Amalia Carbonell - 202122079

Nicolás Arango - 202220342

**Caso 3**

**Descripción de la organización de los archivos:**

Dentro de la carpeta del caso 3 podemos encontrar 2 carpetas, una para el laboratorio 8 que nos sirvió de guía, y una llamada src. En la carpeta src se encuentran los archivos tipo java en los cuales se implementó el proyecto. En src podemos ver las clases servidor, cliente, main y seguridad cliente.

**Instrucciones:**

Para probar el proyecto es necesario correr el archivo main.java. En este se pregunta al usuario el número de clientes a crear.

**1. Para responder las siguientes preguntas puede usar fuentes externas, solo recuerde construir las respuestas con sus propias palabras y citar las fuentes usadas:**

* **(i) En el protocolo descrito el cliente conoce la llave pública del servidor (K\_w +). ¿Cuál es el método comúnmente usado para obtener estas llaves públicas para comunicarse con servidores web?**
* El método más común para obtener las llaves públicas para comunicarse con servidores web por medio de certificados X.509. Estos son certificados emitidos por autoridades de certificación confiables y contienen la información de la llave pública, la identidad, el nombre del dominio y de la organización.
* **(ii) ¿Por qué es necesario cifrar G y P con la llave privada?**
* Es necesario cifrar G y P con la llave privada del servidor para garantizar la autenticidad y confidencialidad de estos valores. Al cifrarlos con la llave privada, solo el servidor legítimo puede haberlos generado, lo que previene que un atacante pueda falsificarlos. Si estos valores no fueran cifrados, se podría descubrir la llave privada. Adicionalmente, se protege su confidencialidad durante la transmisión.
* **(iii) El protocolo Diffie-Hellman garantiza “Forward Secrecy”, presente un caso en el contexto del sistema Banner de la Universidad donde sería útil tener esta garantía, justifique su respuesta (por qué es útil en ese caso).**
* En el contexto de Banner, este protocolo Diffie-Hellman podría ser útil para proteger o manejar los datos sensibles de los estudiantes, información financiera y más. Por ejemplo, la información la cual la universidad debe garantizar su integridad y privacidad puede ser enviada de esta manera. Específicamente pueden ser las calificaciones, pagos, datos personales o de contacto.

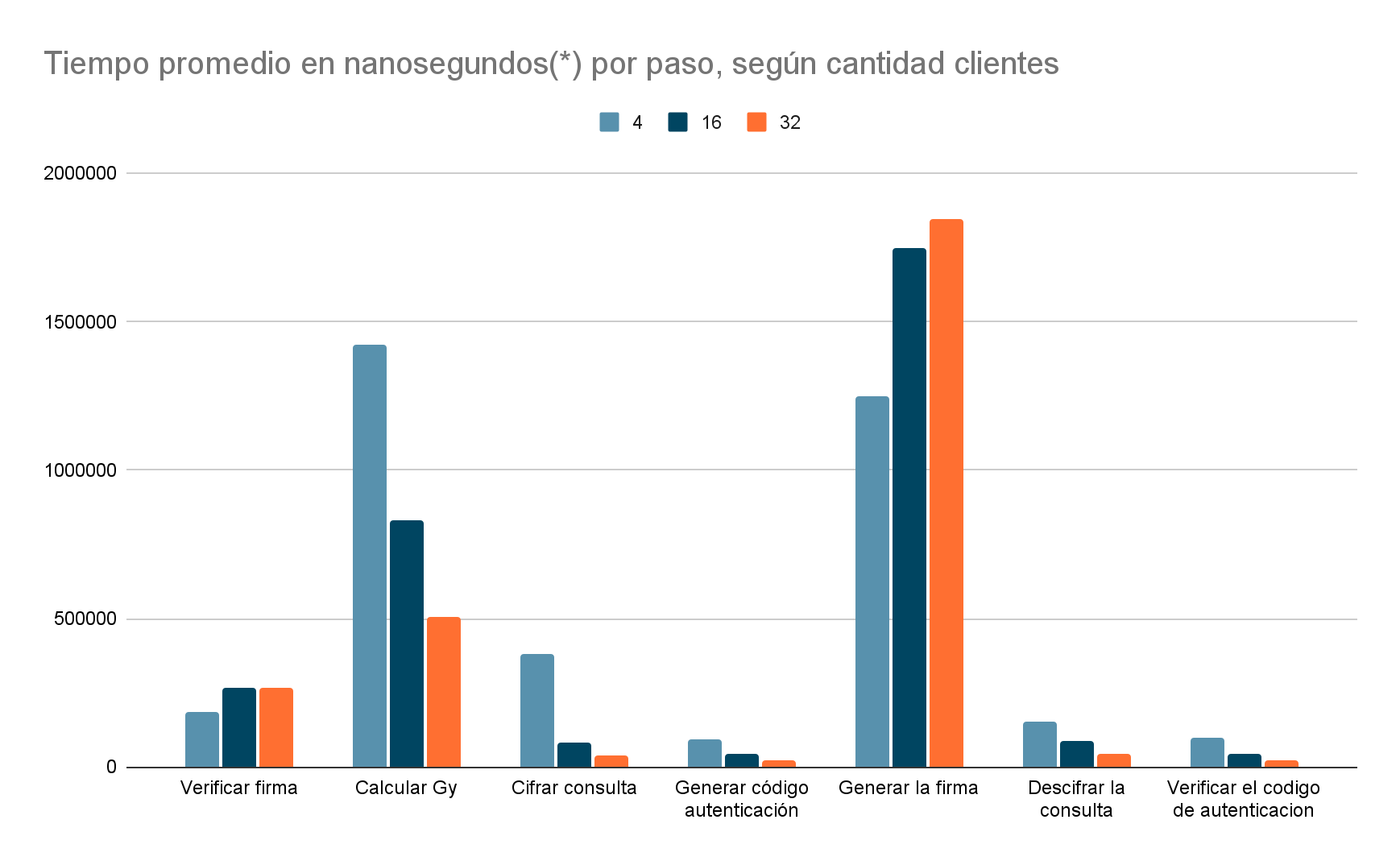
1. **Corra su programa en los diferentes escenarios y mida el tiempo que el cliente demora para:**
   * **(i) Verificar la firma**
   * **(ii) Calcular Gy**
   * **(iii) Cifrar la consulta**
   * **(iv) Generar el código de autenticación**
2. **(los escenarios deben variar el número de clientes delegados debe variar entre 4, 16 y 32 al menos).**
3. **En los mismos escenarios considerados en el punto anterior mida el tiempo que el servidor demora para:**
   * **(i) Generar la firma**
   * **(ii) Descifrar la consulta**
   * **(iii) Verificar el código de autenticación**
4. **Construya una tabla con los datos recopilados (tenga en cuenta que necesitará correr cada escenario en más de una ocasión para validar los resultados) y luego construya una gráfica con los datos de la tabla.**

En las siguientes tablas podemos ver los resultados de tiempo de cada una de las etapas mencionadas anteriormente. Se separan en 3 tablas, para 4 clientes, 16 clientes y 32 clientes.

| **Cantidad clientes** | **Verificar firma** | **Calcular Gy** | **Cifrar consulta** | **Generar código autenticación** | **Generar la firma** | **Descifrar la consulta** | **Verificar el codigo de autenticacion** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **4** | 1375516 | 1732691917 | 187971 | 161833 | 424917 | 282000 | 199200 |
| 126792 | 392363750 | 110208 | 114875 | 1755833 | 109083 | 101125 |
| 143584 | 148580333 | 1109290 | 45834 | 2020917 | 131541 | 46542 |
| 94083 | 9080866458 | 108292 | 42208 | 795583 | 96542 | 42791 |

| **Cantidad clientes** | **Verificar firma** | **Calcular Gy** | **Cifrar consulta** | **Generar código autenticación** | **Generar la firma** | **Descifrar la consulta** | **Verificar el codigo de autenticacion** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **16** | 263292 | 1516165292 | 123332 | 106875 | 4189208 | 136375 | 102459 |
| 213209 | 187745263 | 60357 | 29500 | 114737 | 59417 | 28917 |
| 313666 | 123949874 | 51085 | 19844 | 1507334 | 68541 | 22542 |
| 282508 | 1148792458 | 51667 | 23458 | 1468375 | 48042 | 22873 |
| 169166 | 1173240792 | 59667 | 33083 | 1168041 | 59667 | 31583 |
| 322500 | 828976375 | 64750 | 31583 | 2544542 | 70250 | 33541 |
| 517125 | 1583165291 | 53500 | 27666 | 2535167 | 68667 | 43625 |
| 167541 | 653418208 | 83750 | 34916 | 1453209 | 79833 | 34417 |
| 305083 | 64982260 | 93458 | 38000 | 2433150 | 97250 | 40738 |
| 141542 | 657343750 | 65292 | 32583 | 1351041 | 79167 | 38041 |
| 239500 | 202068427 | 91833 | 39042 | 1468584 | 106041 | 42292 |
| 191875 | 1166585375 | 87000 | 40292 | 1354458 | 98781 | 41750 |
| 192667 | 911252083 | 83958 | 43791 | 1553167 | 80666 | 34708 |
| 447500 | 1470955208 | 108583 | 101167 | 1650750 | 120333 | 104167 |
| 272625 | 1216230042 | 115000 | 41417 | 1674041 | 117750 | 45667 |
| 239292 | 390273333 | 122917 | 47917 | 1542541 | 104125 | 41625 |

| **Cantidad clientes** | **Verificar firma** | **Calcular Gy** | **Cifrar consulta** | **Generar código autenticación** | **Generar la firma** | **Descifrar la consulta** | **Verificar el codigo de autenticacion** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **32** | 231458 | 13590887 | 75209 | 77375 | 3169584 | 67250 | 72750 |
| 378417 | 287909875 | 72625 | 78625 | 1551750 | 63125 | 76458 |
| 285167 | 420958291 | 65583 | 34917 | 1494250 | 68334 | 31834 |
| 210417 | 304536125 | 69292 | 27875 | 1449833 | 56125 | 26416 |
| 282500 | 908581750 | 59958 | 26375 | 1472000 | 62375 | 29709 |
| 273334 | 738737417 | 70167 | 25042 | 1355958 | 53208 | 31083 |
| 268208 | 581479542 | 55083 | 24000 | 1494791 | 59916 | 31959 |
| 298667 | 860134500 | 50708 | 22708 | 1890834 | 55792 | 22125 |
| 238125 | 623502292 | 61792 | 33833 | 1597542 | 44333 | 27083 |
| 205750 | 376352292 | 50834 | 31042 | 2199458 | 53500 | 24916 |
| 207791 | 221015375 | 39459 | 17833 | 1620500 | 64583 | 21084 |
| 225375 | 864723000 | 35125 | 19667 | 1327084 | 47083 | 21041 |
| 208375 | 682861208 | 41292 | 17000 | 1357875 | 31750 | 21875 |
| 177500 | 226631167 | 36583 | 20583 | 1490833 | 50625 | 23083 |
| 157416 | 778912416 | 42709 | 16958 | 523125 | 36333 | 18208 |
| 371000 | 694963708 | 35417 | 24125 | 2932791 | 48333 | 22917 |
| 409208 | 724644708 | 33667 | 18292 | 2408875 | 36125 | 18084 |
| 307375 | 448075875 | 36834 | 14625 | 2559083 | 33209 | 17375 |
| 368000 | 261233708 | 41334 | 23375 | 2489666 | 28834 | 16375 |
| 318416 | 838853167 | 28041 | 12750 | 2304417 | 28959 | 15792 |
| 301625 | 345819917 | 30291 | 17791 | 2479375 | 38584 | 19750 |
| 304084 | 334993167 | 33208 | 12459 | 2294458 | 25667 | 11542 |
| 224584 | 819414917 | 28083 | 14375 | 867625 | 45708 | 17208 |
| 174292 | 475976166 | 25125 | 12375 | 1478709 | 40042 | 20250 |
| 336959 | 701250042 | 22417 | 11417 | 2034500 | 32917 | 13750 |
| 161958 | 233595125 | 38292 | 11834 | 1139125 | 31958 | 10583 |
| 303125 | 444722042 | 21459 | 11209 | 2465500 | 22542 | 9375 |
| 300584 | 827239792 | 19042 | 13042 | 2193292 | 53833 | 13291 |
| 376291 | 433269875 | 25375 | 9375 | 2311041 | 36917 | 15042 |
| 70125 | 162823916 | 24500 | 9375 | 547792 | 22458 | 9375 |
| 287791 | 345118875 | 22625 | 11334 | 2344459 | 26250 | 9708 |
| 311166 | 115077167 | 21583 | 14959 | 2298375 | 18333 | 8541 |

****

**(**\*El valor de calcular Gy fue dividido por 1000 para ajustar la gráfica por lo que este valor está en microsegundos.

1. **Escriba sus comentarios sobre los resultados.**

Al analizar los resultados promedio obtenidos de las tres tablas y en la gráfica mostrada anteriormente, podemos ver como en todos los casos el proceso que más tiempo toma es el de calcular Gy seguido de generar la firma. A excepción de 2 pasos, el proceso de 4 clientes toma más tiempo por paso que 16 y 32 clientes. Cinco de los siete pasos tienen el mismo patrón descendiente de 4 clientes a 16 clientes de manera casi lineal. Los otros dos pasos tienen un tiempo mayor para 32 clientes descendiendo en 16 y en 4 clientes. Nosotros estábamos esperando una distribución contraria a la que obtuvimos, con mayores tiempo en 32 clientes sobre 4 clientes. Tiene sentido que los pasos que más tiempo toman son los de generación y cálculo de algún resultado pues son los pasos que más pasos requieren. El paso que menos tiempo consume es el de verificar pues al ser una simple condición no toma mucho tiempo.

1. **Identifique la velocidad de su procesador, y estime cuántas consultas puede cifrar su máquina, cuántos códigos de autenticación puede calcular y cuántas verificaciones de firma, por segundo. Escriba todos sus cálculos.**

Referencias

*Configuración del servidor para la verificación de la firma digital de solicitudes: elección del método de verificación*. IBM. (2023b, February 13). https://www.ibm.com/docs/es/was/8.5.5?topic=cxdsv5wsat-configuring-server-request-digital-signature-verification-choosing-verification-method-2

Khan Academy. (n.d.). *Cifrado de Llave Pública (artículo)*. Khan Academy. https://es.khanacademy.org/computing/ap-computer-science-principles/x2d2f703b37b450a3:online-data-security/x2d2f703b37b450a3:data-encryption/a/public-key-encryption

López, A. (2024, January 9). *Todo sobre Criptografía: Algoritmos de Clave Simétrica y Asimétrica*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/

SSL.com, E. de soporte de. (2021, February 24). *¿Qué es un certificado x.509?* https://www.ssl.com/es/preguntas-frecuentes/%C2%BFQu%C3%A9-es-un-certificado-x-509%253F/