Miguel Gomez – 202122562
David Pérez - 202123314

# Caso de estudio 3 – Canales Seguros

1. **Preguntas**
   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?**

   En el contexto de los servidores web las llaves públicas de los servidores se distribuyen comúnmente a través de certificados digitales que son documentos electrónicos que utilizan la criptografía de llave pública para probar la propiedad de una llave pública. Estos certificados son emitidos y firmados por una Autoridad Certificadora (CA).

   El proceso comienza con la generación de un par de llaves por el servidor, una pública y otra privada. Luego, el servidor crea una Solicitud de Firma de Certificado (CSR) que incluye su clave pública y detalles de identificación, que se envía a una Autoridad Certificadora (CA) confiable. La CA verifica la identidad del solicitante y, una vez confirmada, firma el certificado con su propia llave privada. Este certificado firmado se instala en el servidor, que lo presenta a los clientes cuando se conectan. Los clientes, a su vez, verifican que el certificado esté firmado por una CA de confianza y que el certificado sea válido en términos de no estar expirado ni revocado, lo que permite establecer una conexión segura usando la llave pública contenida en el certificado. De esta manera se asegura la autenticidad de la llave pública del servidor y facilita que quienes se conecten a él obtengan en sus conexiones una comunicación segura y privada.

   ii. **¿Por qué es necesario cifrar G y P con la llave privada?**

   Es necesario cifrar G y P con la llave privada ya que este proceso sirve como una medida de seguridad para garantizar que toda la información intercambiada entre el cliente y el servidor mantenga su confidencialidad. Al cifrar estos valores, el servidor controla quién tiene acceso a la información para el intercambio de llaves. De esta manera asegura que solo los clientes que poseen la llave pública correcta puedan descifrar y utilizar G y P de manera corriente. Adicionalmente, este método garantiza la integridad y la autenticidad del intercambio de datos, ya que cualquier alteración en los datos cifrados será evidente y fácilmente detectable una vez que el cliente intente descifrarlos con la llave pública del servidor. El cifrado con la llave

privada se complementa con una firma digital sobre el resultado cifrado, proveyendo una capa de seguridad adicional contra actores malintencionados externos. Cifrar G y P con la llave privada no solo protege los datos contra interceptaciones (ataques cibernéticos), sino que también verifica que los datos provengan de fuentes legitimas.

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 del sistema Banner de la Universidad, que maneja información sensible como registros académicos, información personal de estudiantes y empleados, y transacciones financieras, garantizar "Forward Secrecy" mediante el protocolo Diffie-Hellman sería útil durante las comunicaciones entre el cliente y el servidor que aloja el sistema Banner.
"Forward Secrecy" es crucial durante la transmisión de información financiera, como cuando los estudiantes realizan pagos de matrícula. Si en algún momento futuro la llave privada del servidor se ve comprometida, ya sea por un ataque de seguridad o por un error, la "Forward Secrecy" asegura que las sesiones de comunicación pasadas, que podrían haber incluido la transmisión de información financiera sensible, no puedan descifrarse retroactivamente con la llave comprometida.
La "Forward Secrecy" es útil en este caso porque impide que un adversario que haya obtenido acceso a la llave privada del servidor pueda descifrar comunicaciones previas. Sin "Forward Secrecy", todas las comunicaciones pasadas cifradas con esa llave privada serían vulnerables a ser descifradas y expuestas, lo que podría llevar a violaciones significativas de la privacidad de los usuarios involucrados en el sistema.

Miguel Gomez – 202122562
David Pérez - 202123314

2. **Medición de tiempos del cliente**

| **Verificar la firma** | | | **Calcular G^y** | | |
|---|---|---|---|---|---|
| Clientes | Tiempo (ms) | Promedio | Clientes | Tiempo (ms) | Promedio |
| 4 | 22 | 29 | 4 | 7 | 12,25 |
| | 25 | | | 10 | |
| | 34 | | | 11 | |
| | 35 | | | 21 | |

| **Cifrar la consulta** | | | **Generar el código de autenticación** | | |
|---|---|---|---|---|---|
| Clientes | Tiempo (ms) | Promedio | Clientes | Tiempo (ms) | Promedio |
| 4 | 2 | 2,75 | 4 | 0 | 0,5 |
| | 2 | | | 1 | |
| | 3 | | | 1 | |
| | 4 | | | 0 | |

| Verificar la firma | | | | Calcular G^y | | | |
|---|---|---|---|---|---|---|---|
| Clientes | Tiempos (ms) | | Promedio | Clientes | Tiempos (ms) | | Promedio |
| 8 | 35 | 74 | 65,25 | 8 | 14 | 19 | 19,625 |
| | 47 | 76 | | | 17 | 19 | |
| | 48 | 78 | | | 18 | 23 | |
| | 67 | 97 | | | 23 | 24 | |

| Cifrar la consulta | | | | Generar el código de autenticación | | | |
|---|---|---|---|---|---|---|---|
| Clientes | Tiempos (ms) | | Promedio | Clientes | Tiempos (ms) | | Promedio |
| 8 | 1 | 2 | 2,375 | 8 | 0 | 0 | 0,25 |
| | 2 | 2 | | | 0 | 0 | |
| | 2 | 3 | | | 0 | 0 | |
| | 3 | 4 | | | 1 | 1 | |

Miguel Gomez – 202122562
David Pérez - 202123314

| Verificar la firma | | | | | | Calcular G^y | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Clientes | Tiempos (ms) | | | | Promedio | Clientes | Tiempos (ms) | | | | Promedio |
| 16 | 33 | 38 | 42 | 45 | 136,1875 | 16 | 10 | 11 | 12 | 13 | 55,3125 |
| | 48 | 109 | 116 | 153 | | | 13 | 14 | 14 | 14 | |
| | 167 | 169 | 175 | 186 | | | 16 | 17 | 19 | 20 | |
| | 192 | 294 | 250 | 162 | | | 35 | 213 | 222 | 242 | |
| Cifrar la consulta | | | | | | Generar el código de autenticación | | | | | |
| Clientes | Tiempos (ms) | | | | Promedio | Clientes | Tiempos (ms) | | | | Promedio |
| 16 | 1 | 2 | 2 | 2 | 4,5625 | 16 | 0 | 0 | 0 | 0 | 0,3125 |
| | 2 | 2 | 3 | 3 | | | 0 | 0 | 0 | 0 | |
| | 3 | 4 | 4 | 5 | | | 0 | 0 | 0 | 0 | |
| | 5 | 8 | 11 | 16 | | | 1 | 1 | 1 | 2 | |

| Verificar la firma | | | | | | Calcular G^y | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Clientes | Tiempos | | | | Promedio | Clientes | Tiempos | | | | Promedio |
| 32 | 38 | 40 | 41 | 61 | 263,28125 | 32 | 10 | 11 | 13 | 13 | 71,8125 |
| | 142 | 144 | 149 | 154 | | | 14 | 14 | 15 | 15 | |
| | 154 | 165 | 176 | 190 | | | 15 | 18 | 19 | 21 | |
| | 201 | 219 | 243 | 262 | | | 24 | 25 | 31 | 33 | |
| | 264 | 270 | 272 | 289 | | | 39 | 42 | 49 | 54 | |
| | 348 | 357 | 379 | 384 | | | 61 | 69 | 74 | 82 | |
| | 394 | 400 | 405 | 411 | | | 87 | 116 | 117 | 140 | |
| | 413 | 475 | 481 | 504 | | | 150 | 243 | 268 | 416 | |
| Cifrar la consulta | | | | | | Generar el código de autenticación | | | | | |
| Clientes | Tiempos | | | | Promedio | Clientes | Tiempos | | | | Promedio |
| 32 | 1 | 1 | 2 | 2 | 14,71875 | 32 | 0 | 0 | 0 | 0 | 1,21875 |
| | 2 | 2 | 2 | 2 | | | 0 | 0 | 0 | 0 | |
| | 2 | 3 | 3 | 3 | | | 0 | 0 | 0 | 0 | |
| | 4 | 4 | 4 | 4 | | | 0 | 0 | 0 | 0 | |
| | 4 | 4 | 5 | 5 | | | 1 | 1 | 1 | 0 | |
| | 8 | 9 | 10 | 15 | | | 1 | 1 | 1 | 1 | |
| | 26 | 30 | 31 | 43 | | | 1 | 1 | 1 | 1 | |
| | 51 | 55 | 63 | 71 | | | 3 | 7 | 9 | 9 | |

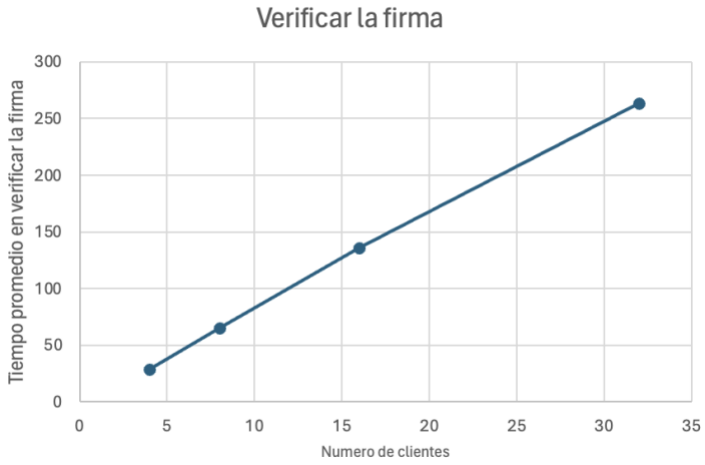
## 3. **Medición de tiempos del servidor**

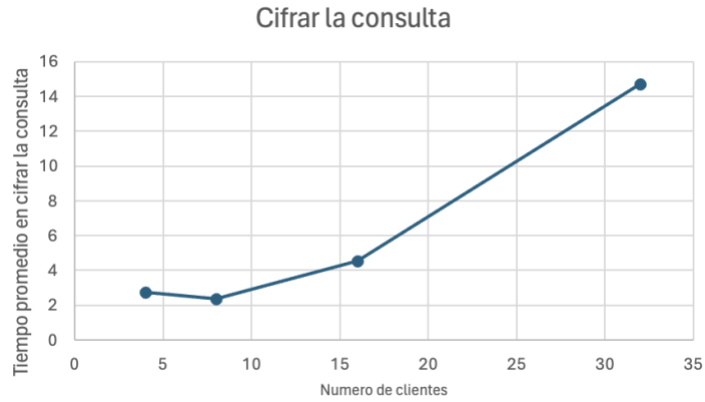
| Tiempo para generar la firma(ms) | | | | | | Tiempo decifrar la consulta (ms) | | | | | | Tiempo verificar el cod(ms) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 44 | 43 | 49 | 35 | 138 | 42 | 2 | 3 | 4 | 6 | 14 | 39 | 0 | 0 | 0 | 0 | 0 | 1 |
| 46 | 27 | 34 | 21 | 328 | 78 | 2 | 3 | 4 | 7 | 17 | 53 | 0 | 0 | 0 | 0 | 0 | 1 |
| 49 | 31 | 75 | 169 | 221 | 146 | 2 | 4 | 5 | 7 | 17 | 56 | 0 | 0 | 0 | 0 | 0 | 1 |
| 86 | 34 | 31 | 219 | 188 | 180 | 2 | 4 | 5 | 7 | 23 | 57 | 0 | 0 | 0 | 0 | 0 | 1 |
| 111 | 82 | 39 | 29 | 275 | 39 | 2 | 4 | 5 | 8 | 26 | 58 | 0 | 0 | 0 | 0 | 0 | 1 |
| 49 | 219 | 40 | 212 | 320 | 44 | 3 | 4 | 5 | 10 | 27 | 71 | 0 | 0 | 0 | 0 | 0 | 1 |
| 63 | 160 | 119 | 188 | 402 | 45 | 3 | 4 | 5 | 11 | 28 | 82 | 0 | 0 | 0 | 1 | 0 | 2 |
| 67 | 46 | 26 | 153 | 450 | 50 | 3 | 6 | 5 | 13 | 146 | 23 | 0 | 0 | 0 | 2 | 0 | 2 |
| 44 | 38 | 259 | 231 | 431 | 59 | 3 | 6 | 6 | 13 | 88 | 45 | 0 | 0 | 0 | 1 | 1 | 2 |
| Promedio | | | | | | Promedio | | | | | | Promedio | | | | | |
| 122,2962963 | | | | | | 19,55555556 | | | | | | 0,314814815 | | | | | |

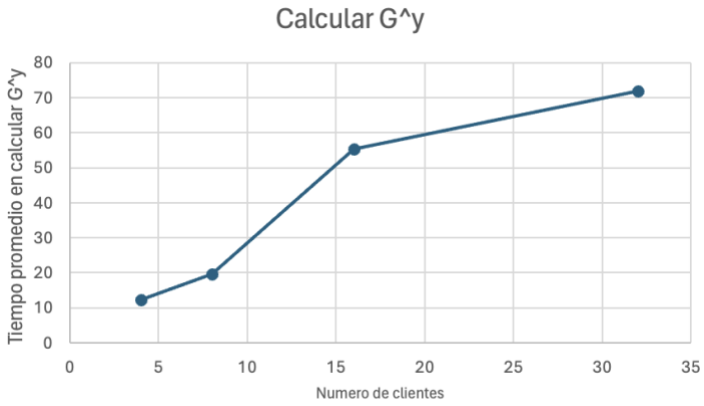
## 4. **Datos recopilados**

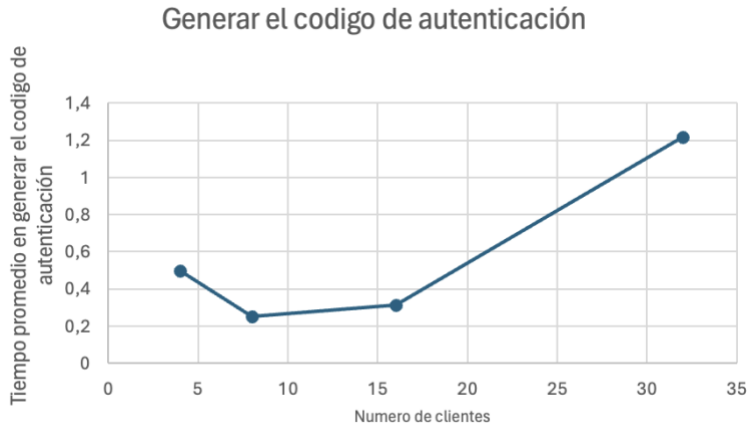
Miguel Gomez – 202122562
David Pérez - 202123314

i. **Cliente**

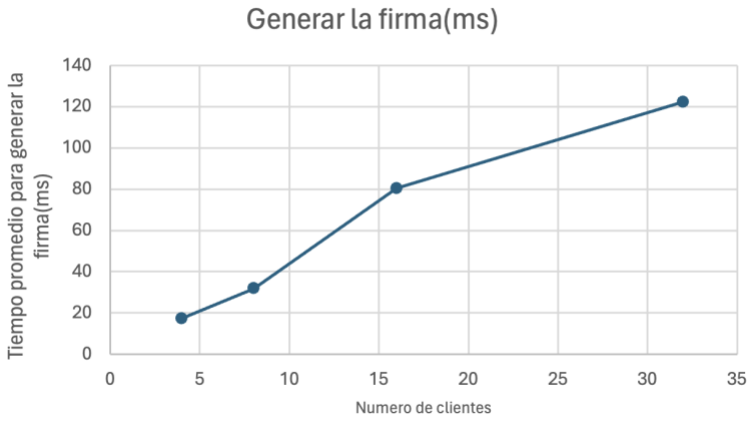


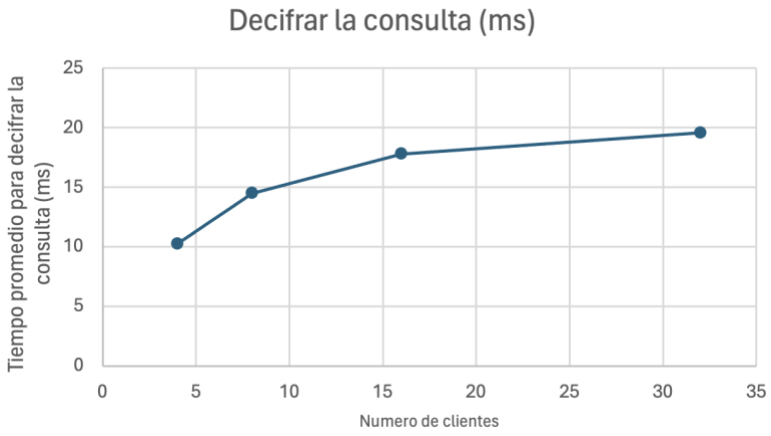



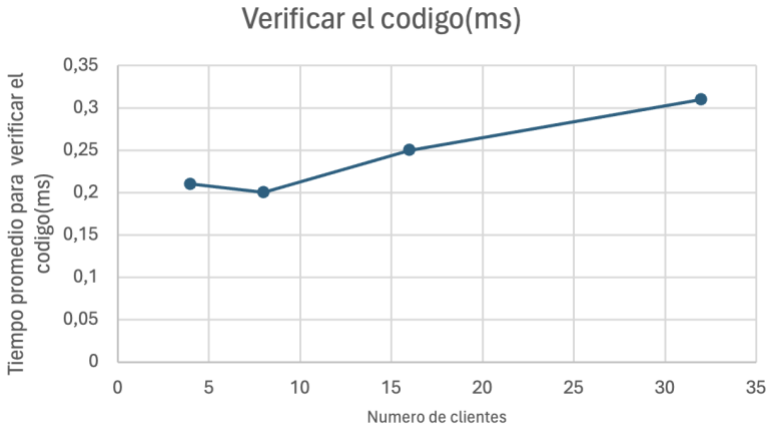

Calcular G^y
Tiempo promedio en calcular G^y
Numero de clientes
0
10
20
30
40
50
60
70
80
0
5
10
15
20
25
30
35


Generar el codigo de autenticación
Tiempo promedio en generar el codigo de autenticación
Numero de clientes
0
0,2
0,4
0,6
0,8
1
1,2
1,4
0
5
10
15
20
25
30
35

ii. **Servidor**


Generar la firma(ms)
Tiempo promedio para generar la firma(ms)
Numero de clientes
0
20
40
60
80
100
120
140
0
5
10
15
20
25
30
35




5. **Comentarios de los resultados**

A partir de la observación de los tiempos de ejecución en un entorno con múltiples clientes concurrentes, se puede concluir que los procesos que implican una mayor carga computacional y dependencia de la capacidad del sistema tienden a escalar en tiempo de ejecución a medida que aumenta la carga de trabajo. El tiempo requerido para verificar la firma digital muestra el mayor incremento, debido a la necesidad de realizar cálculos criptográficos que dependen de la longitud de la clave y del algoritmo utilizado.

Esto es consistente con el comportamiento esperado de operaciones criptográficas, que son conocidas por su demanda de recursos cuando se manejan en volumen. Por otro lado, el tiempo para calcular G^y, aunque también aumenta con el número de clientes, no lo hace en la misma proporción que la verificación de la firma. Esto podría indicar que, aunque el cálculo es también intensivo en recursos, es más eficiente y menos afectado por los incrementos en la

concurrencia comparado con la verificación de la firma. El aumento menos significativo en el tiempo para cifrar la consulta refleja que las operaciones de cifrado, aunque necesarias, están optimizadas y no son el cuello de botella principal en este contexto.

Finalmente, los tiempos para generar códigos de autenticación, que se mantuvieron relativamente estables, muestran que este proceso es eficiente y no está influenciado por el número de transacciones simultáneas en la misma medida que las otras tareas. Por el lado del servidor, la observación de que el tiempo para generar la firma y descifrar la consulta aumenta con más clientes mientras que la verificación del código de autenticación permanece constante, sugiere una buena escalabilidad en la gestión de verificaciones, pero genera una necesidad de mejora en la generación y decodificación de firmas.

6. **Estimaciones sobre maquina**

**Maquina: Apple M1, 16Gb Ram**

$$\boldsymbol{Verificación\ de\ la\ firma}$$

$$\text{Tiempo promedio en verificar la firma} = \mathbf{263.28\ ms}$$

$$\text{Verificaciones por segundo} = \frac{\mathbf{1000\ ms}}{\mathbf{263.28\ ms}} \approx \mathbf{3.8}$$

$$\boldsymbol{Cifrado\ de\ la\ consulta}$$
$$\boldsymbol{textTiempopromedioencifrarlaconsulta} = \mathbf{14.71\ ms}$$

$$\text{Cifrados por segundo} = \frac{\mathbf{1000\ ms}}{\mathbf{14.71\ ms}} \approx \mathbf{68}$$

$$\boldsymbol{Generación\ del\ código\ de\ autenticación}$$

$$\text{Tiempo promedio en generar el código de autenticación} = \mathbf{1.2187\ ms}$$

$$\text{Generaciones de código por segundo} = \frac{\mathbf{1000\ ms}}{\mathbf{1.2187\ ms}} \approx \mathbf{820}$$

Miguel Gomez – 202122562
David Pérez - 202123314

| Operación | Tiempo Promedio (ms) | Operaciones por segundo |
|---|---|---|
| Verificar la firma | 263,28 | 3,8 |
| Cifrar la consulta | 14,71 | 68 |
| Generar el código de autenticación | 1,2187 | 820 |