Santiago Vela – 202026767

Verónica Escobar – 201922197

Caso 3: Canales Seguros

2022-1

Contenido

1. Introducción

El objetivo de este caso es entender, profundizar y poner a prueba la seguridad informática en el ámbito real, como lo es en una empresa transportadora de paquetes, en donde se tiene que mantener una confidencialidad e integridad todo el tiempo, y en donde tanto el cliente como la empresa (servidor) esperan poder tener una comunicación segura y sin intermediarios. Para esto utilizaremos los diferentes tipos de algoritmos de encriptación de datos, como los algoritmos simétricos y asimétricos, y analizaremos en su comportamiento en relación a la demanda del negocio y decidiremos que algoritmo es mejor usar según cada caso posible del negocio.

2. Descripción de la organización de los archivos

Para este caso esta divido en dos partes, el primero es un servidor y cliente concurrente y en el segundo es un cliente y un servidor iterativo.

Para el caso del servidor y cliente concurrente debido a que es concurrente se pueden crear uno o más flujos de comunicación entre un cliente y un servidor es por eso que inicialmente tenemos 5 paquetes en donde en cada uno de ellos están las clases que nos ayudaran a que sea posible esta concurrencia.

Primeramente , tenemos la carpeta cliente en donde tendremos todos los archivos que son necesarios para la comunicación entre el cliente y un servidor. La primera clase es “Client” el cual nos ayudara a la creación y unos de los diferentes clientes con sus canales de comunicación con el servidor(sockets), esta clase crea la cantidad de clientes según el usuario le indique, para cada cliente se le genera su llave publica individual la cual posteriormente será utilizada por el servidor. De igual forma, con la clase “Client Thread” tenemos los métodos necesarios para comunicación efectiva entre el cliente y el servidor ,debido a que esta clase se va a ejecutar una o muchas veces concurrentemente según del flujo esperara o se comunicara con el servidor con tal de tener confidencialidad. Final mente tenemos la clase “Cliente main” en la cual hace llamado a la clase cliente en donde esta se implementa de manera mas organizada.

De la misma forma, para el caso servidor cliente concurrente, tenemos la carpeta récords en la cual nos ayudara a llevar el estado de los paquetes, para este caso tenemos 32 paquetes y 32 usuarios esta clase le permitirá al servidor consultar el estado actual de los paquetes en el momento en el que el cliente desea saber el estado. Esta. Carpeta se compone principalmente de dos clases , y un archivo csv, la primera clase llamada “record” nos ayuda a saber el log de un paquete, este log contiene: el usuario, el ID del paquete y el estatus del paquete. Por otro lado la otra clase que tenemos es “RecordList” la cual nos ayuda a leer el archivo csv y a crear una lista de los log o estados de los paquetes en tiempo real y poder almacenarlos.

Igualmente , para el caso servidor cliente concurrente tenemos la carpeta Security Utils, que le va hacer de gran ayuda tanto al cliente como al servidor en el momento de mantener confidencialidad entre ellos, por un lado tenemos la clase llamada “Key Generators ” la cual nos ayudara a crear llaves privadas y llaves asimétricas. Lo mismo pasa con la clase “Hashing and autocode” el cual le permitirán interactuar al cliente con el servidor en instantes finales como cuando se calcula el digest.

Para finalizar esta segunda parte nos encontramos con dos carpetas más, una que es Server la cual contiene tres clases que al igual que cliente ayuda en asegurar una buena conexión entre el servidor y el cliente, y la otra carpeta que encontramos se llama “Status Request” la cual es usada inicialmente por el cliente una vez los pasos de autenticación ya fueron cumplidos, esta carpeta tiene una clase la cual le permitirá al cliente enviar un request al servidor de su paquete especificando el Id del cliente y el Id del paquete.

Para el caso del servidor y cliente iterativo, se manejan las mismas carpetas sin embargo al ser iterativo no se crearan flujos de o thread si no que una vez acabe un proceso o una ejecución se puede ejecutar la otra, es por eso que tanto para el server que como para el client no vamos a tener clases que extiendan de un thread, con esto dicho la ejecución en la segunda parte será más corta, en términos de tener mas sockets o conexiones entre clientes y servidores.

3. Descripción para correr el prototipo

Las instrucciones para correr el prototipo son muy simples debido a que primeramente siempre tenemos que correr la clase main del server y posteriormente tendremos que correr la clase main del cliente, esto sirve tanto para iterativo como para concurrente.

4. Descripción esquema generación de llaves

Para haber podido implementar la seguridad y confidencialidad entre el cliente y el servidor, utilizamos el paquete de java “ java.security”, el cual consiste básicamente en clases abstractas e interfaces que encapsulan conceptos de seguridad como certificados, claves, resúmenes de mensajes y firmas digitales.

Los proveedores pueden implementar tres clases:

- **KeyPairGenerator**. Se emplea para crear claves públicas y privadas.

- **MessageDigest**. Prorciona la funcionalidad de algoritmos de resumen de mensajes como el MD5 y el SHA.
- **Signature**. Se emplea para el firmado digital de mensajes.

En nuestro caso utilizamos este paquete para crear tanto llaves publicas como privadas tanto del cliente como del servidor. Por otro lado usamos el paquete “javax.crypto”, el cual nos ayudo a mantener confidencialidad en las partes ya que gracias a este paquete pudimos realizar operaciones de encriptación, este paquete lo pudimos usara tanto para cifrado simétrico, como para cifrado asimétrico; para este caso usamos “KeyGenerator” Debido a que proporciona las funciones de un generador de claves simétricas.

5. Datos recopilados

Concurrente Asimetrico 16 delegados

Run	1	2	3	4	5	6	7	8	9	10
Tiempo Delegado 1	37019700	37601400	34025200	40030900	34146100	39207000	45637700	67281300	36953700	47494100
Tiempo Delegado 2	1056300	1078700	675700	996800	1389500	1010400	1422500	1194500	722000	919600
Tiempo Delegado 3	825800	761900	795600	849600	928000	1386000	1156200	767800	561400	905100
Tiempo Delegado 4	865400	844800	638800	891900	620700	1062900	777100	938500	619700	869100
Tiempo Delegado 5	862100	546300	742900	744000	1151000	1278400	1066700	782500	824000	1774000
Tiempo Delegado 6	633500	781000	796900	686900	559000	945700	748900	826100	721500	910500
Tiempo Delegado 7	786500	814300	693600	860200	752500	534800	542900	773700	765600	769300
Tiempo Delegado 8	788100	819500	742000	545700	748900	518500	521000	761700	784200	1057600
Tiempo Delegado 9	767000	798800	780300	776000	927800	537900	804400	499400	742100	735500
Tiempo Delegado 10	694200	622200	730000	787100	695400	488600	727800	773100	794900	785500
Tiempo Delegado 11	819200	808300	613600	1190700	901500	786500	820900	774800	746700	619900
Tiempo Delegado 12	460900	816700	675600	746300	733300	548600	654900	717900	518300	512400
Tiempo Delegado 13	746400	811800	746900	707300	848500	939700	769700	737500	641500	767100
Tiempo Delegado 14	870000	819600	655000	756100	790000	740200	778300	744400	642500	668300
Tiempo Delegado 15	731800	726000	736000	713700	822400	510600	751600	713800	487700	716100
Tiempo Delegado 16	679700	721700	900500	507100	783900	688600	516900	502400	479800	765600
Promedio	3037912.5	3085812.5	2809287.5	3236893.75	2924906.25	3199025	3606093.75	4924337.5	2937850	3766856.25
Desviacion estandard	9062713.728	9204834.076	8324546.412	9813059.95	8328049.754	9606307.885	11210934.95	16629253.62	9071577.728	11663926.38

Concurrente Asimetrico 32 delegados

Run	1	2	3	4	5	6	7	8	9	10
Tiempo	40377400	35743900	45923700	39769800	37704600	37664600	43877200	45816700	36446300	44346200

Delegado 1										
Tiempo Delegado 2	1250200	926100	1135400	1450200	1883000	706000	910500	1145900	1189800	955600
Tiempo Delegado 3	908700	1809300	1146600	936700	2581300	1012100	865000	2103200	948800	917000
Tiempo Delegado 4	850000	554200	971500	712600	673600	824200	790500	993500	1016300	598600
Tiempo Delegado 5	514300	897400	982200	901000	968400	716800	852200	767400	1035800	584800
Tiempo Delegado 6	773200	687500	1149800	637000	823900	797200	839900	547500	1788400	760100
Tiempo Delegado 7	815500	814000	786700	820100	722700	531900	556800	792900	908200	813400
Tiempo Delegado 8	504200	742400	566400	762800	776400	786100	819000	767700	704800	741200
Tiempo Delegado 9	649400	929100	731500	810300	913000	806600	743100	754600	771500	845700
Tiempo Delegado 10	777300	712300	676600	813000	761700	759700	1271000	739100	714000	755900
Tiempo Delegado 11	759400	775900	688200	727500	874800	767100	793400	741300	775700	865800
Tiempo Delegado 12	763900	729000	501200	714000	761700	682300	751900	675900	624800	776800
Tiempo Delegado 13	528500	1061000	640600	719900	731900	636600	947600	738600	692300	875300
Tiempo Delegado 14	689700	1186800	650100	716400	757400	707900	729500	725600	599000	741400
Tiempo Delegado 15	774900	678000	634700	704500	734000	845800	2000100	739200	660500	816200
Tiempo Delegado 16	1005600	968400	680900	732400	781500	693100	3595300	488500	638200	681400
Tiempo Delegado 17	728000	760400	652700	616400	806200	722300	777000	698500	632000	678900
Tiempo Delegado 18	724500	660400	649500	959600	665500	707500	736600	596600	433700	701300
Tiempo Delegado 19	715200	706500	716000	820700	887600	858400	821200	940100	752600	734600

Tiempo Delegado 20	718900	728400	702100	804400	872300	743100	1095800	684600	726300	668700
Tiempo Delegado 21	721900	669600	691900	472400	907000	814700	817900	690900	633200	644300
Tiempo Delegado 22	1409700	2301800	1515600	1367300	1823900	1259700	2185600	1405000	1392100	1522100
Tiempo Delegado 23	508100	777700	607600	753300	664800	697000	703500	663700	721200	661100
Tiempo Delegado 24	672700	558100	656000	912400	729400	746200	733500	707700	675200	649100
Tiempo Delegado 25	744400	670700	761000	659000	506400	716500	746700	693000	672500	550800
Tiempo Delegado 26	3105000	1750900	665300	732700	748800	823100	664900	1114500	584100	659800
Tiempo Delegado 27	761400	789100	753200	758200	704100	515300	721200	742700	677700	490400
Tiempo Delegado 28	760200	682000	586800	545800	669400	664100	763200	706600	597200	572400
Tiempo Delegado 29	658300	591400	698400	556900	732000	626400	670400	763900	602600	578900
Tiempo Delegado 30	707400	626700	719400	677400	814300	838100	658900	597400	391200	613800
Tiempo Delegado 31	680800	585200	666000	627000	637400	598600	630800	1168500	615800	635900
Tiempo Delegado 32	712300	577800	584800	804400	659800	641300	634100	626400	577400	645200
Promedio	2070968.75	1957875	2171637.5	1999878.125	2039962.5	1903446.875	2303259.375	2229303.125	1881225	2096334.375
Desviacion estandard	7004824.754	6177630.193	7986719.165	6895067.859	6521575.1	6527077.751	7609561.801	7959588.482	6313424.716	7711859.19

Concurrente Asimetrico 4 delegados

Run	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Tiempo Delegado 1	40114600	43612700	39423600	33913300	38087300	31874100	39366600	49822000	42734800	37872700
Tiempo Delegado 2	1589500	992400	1041000	1295600	1754900	1287300	925600	1023000	1141000	1143800
Tiempo Delegado 3	1221300	913400	781800	1022800	1323700	986900	899400	2069300	957700	756700
Tiempo Delegado 4	905300	736000	762400	954700	1127500	787400	705100	843000	945100	803700
Media	10957675	11563625	10502200	9296600	10573350	8733925	10474175	13439325	11444650	10144225
Desviacion Estandard	19439960.73	21366318.99	19281351.64	16411794.36	18344505.19	15428151.53	19261867.77	24261142.04	20860292.11	18486454.58

Promedio

Run	1	2	3	4	5	6	7	8	9	10
Media 4 Delegados	10957675	11563625	10502200	9296600	10573350	8733925	10474175	13439325	11444650	10144225
Media 16 Delegados	3037912.5	3085812.5	2809287.5	3236893.75	2924906.25	3199025	3606093.75	4924337.5	2937850	3766856.25
Media 32 Delegados	2070968.75	1957875	2171637.5	1999878.125	2039962.5	1903446.875	2303259.375	2229303.125	1881225	2096334.375

Media 4 Delegados general	10712975	nanosegundos	
Media 16 Delegados Geneal	3352897.5	nanosegundos	
Media 32 Delegados General	2065389.063	nanosegundos	
Media total	3126744.423	nanosegundos	

Simétrico Concurrente 4 delegados

Run	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Tiempo Delegado 1	11158400	12643300	11600400	12545000	8497800	12797900	9810100	9618900	12560300	11721800
Tiempo Delegado 2	333300	263200	265400	261500	252400	271300	297300	275300	268200	308200
Tiempo Delegado 3	306400	296100	285900	288700	254600	256900	270100	201500	256900	1505400
Tiempo Delegado 4	321800	255400	249100	234700	219600	250200	305400	237000	266100	281100
Media	3029975	3364500	3100200	3332475	2306100	3394075	2670725	2583175	3337875	3454125
Desviacion Estandard	5418961	6185892	5666820	6141723	4127831	6269223	4759607	4690580	6148285	5541267

Simétrico Concurrente 16 delegados

Run	1	2	3	4	5	6	7	8	9	10
Tiempo Delegado 1	10960000	10115100	12027000	10783200	11076200	15523500	10209500	10982900	12201200	12275300
Tiempo Delegado 2	372100	271400	452000	274400	287400	285200	325100	291500	314200	286500
Tiempo Delegado 3	235700	266500	239700	256200	282100	259300	247200	252700	286000	267400
Tiempo Delegado 4	249100	249100	227000	285000	175400	237400	299900	213900	257600	252800
Tiempo Delegado 5	263400	234000	231600	238200	382100	235300	227900	182600	239600	218200
Tiempo Delegado 6	239400	214200	173300	241600	238500	274700	325200	234800	229800	239400
Tiempo Delegado 7	199600	208300	214500	233200	214000	224100	253500	218500	209800	183000
Tiempo Delegado 8	230300	222800	213700	206500	234400	234900	219600	214800	200100	195100
Tiempo Delegado 9	254600	233300	218300	220700	189700	215800	222900	231200	218100	209600
Tiempo Delegado 10	210600	213600	222500	203600	217400	212200	197700	225500	149600	246400
Tiempo Delegado 11	185400	215500	186800	265000	189800	201200	217400	203800	244400	200000
Tiempo Delegado 12	214800	251400	251100	215000	226700	211900	211100	218800	204700	176500
Tiempo Delegado 13	169500	239500	119600	161300	193300	226300	214900	220300	222200	197800
Tiempo Delegado 14	195000	332400	224900	215600	231600	215200	237100	167700	202200	217300

Tiempo Delegado 15	219100	234900	155200	197700	251000	205900	218200	194700	214900	204300
Tiempo Delegado 16	170500	217100	184600	143300	206100	186300	202200	156200	134200	175100
Media	898068.75	857443.75	958862.5	883781.25	912231.25	1184325	864337.5	888118.75	970537.5	971543.75
Desviacion Estandard	2683608.395	2468901.852	2952341.96	2640117.665	2710858.002	3823870.7	2492375.428	2692132.056	2995166.896	3014510.943

Simétrico Concurrente 32 delegados

Run	1	2	3	4	5	6	7	8	9	10
Tiempo Delegado 1	12609600	13063500	10637900	13142500	10050700	11754500	11368100	17281800	12405200	12548700
Tiempo Delegado 2	278800	292000	269000	280000	274600	290600	288400	276500	267500	302100
Tiempo Delegado 3	186900	215400	253900	284900	316100	266300	260100	248300	270900	216200
Tiempo Delegado 4	838300	218900	250900	244400	244100	400600	278700	273000	686600	234600
Tiempo Delegado 5	212000	227500	181400	233700	220300	233800	223100	235200	223300	234800
Tiempo Delegado 6	217400	250800	236500	263500	296300	281800	244400	251700	269400	182500
Tiempo Delegado 7	221000	219700	226700	246100	203000	201500	223100	177500	211000	210500
Tiempo Delegado 8	221200	196500	216300	261100	198300	224100	220700	274600	158800	256600
Tiempo Delegado 9	409900	216000	216200	157000	189100	150300	213100	207600	236900	144800
Tiempo Delegado 10	221800	211300	211400	215800	213800	162200	221500	240800	182000	261500
Tiempo Delegado 11	223000	223200	208400	221800	200400	193800	200100	218300	200800	204300
Tiempo Delegado 12	182900	199500	216900	243600	195500	140400	189000	241300	202900	183100
Tiempo Delegado 13	203500	146200	201700	330900	189500	148400	217200	245600	196500	215200
Tiempo Delegado 14	191800	260000	230300	218900	250800	251300	158600	195700	200200	232000
Tiempo Delegado 15	195700	206000	219400	163200	231800	204600	201100	239000	160900	191600
Tiempo Delegado 16	200900	190200	197900	154200	188700	186300	149200	165400	178300	217900

Tiempo Delegado 17	230700	191400	188300	191200	182200	189800	189500	186300	183300	202900
Tiempo Delegado 18	180500	176800	236400	190400	206600	219300	194900	216500	175900	249300
Tiempo Delegado 19	185800	173900	235200	195300	469400	175000	212200	202500	193800	177600
Tiempo Delegado 20	175300	192500	167300	227100	168300	176000	183000	183800	196400	188000
Tiempo Delegado 21	170700	166500	230900	123000	178300	181500	181500	204200	164100	171000
Tiempo Delegado 22	875900	807700	954000	923100	743000	800400	885000	894100	2834500	692900
Tiempo Delegado 23	173200	151800	130700	168000	129000	163700	155200	178000	156900	154500
Tiempo Delegado 24	180400	182000	203200	188600	213600	198400	159200	228800	181100	203100
Tiempo Delegado 25	162400	171000	1967100	194600	177300	214400	155600	232100	183600	149600
Tiempo Delegado 26	162900	160500	181000	172800	135000	128700	174600	190100	182000	156900
Tiempo Delegado 27	158800	156000	176600	166100	156400	165700	150400	186900	166600	167900
Tiempo Delegado 28	158700	154400	164800	194500	166600	156800	148800	239500	161800	167300
Tiempo Delegado 29	160900	166500	164700	168800	159900	209100	173300	293100	159000	169000
Tiempo Delegado 30	135500	161700	998300	165500	165700	208700	648900	372500	1100100	181100
Tiempo Delegado 31	169100	171000	191300	145600	165900	168600	166700	189300	166500	170400
Tiempo Delegado 32	165700	171800	156900	121400	182100	178300	153700	177700	150400	202900
Media	626912.5	615381.25	635046.875	631175	533196.875	582028.125	580903.125	779615.625	700225	601275
Desviacion Estandard	2193109.323	2274357.097	1860034.005	228709 7.63	1740457.891	2042170.238	1974001.088	3013920.186	2192219.148	2182192.227

Promedio

Run	1	2	3	4	5	6	7	8	9	10
Media 4 Delegados	3029975	3364500	3100200	3332475	2306100	3394075	2670725	2583175	3337875	3454125
Media 16 Delegados	898068.75	857443.75	958862.5	883781.25	912231.25	1184325	864337.5	888118.75	970537.5	971543.75
Media 32 Delegados	626912.5	615381.25	635046.875	631175	533196.875	582028.125	580903.125	779615.625	700225	601275

Media 4 Delegados	3057322.5	nanosegundos
Media 16 Delegados	938925	nanosegundos
Media 32 Delegados	628575.94	nanosegundos
Media Total todos los casos	910894.62	nanosegundos

Asimétrico Iterativo. 32 Requests

Run	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Consulta 1	43452500	41060400	34163100	38556300	34959500	41293900	34375600	47458600	38868200	38771400	34464400	31897800	39908600	33254800
Consulta 2	869200	976000	824000	994500	798000	1098800	850200	686100	978100	823000	932100	866900	947200	676900
Consulta 3	713400	826100	687800	937300	733900	907000	759000	669000	817800	749800	630500	964600	780400	705100
Consulta 4	668200	917600	677100	872500	575300	677800	742100	592100	804200	649800	706900	925500	781200	632100
Consulta 5	767900	765900	827900	4296700	650900	730500	773900	680500	701800	719600	471600	934500	752600	623700
Consulta 6	733600	806700	621700	1868800	677500	651800	767000	494800	997500	661400	788500	701600	717400	494200
Consulta 7	791400	718900	640300	921800	666800	721900	735400	566300	807100	615500	751000	664400	716800	641800
Consulta 8	689800	777800	623800	872200	636000	610200	768400	636300	795600	651500	794900	660600	713000	496500
Consulta 9	792200	913000	638300	928700	689500	500500	644900	547900	863400	592600	723600	622000	740300	695000
Consulta 10	864900	646200	583000	813400	635500	667700	741100	544100	755900	638100	779600	625100	716500	555200
Consulta 11	734700	696700	580300	844700	647100	650700	1085600	553100	804400	648100	701500	616000	642200	548800
Consulta 12	616200	688400	632400	661300	626800	602200	699100	497900	753800	591600	772300	614300	653100	552200
Consulta 13	709400	818900	596300	715600	643000	595300	529100	622900	688300	619400	843900	603500	498800	558100
Consulta 14	673700	685900	554000	582800	511500	630700	500900	528100	639800	596500	725500	598700	541900	633200
Consulta 15	753300	917700	613200	588400	718200	580800	556700	547200	596100	655300	755500	608200	516700	566300
Consulta 16	811100	639500	735400	624700	713200	591300	509000	540200	589300	1101100	722900	580400	385500	527700
Consulta 17	660900	683700	561100	553600	697800	636400	535400	539500	533800	707200	719600	619300	551600	602200
Consulta 18	628900	670600	620300	633300	610400	691300	540000	547200	579300	575700	691900	525000	533900	526000
Consulta 19	667900	676100	623800	610200	625800	741500	538000	549800	619800	572900	727000	593700	532700	572400
Consulta 20	739600	666100	548300	626400	592000	624300	1593200	546100	645100	512100	676500	684500	512300	610000
Consulta 21	648500	689200	662400	600500	830300	632500	588700	612000	561500	524900	746300	585300	579200	480300
Consulta 22	16663300	13854400	10962200	14365500	11542200	11406600	12206600	10164400	12107700	11645500	12969900	12913300	10453300	11909900
Consulta 23	647800	645900	561400	608500	584700	715500	528400	498000	761700	524000	636600	558500	699000	534000

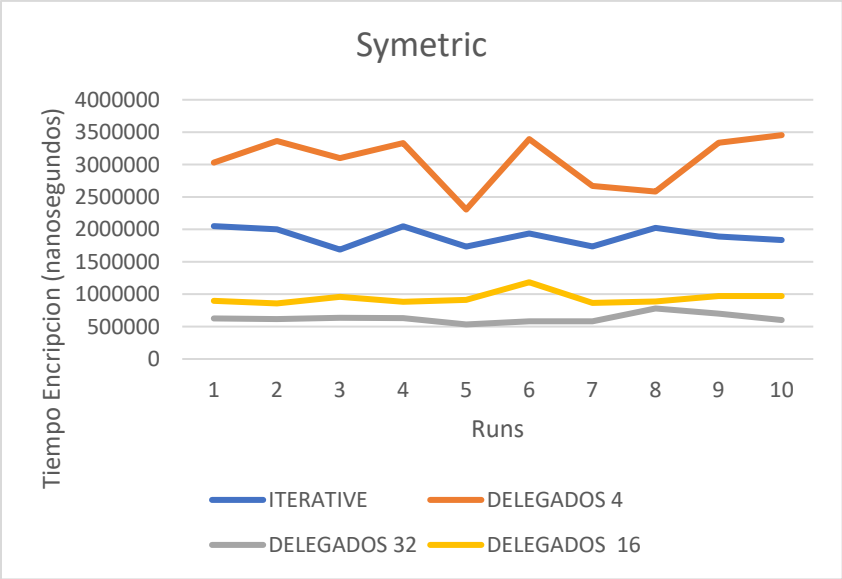
Consulta 24	598100	554200	612500	693000	582700	581500	563400	497700	548300	606900	641300	658000	512400	464100
Consulta 25	615300	596900	741200	609900	549200	554900	586300	451900	604800	482900	601400	598000	555100	491000
Consulta 26	593000	629400	580500	785000	730900	581700	614600	515000	584600	462900	678600	634600	475600	492100
Consulta 27	687500	900300	657000	604500	606900	729400	595700	528100	621700	575700	824200	678200	590400	512400
Consulta 28	588500	636700	533000	555700	631700	588000	527000	509600	505400	601600	652100	554700	501600	503200
Consulta 29	550900	622800	660100	517800	677000	580900	500600	550500	549200	561100	579000	580200	497100	500500
Consulta 30	606800	638300	506200	535300	573400	594500	549200	468600	628100	575900	711900	625400	527600	506300
Consulta 31	523700	589000	552200	562100	559400	514700	512200	457900	537000	640200	664400	589600	503800	513600
Consulta 32	545800	568700	502900	541300	618500	585500	552800	318100	518200	550200	797800	505800	487500	448000
Media	2050344	2000281	1688053	2048541	1734613	1937634	1737003	2024109	1889703	1835106	1787819	1648944	1847416	1597144
Desviacion Estandard	7557534	7129516	5927110	6696964	6063911	7183098	5960477	8291582	6749702	6741743	5964292	5522100	6946864	5778348

Symetrico Iterativo 32 delegados

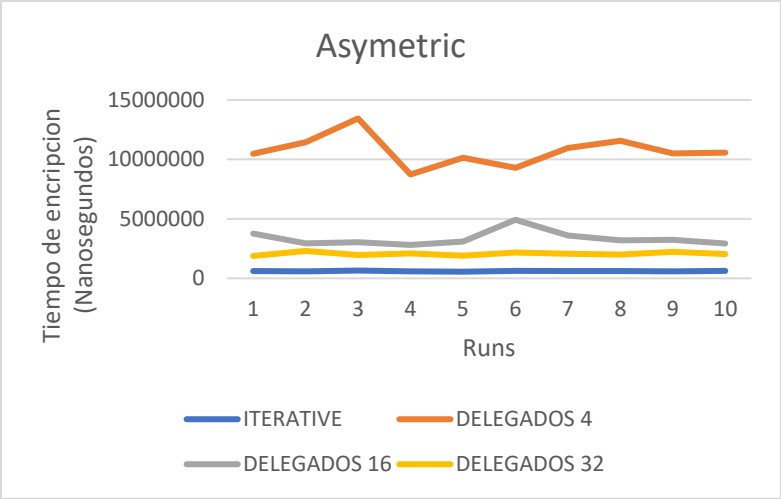
Run	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Consulta 1	13216800	12010800	12964100	11618800	11378700	12997300	12936100	12640000	12038500	12778300	12634500	12447300	13578600	12777600
Consulta 2	274200	261400	361500	554400	269300	293000	281200	275100	266000	264900	272500	274300	276600	326100
Consulta 3	281000	183800	236800	242500	254400	240100	253700	243700	246700	326500	251000	284400	267200	247500
Consulta 4	255800	273500	325500	308700	252400	253500	254800	261700	317600	251500	249500	238100	253300	261400
Consulta 5	244900	217200	319700	246800	187100	242800	216200	180600	249100	254500	241300	240200	230000	149500
Consulta 6	247600	205900	269500	207300	212700	246200	205200	227800	264400	252900	229200	205000	242700	250900
Consulta 7	212400	197300	276900	188000	203900	220600	172100	199800	200900	230700	193200	169500	250700	199900
Consulta 8	223700	226500	242300	239700	215800	271700	186900	198400	217600	221900	226600	219100	226400	214200
Consulta 9	224300	211600	213200	199900	169700	219700	207700	194600	247800	229300	219300	196300	288700	198200
Consulta 10	204800	198000	217100	169400	161200	213500	135100	289300	136600	217000	230300	145700	220600	229800
Consulta 11	197900	198800	209900	197100	196500	213900	210800	205600	220800	208400	306100	205700	204000	202000
Consulta 12	193700	202200	220200	193100	147600	211500	202100	197800	197800	211000	183900	139000	190500	209000
Consulta 13	195100	195500	226400	194700	200600	198100	177000	218700	202700	207300	201400	194200	214200	228900
Consulta 14	183500	304400	229900	211700	262700	269800	240700	257800	243800	255400	209500	208400	177900	255200
Consulta 15	171200	200500	208000	233600	194000	214300	369900	210100	186400	201500	189000	326000	204300	198300
Consulta 16	232900	223300	346200	220100	153000	220600	216100	218500	241300	227100	227400	222500	215300	157500
Consulta 17	164200	205400	220100	173600	181700	171900	220800	178400	212100	391600	197000	178700	193900	187400
Consulta 18	174200	182900	215900	189800	192300	177000	235100	186200	192900	187500	212800	181700	181500	188100
Consulta 19	205200	180300	268100	194400	175000	165900	222700	194900	191600	196200	180600	172700	222600	189100
Consulta 20	165300	184400	168700	173100	191300	167100	177700	163000	197900	216000	184900	342300	184400	299000

Consulta 21	184000	172600	175800	171800	181600	207900	189200	162500	159400	186600	399400	165900	171700	169400
Consulta 22	735000	763700	820500	1021100	815600	856000	730000	1116900	791900	786700	786000	950700	1261800	769300
Consulta 23	165300	154400	166900	155000	161200	164800	163100	176900	184100	159100	163900	171600	171800	174300
Consulta 24	167600	151000	184800	178500	173600	184100	166900	169700	200400	184700	183000	172000	171900	186100
Consulta 25	162900	182200	320800	196000	142600	180200	160200	168700	191300	253900	165400	165400	171700	171500
Consulta 26	157900	159300	176500	158900	165800	166900	161500	174000	161600	162200	164600	157500	164800	346600
Consulta 27	168400	172100	183900	154400	266000	158200	159500	169400	197500	183200	170700	147000	172100	152600
Consulta 28	157200	156300	193600	157300	182300	171100	212100	172600	151400	168500	155700	158800	157800	148700
Consulta 29	206200	175900	390800	163000	142100	159400	162300	156800	154700	207700	172600	154600	170300	176300
Consulta 30	182100	163100	229000	156800	160100	164100	156300	169900	167200	156400	160300	163400	155300	165800
Consulta 31	163800	171500	201200	168800	176400	180200	170800	188800	133900	270200	265000	180000	165900	191900
Consulta 32	134000	163500	167900	193800	147000	172700	173600	164100	173300	180300	155600	197800	162600	162600
Media	620409.4	582790.6	654740.6	588503.1	559818.8	624190.6	616481.3	616634.4	591850	632156.3	618193.8	605493.8	653784.4	618271.9
Desviacion Estandard	2300829	2088068	2249344	2019213	1977640	2261070	2250469	2200269	2091758	2219190	2195649	2165525	2366207	2221580

6. Grafica simétrica



7. Grafica asimétrica.



8. Comentarios Graficas y comportamientos

Para empezar el análisis de comportamiento del servidor con los diferentes tipos de cifrado iniciaremos con **cifrado simétrico**, y para este caso los tiempos de cifrado tanto para servidor iterativo como para los casos de concurrencia son muy diferentes y muchas veces contrario a lo que uno pensaría, ya que en el caso de concurrencia y teniendo 4 delegados el servidor se toma más tiempo en cifrar, cosa que uno pensaría que al ser menor cantidad de solicitudes menor seria el tiempo en cifrar. Por otro lado para el caso de un servidor iterativo este puede tomar más tiempo en relación a las pruebas de 16 y 32 delegados. De igual manera, pudimos evidenciar que para el caso de 16 delegados esta llego a tomar más tiempo que la prueba con 32 delegados sin embargo, uno pensaría que al tener gran cantidad de delgados esta se podría tomas tiempo, pero este no fue el caso. Y finalmente, el escenario que no demoro en promedio menos tiempo es el de 32 delegados este manteniéndose en un rango de 500 mil a 1 millon nano segundos. Con lo cual, podríamos concluir que para el caso de servidores iterativos, el cifrado simétrico puede ser una buena herramienta de encripcion en términos de tiempo. Si bien se sabe el cifrado simétrico esta caracterizado porque puede ser muy eficaz ya que no experimenta ningún retraso de tiempo significativo como resultado del cifrado y también en el descifrado.

Del mismo modo, con el **cifrado asimétrico** al solo verlo podemos ver que los resultados del tiempo que tenemos cambian considerablemente a la de la gráfica anterior, recordemos que una de las ventajas del cifrado asimétrico es que el aumento de la seguridad de los datos. Es este cifrado es más seguro porque los usuarios nunca tienen que revelar o compartir sus claves privadas. Para empezar este análisis lo primero seria empezar con el escenario iterativo ya que los tiempos de cifrado con relación al cifrado simétrico no cambian bastante ya que ahora su tiempo de cifrado se encuentra en el rango de 0 a 2

millones de nanosegundos lo cual no representa mucho debido a que antes se situaba en un rango entre millón quinientos dos millones de nanosegundos, si bien este escenario es el que menos tiempo se demora, es importante decir que para el escenario iterativo su cambio no es marcado como en los escenarios concurrentes. Para el caso de 32 delegados su tiempo de cifrado cambio demasiado en relación a la grafica anterior debido a que su rango antes era entre 500 mil nanosegundos y 700 mil nanosegundos , ahora su rango de cifrado aumento entre millón ochocientos y dos millones, teniendo una tendencia a estar mas en dos millones. Continuando, tenemos el caso de 16 delegados en el cual podemos observar su tiempo de cifrado no vario demasiado a la el cifrado anterior puesto que 5 millones y 3 millones de nanosegundos
, para esta nueva grafica de cifrado tenemos que su rango ahora se encuentra entre 3 millones 500 mil nanosegundos y 5 millones. Y por último para el caso de 4 delegados es donde se ve mayor incremento, ya que su rango anterior era entre 2 millones 500 mil nanosegundos y 3 millones 500mil nanosegundos, en cifrado asimétrico su rango esta entre ocho millones nano segundos y 13 millones de nanosegundos, con lo cual podemos decir que el tanto el cifrado simétrico como el cifrado asimétrico pueden llegar a ser muy buenos dependiendo el caso de negocio y su necesidad.

9. Cálculos

Las especificaciones del computador usado para realizar las pruebas son las siguientes.

Processor: 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz 2.80 GHz
Installed RAM: 16.0 GB (15.7 GB usable)
System type: 64-bit operating system, x64-based processor
Operating system: Windows 11

Para tomar como referencia los tiempos calculados se usaron las siguientes tablas

Asimetrico Concurrente

	Tiempo (nano)	Tiempo(segundos)
Media 4 Delegados general	10712975	0.010712975
Media 16 Delegados Geneal	3352897.5	0.003352898
Media 32 Delegados General	2065389.063	0.002065389
Media total	3126744.423	0.003126744

Simetrico Concurrente

	Tiempo (nano)	Tiempo(segundos)
Media 4 Delegados	3057322.5	0.003057323
Media 16 Delegados	938925	0.000938925
Media 32 Delegados	628575.9375	0.000628576
Media Total todos los casos	910894.6154	0.000910895

Asimetrico Iterativo

	Tiempo (nano)	Tiempo(segundos)
Media general	1844764.955	0.001844765

Simetrico Iterativo

	Tiempo (nano)	Tiempo(segundos)
Media general	613094.1964	0.000613094

El procesador usado tenia la siguiente velocidad:

	GHz	Cycles/Second
Velocidad de reloj	2.80GHz	3006477107

En este caso se tomo referencia de tanto el tiempo teórico que se debería tomar el procesador en encriptar usando los algorimtos simétricos tanto como asimétricos

	Caso Asimetrico Iterativo		
	Average Encryption time	0.001845	Segundos
	Algoritmo usado	RSA 1024 bits	
Teorico	Tiempo por operacion	0.0008	Segundos

Tiempo (Teorico)	1250	retos
Tiempo(Practica)	542	retos

	Caso Asimetrico Concurrente		
	Average Encryption time	0.003126744	Segundos
	Algoritmo usado	RSA 1024 bits	
Teorico	Tiempo por operacion	0.0008	Segundos

Tiempo (Teorico)	1250	retos
Tiempo(Practica)	319	retos

En este caso se consulto una pagian con benchmarks de diferentes algoritmos de encripcion y se encontró que con una implementación en C++ un algoritmo RSA con una llave de 1024 bits tal como el que estamos usando en el proyecto se debe tomar 0.0008 segundos en encriptar los datos dados. El tiempo de encripcion de un algoritmo como RSA es dependiente completamente en el tamaño de la llave dada, 1024 bits en este caso, por lo

tanto el tamaño del reto no afectaría su tiempo de encripcion en teoría. En este caso los tiempos en practica que se demora en encriptar el retoson mucho menores de los teóricos, pero esto se puede atribuir a la forma en la que fue implmentado RSA en Java y las librerías usadas.

	Caso Simetrico Iterativo		
	Average Encryption time	0.000613094	Segundos
	Algoritmo usado	AES/ECB/PKCS5 256 bits	
Teorico	Ciclos/Byte AES	1.3	cycles/bytes

Tiempo (Teorico)	2312674698	retos
Tiempo(Practica)	1631.070732	retos

	Caso Simetrico Concurrente		
	Average Encryption time	0.000910895	Segundos
	Algoritmo usado	AES/ECB/PKCS5 256 bits	
Teorico	Ciclos/Byte AES	1.3	cycles/bytes

Tiempo (Teorico)	2312674698	retos
Tiempo(Practica)	1097.821837	retos

En los casos simétricos se encontró una referencia dada por Intel sobre el tiempo mínimo para encripcion usando AES con ECB con una llave de 256 bits (no encontré referencias de los ciclos por bit para padding de PKCS5) . En este caso no se esperaría que la maquina usada produjera velocidades de encripcion comparables, puesto Intel uso un procesador mucho mas rápido y implmento AES con instrucciones de maquina. En este caso la diferencia entre el tiempo teórico máximo posible y el tiempo en practica que se demora mi maquina es bastante notable.

En términos generales cuando se compara los algoritmos simétricos con los asimétricos en general se puede ver que como es esperado los algorimtos simétricos son mucho mas rápidos en practica, puesto permtien encriptar una cantidad de retos casi doble o triple que un algoritmo asimetrico en la misma maquina. Comparando entre iterativo y concurrente se puede ver que en ambos casos los iterativos fueron considerablemente mas eficientes que los concurrentes.

10. Conclusiones

Podemos concluir que la seguridad informática es muy importante, pero mas importante es saberla utilizar de la manera correcta ya que gracias a esta nos podemos ahorrar tiempo y recursos, si bien esta nos puede ayudar a mantener confidencialidad e integrad esta misma también nos ayudara a mantener una comunicación segura, es verdad que se tiene que saber aplicar de manera correcta, pero al final de cuentas ayuda a mantener a protegerse de

factores externos. Por otro lado también nos dimos cuenta de que existen muchas formas de proteger información y de mantener esa información y según la que uno escoja esta puede tomar mas tiempo y recursos que la otra, pero sin embargo siempre mantendrá la información protegida. Finalmente concluimos que los socekts son buenos caneles de comunicación entre usuarios y servidores debido a que ayuda al manejo y traspaso de información y también a mantener integridad en las comunicaciones.