GUÍA PRÁCTICA DIDÁCTICA: CIFRADO ASIMÉTRICO OPENPGP

Implementación de Seguridad con Gpg4win 4.3.1 y Gestor de Claves Kleopatra

Asignatura: Base de Datos II / Seguridad Informática
Herramienta: Gpg4win v4.3.1 (Kleopatra)
Carrera: Licenciatura en Sistemas de Información
Unidad: Criptografía Asimétrica y Firma Digital

Objetivo General de la Práctica

Comprender y aplicar los principios de la **criptografía de clave pública (asimétrica)** utilizando el estándar OpenPGP implementado en el software libre **Gpg4win (versión 4.3.1)**. Al finalizar esta guía, el estudiante estará capacitado para generar pares de claves, exportar e importar certificados públicos, y llevar a cabo las operaciones fundamentales de cifrado, descifrado y firma digital de archivos.

1. MARCO TEÓRICO Y ACLARACIÓN TÉCNICA FUNDAMENTAL

⚠️ Aclaración Conceptual Importante sobre el Inciso (c) del Ejercicio

El enunciado del ejercicio menciona: *"Cifre un archivo con su certificado generado y envíelo a su compañero de grupo y verifique que lo pueda descifrar con la clave pública enviada"*.

Desde el punto de vista de la **Criptografía Asimétrica (OpenPGP)**, es vital comprender la simetría operativa de los roles de las claves:

- **Cifrado para Privacidad (Confidencialidad):** Si deseas enviar un archivo cifrado a tu compañero para que solo él pueda leerlo, debes cifrar el archivo usando la **clave pública de tu compañero**. Él utilizará su propia **clave privada** (que nunca comparte) para descifrarlo.
- **Uso de la Clave Pública Propia:** Si cifras un archivo utilizando únicamente tu propia clave pública, tu compañero **NO podrá descifrarlo** utilizando solo tu clave pública. La clave pública sirve para *encapsular/bloquear* los datos, y solo la clave privada correspondiente puede *desbloquearlos*.
- **Firma Digital (Autenticidad e Integridad):** Si cifras/firmas un archivo con tu **clave privada**, tu compañero sí usará tu **clave pública** para verificar tu identidad y que el archivo no fue alterado en tránsito.

Modalidad Didáctica Adoptada: En esta guía realizaremos la experiencia completa e interactiva en ambas direcciones para que comprendas de manera rigurosa cómo interactúan las claves públicas y privadas en un canal de comunicación seguro real.

2. PREPARACIÓN E INSTALACIÓN DEL ENTORNO

Paso 1 Descarga e Instalación de Gpg4win 4.3.1

1. Acceda al sitio web oficial de la herramienta: `https://gpg4win.org/download.html`.
2. Descargue la versión **Gpg4win 4.3.1** (o la versión estable actual de la rama 4.3.x).
3. Ejecute el instalador `gpg4win-4.3.1.exe` con privilegios de administrador.

4. Durante el asistente de selección de componentes, asegúrese de marcar obligatoriamente:
    - **Kleopatra:** El gestor gráfico de certificados OpenPGP y S/MIME.
    - **GnuPG:** El motor criptográfico subyacente.
    - **GpgEX:** Extensión para el Explorador de Windows (permite cifrar con clic derecho).
5. Complete el proceso de instalación y ejecute la aplicación **Kleopatra** desde el menú de inicio.

3. DESARROLLO PASO A PASO DEL TRABAJO PRÁCTICO

Inciso A: Generación del Par de Claves Asimétricas

En este paso, cada integrante del grupo creará su propia identidad criptográfica formada por dos claves matemáticamente vinculadas: la clave pública y la clave privada.

1. Abra la interfaz principal de **Kleopatra**.
2. Haga clic en el botón **"Nuevo par de claves..."** (o vaya al menú *Archivo > Nuevo par de claves...*).
3. Seleccione la opción **"Crear un par de claves personales OpenPGP"**.
4. Ingrese sus datos personales:
    - **Nombre completo:** (Ejemplo: *Juan Pérez*)
    - **Correo electrónico:** (Ejemplo: *juan.perez@alumnos.unlar.edu.ar*)
5. Haga clic en el botón **"Configuración avanzada..."** para seleccionar el algoritmo criptográfico solicitado por la cátedra.

> **Configuración de Algoritmos Criptográficos en Kleopatra:**
> En la ventana de Configuración Avanzada, podrá elegir entre diversos algoritmos de clave pública:
> - **RSA (Recomendado estándar):** Seleccione el tamaño de clave de **3072 bits** o **4096 bits** para máxima seguridad.
> - **ECDSA / EdDSA (Curvas Elípticas):** Algoritmos modernos como *Ed25519 / Cv25519* que ofrecen alta seguridad con claves de menor tamaño y alto rendimiento.
>
> *Sugerencia para el informe:* Seleccione **RSA de 4096 bits** para este ejercicio.

1. Establezca la fecha de caducidad de la clave (por defecto 2 años, o deshabilítela para uso académico).
2. Haga clic en **OK** y luego en **Crear**.
3. El sistema le solicitará ingresar una **Frase de paso (Passphrase)** para proteger la clave privada:
    - Elija una contraseña robusta (mezcla de mayúsculas, minúsculas, números y símbolos).
    - Esta frase de paso encripta localmente su clave privada en el disco duro.
4. Una vez completado el proceso, verá la confirmación: *"Par de claves creado con éxito"*.

Inciso B: Exportación e Intercambio de Claves Públicas

Para establecer un canal confidencial, los compañeros de grupo deben intercambiar únicamente sus **claves públicas**.

1. **Exportar su Clave Pública:**
   - En Kleopatra, haga clic derecho sobre el certificado recién creado.
   - Seleccione **"Exportar..."** y guarde el archivo en su equipo con el nombre `ClavePublica_SuNombre.asc`.
   - *Alternativa:* Puede elegir *"Copiar"* al portapapeles si prefiere enviar el texto plano del bloque de clave PGP.
2. **Envío al Compañero:** Envíe el archivo `.asc` a su compañero de grupo mediante correo electrónico o mensajería.
3. **Importación de la Clave Pública del Compañero:**
   - Al recibir la clave pública de su compañero (ej: `ClavePublica_Compañero.asc`), guarde el archivo.
   - En Kleopatra, haga clic en **"Importar..."** y seleccione el archivo recibido.
   - Kleopatra mostrará los detalles del certificado importado. Haga clic en **"Aceptar"**.
   - **Certificación** / **Confianza:** Kleopatra le preguntará si desea certificar que la clave pertenece realmente a su compañero. Seleccione *"Certificar..."*, marque la clave e ingrese su frase de paso para validar la identidad de su compañero.

> **¡REGLA DE ORO DE LA CRIPTOGRAFÍA ASIMÉTRICA!**
> **NUNCA** envíe ni comparta su *Clave Privada* (opción "Exportar claves secretas..."). La clave privada debe permanecer almacenada únicamente en su equipo local y protegida con su frase de paso.

Inciso C: Proceso Práctico de Cifrado, Envío y Descifrado

Escenario A: Cifrado de Confidencialidad (Recomendado Criptográficamente)

Objetivo: Usted quiere enviar un archivo a su compañero asegurando que *solamente su compañero* pueda leerlo.

1. Cree un archivo de texto de prueba, por ejemplo: `Mensaje_Secreto.txt` con un texto breve.
2. En Kleopatra, haga clic en el botón **"Sign/Encrypt" (Firmar/Cifrar)** o haga clic derecho sobre el archivo en el explorador de Windows y seleccione *"Firmar y Cifrar"*.
3. En la ventana emergente de selección de destinatarios:
   - Desmarque *"Encrypt for me" (Cifrar para mí)* si solo quiere cifrarlo para él, o déjelo marcado si desea poder abrirlo usted también.
   - Marque **"Encrypt for others" (Cifrar para otros)**.
   - Seleccione de la lista la **Clave Pública de su compañero**.
   - (Opcional) Marque *"Firmar como"* y seleccione su clave para añadir firma digital.
4. Haga clic en **Cifrar** / **Encrypt**. Kleopatra generará un archivo cifrado con extensión `.gpg` (o `.asc`).
5. Envíe dicho archivo cifrado por correo electrónico a su compañero.

6. **Proceso en el equipo de su compañero (Descifrado):**
   - El compañero recibe el archivo y hace doble clic sobre él (o lo arrastra a Kleopatra y selecciona *"Descifrar/Verificar"*).
   - Kleopatra detectará que el archivo está cifrado con su clave pública y le solicitará **su frase de paso privada**.
   - Al ingresar la clave privada correcta, el archivo se descifra exitosamente y se guarda en su disco.

Escenario B: Cifrado con su Propio Certificado y Demostración de Descifrado

Objetivo: Ejecutar literalmente el procedimiento según la interpretación directa del texto de la consigna para documentar sus resultados.

1. Seleccione el archivo `Prueba_Certificado_Propio.txt`.
2. En Kleopatra, seleccione **Firmar/Cifrar**.
3. En los destinatarios, seleccione **únicamente su propia Clave Pública**.
4. Guarde el archivo cifrado resultante `Prueba_Certificado_Propio.txt.gpg` y envíelo a su compañero.
5. **Verificación por parte del compañero:**
   - Su compañero intenta abrir/descifrar el archivo con Kleopatra.
   - **Resultado obtenido:** Kleopatra mostrará un error indicando: *"No se dispone de la clave secreta adecuada para descifrar los datos"*.
   - **Conclusión:** Su compañero no puede descifrarlo solo con la clave pública de usted, demostrando la propiedad fundamental del trampa-puerta (one-way trapdoor function) del cifrado asimétrico. Para que él lo lea, el remitente debe usar la clave pública del receptor.

4. MATRIZ RESUMEN DE OPERACIONES CRIPTOGRÁFICAS

Operación Criptográfica	Clave Utilizada al Emisor	Clave Utilizada al Receptor	Propiedad de Seguridad
Cifrado de Mensaje	Clave Pública del Receptor	Clave Privada del Receptor	Confidencialidad (Solo el receptor lo lee)
Firma Digital	Clave Privada del Emisor	Clave Pública del Emisor	Autenticidad, No Repudio e Integridad
Cifrado y Firma Combinados	Pública Receptor + Privada Emisor	Privada Receptor + Pública Emisor	Confidencialidad + Autenticidad + Integridad

5. GUÍA PARA LA ELABORACIÓN DEL INFORME DE TRABAJO PRÁCTICO

Para presentar la resolución de este práctico ante la cátedra, estructurar el informe final con las siguientes evidencias:

1. **Captura de Pantalla 1:** Interfaz de Kleopatra mostrando las claves generadas, destacando la columna del algoritmo seleccionado (RSA 4096 / Ed25519) y las huellas digitales (Fingerprints).
2. **Captura de Pantalla 2:** Proceso de exportación de la clave pública y visualización del archivo `.asc` en un editor de texto (mostrando las líneas `-----BEGIN PGP PUBLIC KEY BLOCK-----`).
3. **Captura de Pantalla 3:** Lista de certificados en Kleopatra donde se observe la clave pública del compañero importada y certificada.
4. **Captura de Pantalla 4:** Proceso de cifrado de un archivo seleccionando al compañero como destinatario.
5. **Captura de Pantalla 5:** Ventana de éxito al descifrar el archivo recibido del compañero e ingresar la frase de paso privada.
6. **Análisis Crítico / Discusión:** Explicación teórica de los resultados obtenidos en el Escenario A y Escenario B sobre la asimetría funcional de las claves.

Conclusión Pedagógica:
La criptografía asimétrica resuelve de forma elegante el problema de la distribución de llaves de la criptografía simétrica. Con Gpg4win/Kleopatra, cualquier usuario puede mantener un esquema de comunicación 100% seguro y verificado sin requerir un canal previo seguro para intercambiar secretos.