MyPGP
Interfaz de usuario para PGP

6.2.2020

1 Requisitos previos

MyPGP se basa completamente en BouncyCastle para todas las funciones criptográficas: es meramente una interfaz de usuario. Salvo en lo que se indica en la sección “Cifrado Elgamal” más adelante.

MyPGP se distribuye con la última versión de BouncyCastle.

2 Ficheros y directorios

2.1 El directorio HOME

Cuando MyPGP arranca, le pedirá seleccionar una carpeta en su sistema de ficheros. La carpeta seleccionada se considerará HOME para esta ejecución.

2.2 Directorios de claves

MyPGP usa carpetas del sistema de ficheros para organizar las claves, tanto públicas como privadas.

Todas las claves que se encuentren en la carpeta HOME se cargan y aparecen en la rama HOME del panel de claves de la consola.

Si HOME tiene sub-carpetas, estas sub-carpetas se cargan igualmente, apareciendo como ramas anidadas en el panel de claves. Las carpetas se pueden anidar cuantas veces sea conveniente.

Añadir claves es tan sencillo como copiarlas en la carpeta deseada. Eliminar claves es tan sencillo como eliminarlas de la carpeta. La misma clave puede aparecer en más de una carpeta.

Los ficheros en las carpetas citadas pueden ser simples claves, o anillos de claves como

- pubring.pkr
- secring.skr

MyPGP ignora los ficheros y carpetas cuyos nombres empiezan por un carácter de subrayado:

_

o terminan en alguna de las siguientes extensiones:

.skip

.mypgp

.jar

MYPGP no tiene ningún concepto de directorio único de claves. Usted puede tener diferentes grupos de claves en diferentes directorios. Solo tiene que elegir el grupo deseado al iniciar. Esto permite tener diferentes directorios para diferentes proyectos no relacionados entre sí.

2.3 database.mypgp

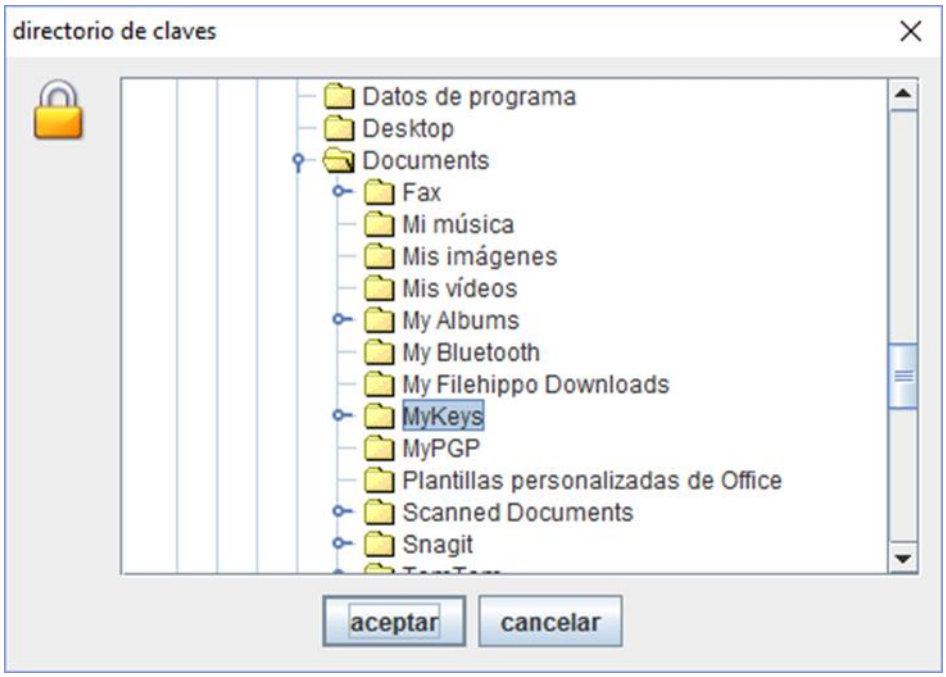
MyPGP usa un fichero de nombre "database.mypgp" en la carpeta HOME para almacenar información acerca de

- aliases
- listas de claves

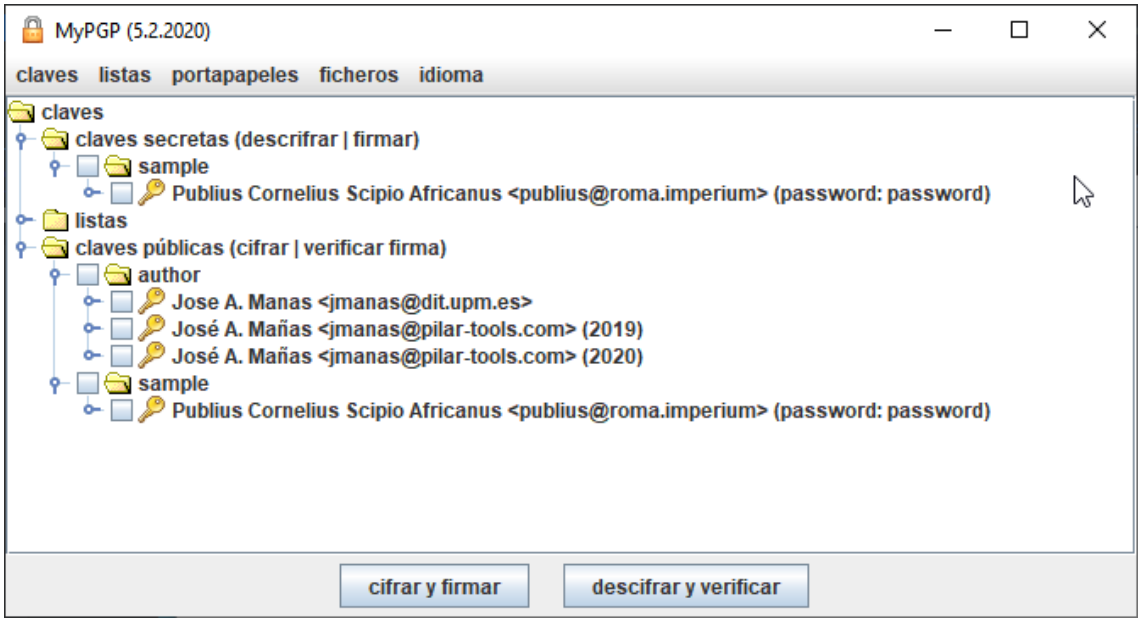
El fichero es de texto y puede editarse, aunque normalmente se encarga MyPGP de escribirlo a partir de las acciones en la interfaz de usuario.

3 Arranque

Seleccione el directorio de claves



4 Panel principal



4.1 Ejemplo: cifrar un fichero

1. Seleccione una o más claves públicas
2. Navegue y seleccione el fichero que desea cifrar (uno o más)
   ficheros >> cifrar

También puede arrastrar el fichero desde un explorador al botón CIFRAR y FIRMAR.

Una traza aparece en la consola indicando el éxito o el fracaso de la operación

4.2 Ejemplo: firmar un fichero

1. Seleccione una o más claves de firma del directorio
2. Navegue y seleccione uno o más ficheros a firmar
   ficheros >> firmar

También puede arrastrar el fichero desde un explorador al botón CIFRAR Y FIRMAR.

En consola queda una traza de la operación

4.3 Ejemplo, cifrar y firmar

De forma igual a los ejemplos anteriores, pero seleccionando tanto claves secretas para la firma como claves públicas para la cifra.

5 Menú claves

nueva clave

Permite generar una nueva clave. Las pantallas van solicitando la información necesaria.

Siempre se genera una clave de firma. La clave de cifra es opcional.

Es una operación lenta. Dele un tiempo a responder.

MyPGP genera 2 ficheros bajo HOME

- clave pública: email_pub.asc
- clave secreta: email_sec.asc

Aunque MyPGP requiere una contraseña, realmente no se verifica su robustez. Encárguese de usar contraseñas de calidad.

alias

El que genera la clave decide el nombre que aparecerá en ella. Ese nombre no podemos modificarlo los demás. Si deseamos tener otro nombre, podemos asignarle un alias que será el nombre que presente MyPGP.

Seleccione una clave y haga clic en claves / alias.

copiar

Copia el nombre y la huella de la(s) clave(s) seleccionada(s) al portapapeles.

exportar

Genera ficheros con las claves públicas o secretas seleccionadas.

Para las claves públicas, simplemente se genera un fichero X_pub.asc en el directorio seleccionado.

Para las claves secretas, se requiere facilitar la contraseña y se requiere especificar una nueva contraseña. Puede utilizarse para cambiar la contraseña de una clave secreta. Se genera un fichero X_sec.asc en el directorio seleccionado.

Tenga cuidado con el directorio de destino. Si la clave está en el directorio HOME de MyPGP, se cargará en la próxima ejecución. Si la misma clave se carga dos veces con diferentes contraseñas, MyPGP utilizará la última cargada, lo que puede causar una cierta confusión.

refrescar

Carga las claves en HOME.

ficheros y claves

Se presenta una relación de qué claves se cargan de qué fichero. Tenga en cuenta que cuando se cargan llaveros (rings) de otras herramientas PGP, es frecuente que incluyan múltiples claves.

6 Menú listas

añadir clave(s) a lista(s)

Seleccione una o más listas y una o más claves. Todas las claves seleccionadas se añaden a todas las listas seleccionadas.

eliminar clave(s) de lista(s)

Seleccione una o más listas y una o más claves. Todas las claves seleccionadas se eliminan de todas las listas seleccionadas.

nueva lista

Se crea una nueva lista.

eliminar lista(s)

Se elimina una lista. Las claves públicas sólo se eliminan de la lista.

7 Menú portapapeles

Seleccione un texto en alguna pantalla. Páselo al portapapeles (ctrl-C, habitualmente). Opere sobre el portapapeles y pegue el resultado en donde convenga (ctrl-V, habitualmente).

Claves públicas. Se usan para cifrar. Seleccione una o más claves públicas. Puede seleccionarlas:

- una a una, o
- seleccionar una o más listas, o
- seleccionar uno o más [sub-]directorios.

La operación se realiza con todas las claves seleccionadas directa o indirectamente.

Claves secretas. Se usan para firmar. Seleccione una clave secreta.

ver

Se presenta en una ventana el contenido actual del portapapeles.

cifrar

El portapapeles se cifra para todas las claves públicas seleccionadas.

firmar

El portapapeles se firma con la clave secreta.

cifrar y firmar

El portapapeles se firma con la clave secreta seleccionada y se cifra para todas las claves públicas seleccionadas.

descifrar y verificar

El portapapeles incorpora información de si está cifrado y/o firmado. Para verificar la firma, si la hubiera, el usuario no tiene que hacer nada. Para descifrar, es necesario aportar la clave de una de las claves para las que fue cifrado.

8 Menú ficheros

Seleccione uno o más ficheros en el explorador del disco. Las operaciones se realizan sobre los ficheros seleccionados.

Claves públicas. Se usan para cifrar. Seleccione una o más claves públicas. Puede seleccionarlas:

- una a una, o
- seleccionar una o más listas, o
- seleccionar uno o más [sub-]directorios.

La operación se realiza con todas las claves seleccionadas directa o indirectamente.

Claves secretas. Se usan para firmar. Seleccione una clave secreta.

cifrar

El fichero se cifra para todas las claves públicas seleccionadas.

firmar

El fichero se firma con la clave secreta.

cifrar y firmar

El fichero se firma con la clave secreta seleccionada y se cifra para todas las claves públicas seleccionadas.

descifrar y verificar

El fichero incorpora información de si está cifrado y/o firmado. Para verificar la firma, si la hubiera, el usuario no tiene que hacer nada. Para descifrar, es necesario aportar la clave de una de las claves para las que fue cifrado.

borrado seguro

El fichero se elimina de forma segura. Primero se reescribe varias veces combinando 0s y 1s. Luego se elimina del directorio.

9 Menú idioma

Elija el idioma de la interfaz de entre los disponibles.

10 Otros asuntos

10.1 Cifrado Elgamal

El método Elgamal de cifra emplea como clave secreta un valor aleatorio en un grupo cíclico G de orden q con un generador g. Generar estos grupos no es una tarea fácil y puede requerir desde varios minutos hasta varias horas en su versión más perfeccionista. Aunque seguro, puede ser incómodo.

MyPGP ofrece 3 alternativas:

IETF

MyPGP usa alguno de los grupos estandarizados por el IETF en las normas

- RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)

Esta opción es muy rápida. Los grupos son seguros.

Estos grupos están cableados en el código de MyPGP.

bits	fortaleza	grupo DH	RFC
1024	~80	2	4306
1536		5	3526
2048	~112	14	3526
3072	~128	15	3526
4096		16	3526

GnuPG

GnuPG usa varios primos pequeños. La generación del primo seguro recurre al algoritmo de Lim & Lee. Este algoritmo crea un conjunto de primos pequeños y selecciona unos cuantos de ellos para componer un primo probablemente seguro como

$$p = 2 * p_0 * p_1 * ... * p_n + 1$$

A continuación, valida la primalidad de p y permuta el conjunto de primos hasta encontrar un número primo aceptable.

Esta opción es lo bastante rápida como para ser cómoda.

Este algoritmo se implementa en MyPGP, si bien se recurre a Bouncycastle para generar números primos pequeños y para validar si el número es primo.

Estándar

La forma más ortodoxa de generar el grupo es calcular un primo seguro p del tamaño elegido por el usuario. A fin de encontrar p, MyPGP sigue el procedimiento habitual:

1. se elige un número primo al azar, q; se calcula p= 2q+1 y se repite hasta que p es primo.
2. se selecciona un generador g

El paso 1 consume una enormidad de tiempo. El paso 2 es rápido.

La implementación de este algoritmo está en MyPG, copiada de Bouncycastle, e instrumentada para permitir que el usuario pueda cancelar el proceso.

10.2 Curvas elípticas (EC)

MyPGP soporta las siguientes curvas:

bits	NIST FIPS 186-4	SEC	RFC6637
192	P-192	secp192r1	
224	P-224	secp224r1	
256	P-256	secp256r1	must
384	P-384	secp384r1	may
521	P-521	secp521r1	should

Tenga en cuenta que las curvas elípticas sólo la soporta un número limitado de implementaciones de PGP.

10.3 Fortaleza (número de bits)

Fuente: http://www.keylength.com/

	RSA	DSA Elgamal	ECDSA ECDH	clave simétrica	comentario
2010	1024	1024	160	80	debería evitarse
2010-2030	2048	2048	224	112	adecuado para un uso normal
> 2030	3072	3072	256	128	
>> 2030	7680	7680	384	192	a largo plazo
>>> 2030	15360	15360	512	256	