



Universidad Anáhuac Mayab

Ingeniería en tecnologías de información y negocios digitales

Asignatura: Seguridad informática y análisis forense

Parcial 1

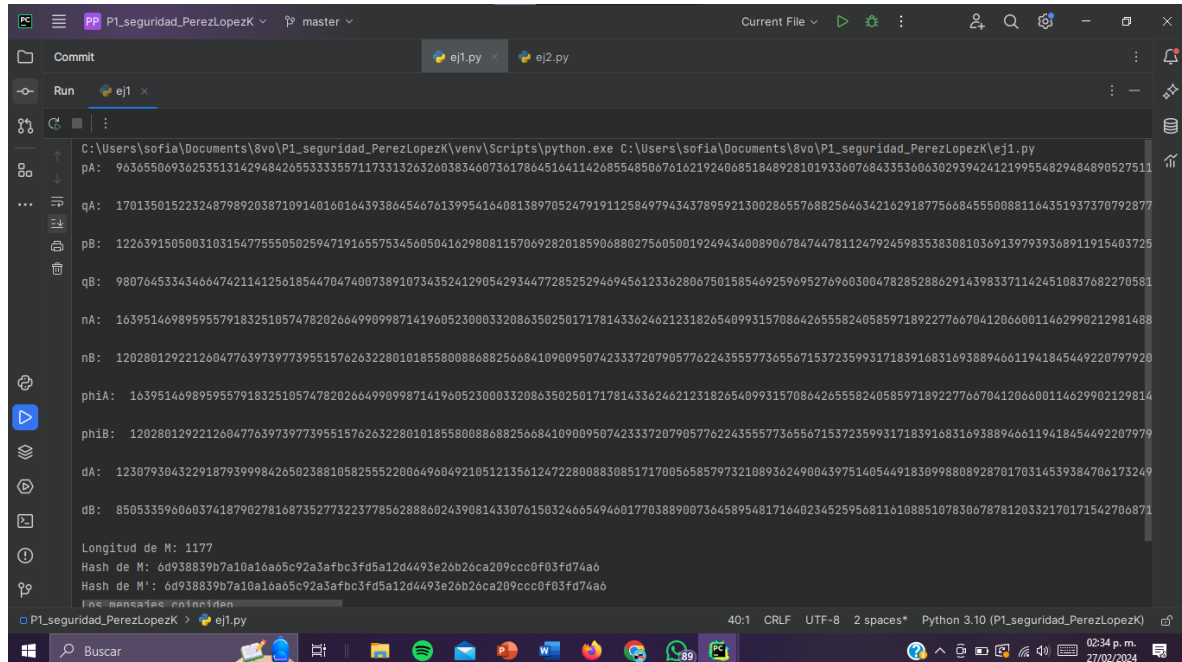
Docente: Fabricio A. Suarez Dominguez

Fecha de entrega: 27/Agosto/2022

REPOSITORIO:

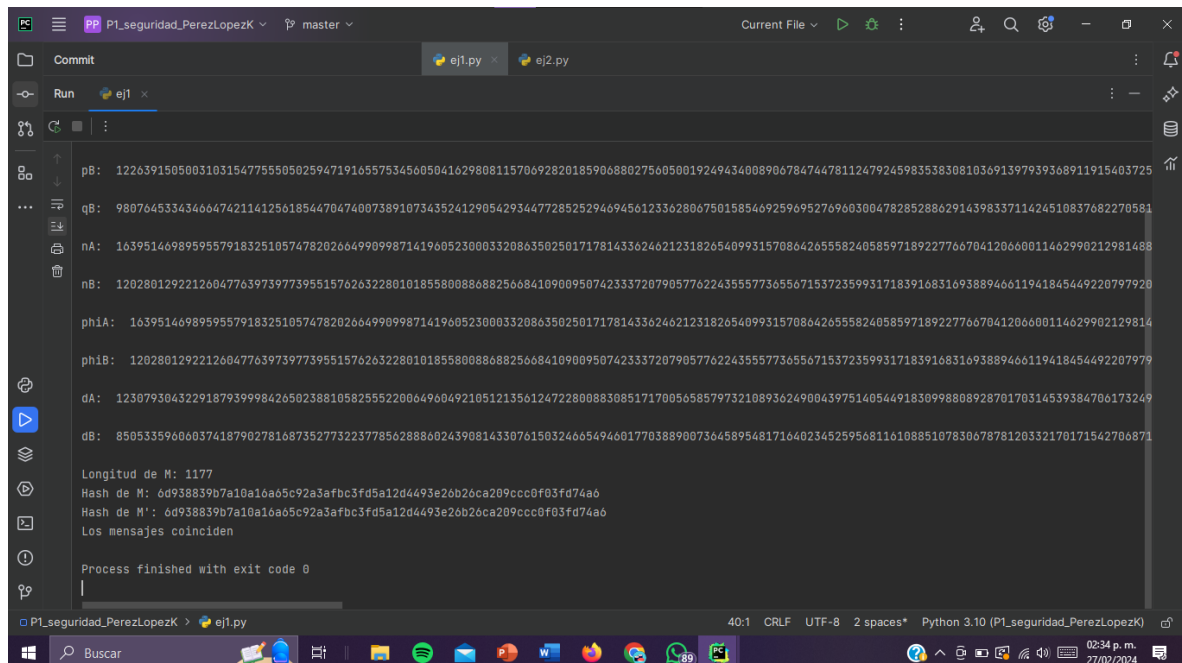
https://github.com/KSofiaPerez14/P1_seguridad_PerezLopezK.git

EJERCICIO 1:



```
C:\Users\sofia\Documents\8vo\P1_seguridad_PerezLopezK\venv\Scripts\python.exe C:\Users\sofia\Documents\8vo\P1_seguridad_PerezLopezK\ej1.py
pA: 963655069362535131429484265533335571173313263260383460736178645164114268554850676162192406851848928101933607684335360630293942412199554829484896527511
qA: 170135015223248798920387109140160164393864546761399541640813897052479191125849794343789592130028655768825646342162918775668455500881164351937370792877
pB: 122639150500310315477555050259471916557534560504162980811570692820185906880275605001924943400890678474478112479245983538308103691397939368911915403725
qB: 980764533434664742114125618544704740073891073435241290542934477285252946945612336280675015854692596952769603004782852886291439833711424510837682270581
nA: 163951469895955791832510574782026649909987141960523000332086350250171781433624621231826540993157086426555824058597189227766704120660011462990212981488
nB: 120280129221260477639739773955157626322801018558008868825668410900950742333720790577622435557736556715372359931718391683169388946611941845449220797920
phiA: 1639514698959557918325105747820266499099871419605230003320863502501717814336246212318265409931570864265558240585971892277667041206600114629902129814
phiB: 1202801292212604776397397739551576263228010185580088688256684109009507423337207905776224355577365567153723599317183916831693889466119418454492207979
dA: 12307930432291879399984265023881058255220064960492105121356124722800883085171700565857973210893624900439751405449183099880892870170314539384706173249
dB: 850533596060374187902781687352773223778562888602439081433076150324665494601770388900736458954817164023452595681161088510783067878120332170171542706871

Longitud de M: 1177
Hash de M: 6d938839b7a10a16a65c92a3afbc3fd5a12d4493e26b26ca209ccc0f03fd74a6
Hash de M': 6d938839b7a10a16a65c92a3afbc3fd5a12d4493e26b26ca209ccc0f03fd74a6
Los mensajes coinciden
```

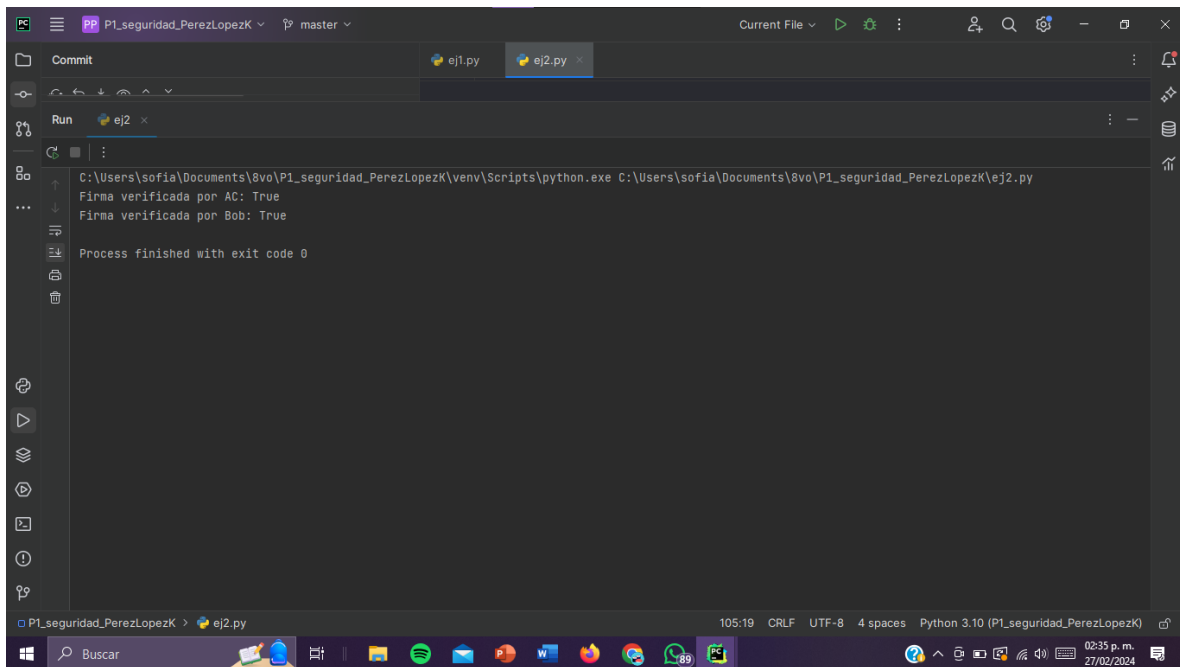


```
pB: 122639150500310315477555050259471916557534560504162980811570692820185906880275605001924943400890678474478112479245983538308103691397939368911915403725
qB: 980764533434664742114125618544704740073891073435241290542934477285252946945612336280675015854692596952769603004782852886291439833711424510837682270581
nA: 163951469895955791832510574782026649909987141960523000332086350250171781433624621231826540993157086426555824058597189227766704120660011462990212981488
nB: 120280129221260477639739773955157626322801018558008868825668410900950742333720790577622435557736556715372359931718391683169388946611941845449220797920
phiA: 1639514698959557918325105747820266499099871419605230003320863502501717814336246212318265409931570864265558240585971892277667041206600114629902129814
phiB: 1202801292212604776397397739551576263228010185580088688256684109009507423337207905776224355577365567153723599317183916831693889466119418454492207979
dA: 12307930432291879399984265023881058255220064960492105121356124722800883085171700565857973210893624900439751405449183099880892870170314539384706173249
dB: 850533596060374187902781687352773223778562888602439081433076150324665494601770388900736458954817164023452595681161088510783067878120332170171542706871

Longitud de M: 1177
Hash de M: 6d938839b7a10a16a65c92a3afbc3fd5a12d4493e26b26ca209ccc0f03fd74a6
Hash de M': 6d938839b7a10a16a65c92a3afbc3fd5a12d4493e26b26ca209ccc0f03fd74a6
Los mensajes coinciden

Process finished with exit code 0
```

EJERCICIO 2:



```
C:\Users\sofia\Documents\8vo\P1_seguridad_PerezLopezK\venv\Scripts\python.exe C:\Users\sofia\Documents\8vo\P1_seguridad_PerezLopezK\ej2.py
Firma verificada por AC: True
Firma verificada por Bob: True
Process finished with exit code 0
```

PREGUNTAS:

1. Describir la importancia del método RSA en el contexto del protocolo https.

El método RSA es muy importante para la seguridad del protocolo HTTPS principalmente porque la seguridad de dicho método se basa en la dificultad de factorizar números enteros grandes, lo que lo hace muy resistente a los ataques, además de que es rápido y eficiente, lo que lo hace adecuado para su uso en aplicaciones web, por lo que se puede utilizar para una variedad de aplicaciones, incluyendo la firma digital, el cifrado de correo electrónico y la protección de datos.

2. Describa en que consiste la capa 7 del modelo OSI y cuáles son los principales ataques a dicha capa.

La capa 7 o capa de aplicación, es la capa más alta del modelo OSI. Se encarga de la interacción entre las aplicaciones del usuario y la red. Esta capa permite que las aplicaciones se comuniquen entre sí, define cómo se codifican y decodifican los datos para su transmisión, establece, mantiene y termina las sesiones de comunicación entre las aplicaciones y se asegura de que los datos se transmiten y reciben de forma coherente.

Los principales ataques a la capa 7 son:

- Ataques de denegación de servicio (DoS): Inundan el servidor con solicitudes falsas, lo que lo hace inoperable.

- Ataques de phishing: Intentan engañar al usuario para que revele información confidencial.
- Ataques de inyección de código: Insertan código malicioso en una aplicación web.
- Ataques de secuestro de sesión: Roban la sesión de un usuario legítimo.
- Ataques de intermediario (Man-in-the-Middle): Interceptan la comunicación entre dos aplicaciones y modifican los datos.

3. Describe cuál es la importancia del algoritmo RSA en tus propias palabras.

La importancia del algoritmo RSA desde mi punto de vista, radica principalmente en la seguridad y confidencialidad, ya que permite encriptar información, convirtiéndola en un código indescifrable para quienes no poseen la clave de descryptación, protegiendo la información sensible, como contraseñas, datos bancarios o comunicaciones privadas, de posibles atacantes. Además permite verificar la integridad de los datos, asegurando que no hayan sido modificados o alterados desde su origen, lo cual nos puede ayudar a evitar fraudes, manipulaciones y garantizar la confiabilidad de la información, también es funcional para la autenticación de usuarios y dispositivos, ya que verifica la identidad de las partes involucradas en una comunicación digital, evitando suplantaciones de identidad y ataques de intermediario. Todo esto es aplicable en las cosas que realizamos en el día a día, desde navegar en internet y proteger nuestra información en nuestras búsquedas y visitas a sitios web, hasta las firmas digitales o las compras en línea.

4. ¿Qué uso le darías en la vida real al cifrado asimétrico usando RSA?

Para enviar correos electrónicos seguros que contengan información confidencial o sensible para poder proteger la privacidad de mis comunicaciones, para firmar documentos digitales, y así poder garantizar la autenticidad e integridad de mis documentos, para proteger mi identidad y datos al navegar en internet, para realizar transacciones en línea seguras, ya que esto me ayudaría a proteger mis datos financieros durante compras y pagos y para almacenar mi información confidencial, ya que esto aseguraría la privacidad de mis datos sensibles, como contraseñas o información médica o bancaria.

5. Describe cuál es la importancia de la ciberseguridad en nuestro entorno y como debemos protegernos.

La importancia de la ciberseguridad en nuestro entorno radica en que protege información personal y financiera, como nuestras contraseñas, números de tarjetas

de crédito y registros médicos son vulnerables a ataques cibernéticos, previene el robo de identidad, ya que los hackers pueden suplantar nuestra identidad para cometer fraudes o delitos y la ciberseguridad ayuda a prevenir el robo de identidad, así como ayuda a disminuir el impacto de ataques cibernéticos que pueden causar daños económicos y afectar la confianza de los usuarios. La ciberseguridad, además protege los sistemas como redes eléctricas, sistemas de transporte y hospitales dependen de la tecnología digital. Algunas maneras de protegernos podrían ser utilizar contraseñas seguras y diferentes para cada cuenta, mantener software y sistemas operativos actualizados, tener cuidado al hacer clic en enlaces o descargar archivos o no entrar a links que nos proporcionen desconocidos, utilizar un antivirus y firewall confiables, realizar copias de seguridad de datos importantes y cifrar la información sensible.