalidad, pero termina mostrando los mismos resultados o conclusiones (partiendo del hecho de que es el cuadrado de la desviación).

5. Gráficas de tiempos y Análisis


Comparación Tiempos Firmar (ms)
3500000
3000000
2500000
2000000
1500000
1000000
500000
0
Firmar
Escenario 1
Escenario 2


Comparación Tiempos Cifrar (ms)
600000
500000
400000
300000
200000
100000
0
Cifrar
Escenario 1
Escenario 2

Sobre las gráficas anteriores, es posible revisar que evidentemente, en cualquier caso, o resultado de tiempo determinado, el escenario 1, o el proceso iterativo de cifrado, siempre será más rápido en tiempo que el 2, que usa concurrencia.

Adicionalmente, es posible abstraer ciertos datos, y es que el proceso de cifrado en general tomo bastante tiempo en comparación con Firmar y la Verificación, esto puede deberse a que el proceso de cifrado se lleva a cabo en su totalidad con un mensaje o contenido plano, siendo muy lenta la iteración o recorrido byte por byte. Por el contrario, Firmar y Verificar trabajan sobre un resumen, o específicamente como se vio en el curso, con un HASH.

Cabe destacar finalmente la razón por la cual el cifrado asimétrico en general tomó bastante más tiempo en comparación con el simétrico, y es que el primero involucra exponenciaciones modulares, que son pesadas o largas matemáticamente hablando. Esto se evidencia en la actualidad, en donde generalmente se emplea el cifrado simétrico sobre el asimétrico, por su velocidad precisamente. Asimismo, el hecho de trabajar concurrentemente sobre tantos delegados y clientes puede hacer el desarrollo de los procesos mucho más lentos, como bien se mostró en el caso.

6. Escenario Solicitado

Se realizó una serie de experimentos en los que se midieron los tiempos de operación de cifrado simétrico y asimétrico en dos escenarios diferentes, procesando múltiples consultas en un servidor y midiendo los tiempos promedios de cada operación. Con base en los tiempos medios registrados, se estimó que el procesador puede realizar aproximadamente 19 operaciones de cifrado simétrico por segundo y 15 de cifrado asimétrico en el escenario más favorable, mientras que en condiciones de carga (escenario 2), estas cifras bajan a 9 y 2 operaciones por segundo respectivamente. Esto se evidenciará a continuación:

Se debe tener en cuenta inicialmente que 1ms = 1000 microsegundos

Entonces…
Operaciones por segundo = 1segundo / tiempo promedio de una operación (en segundos)

- Para cifrado simétrico (Esc. 1)

  - Tiempo promedio de operación = 51,9166 ms, por lo que…
  - |*Operaciones por segundo = 1000/51,966 =* ***19,26 operaciones por segundo***

- Para cifrado simétrico (Esc. 2)

  - Tiempo promedio de operación = 102,7634 ms, por lo que…
  - *Operaciones por segundo = 1000/102,7634 =* ***9,73 operaciones por segundo***

- Para cifrado asimétrico (Esc. 1)

  - Tiempo promedio de operación = 63,4467 ms, por lo que…
  - *Operaciones por segundo = 1000/63,4467 =* ***15,76 operaciones por segundo***

- Para cifrado asimétrico (Esc. 2)

  - Tiempo promedio de operación = 411,0983 ms, por lo que…
  - *Operaciones por segundo = 1000/411,0983 =* ***2,43 operaciones por segundo***

ANÁLISIS: como ya se ha evidenciado antes, el cifrado simétrico es mucho más rápido que el asimétrico, así como el escenario 2 es mucho más lento que el escenario 1, en cualquier cifrado. Adicionalmente, la capacidad del procesador permite realizar aproximadamente 19 operaciones de cifrado simétrico por segundo en el mejor caso, y unas 2-3 operaciones de cifrado asimétrico por segundo en el peor caso.