

SIN CLASIFICAR



Manual de uso

CCNDROID CRYPTER



22 de julio de 2015

SIN CLASIFICAR

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1.	INTRODUCCIÓN	4
2.	INSTALACIÓN DE LA APLICACIÓN	4
3.	CONFIGURACIÓN DE LA APLICACIÓN	5
4.	USO DEL EXPLORADOR DE ARCHIVOS	8

1. INTRODUCCIÓN

La aplicación **CCNDROID CRYPTER** es una herramienta desarrollada por el CCN-CERT para el cifrado de ficheros en dispositivos Android. La aplicación soporta algoritmos de cifra simétricos (AES-256-CBC) y asimétricos (PGP, con claves RSA y ELGAMAL).

El manual se ha realizado sobre la versión 5.1.0 (Lollipop) de Android, en inglés (en-US).

2. INSTALACIÓN DE LA APLICACIÓN

Al igual que ocurre con cualquier aplicación de Android que se quiere instalar desde un origen distinto al de la tienda oficial de Android (Google Play), es necesario habilitar la instalación de aplicaciones desde orígenes desconocidos e invocar el instalador ejecutando el APK.

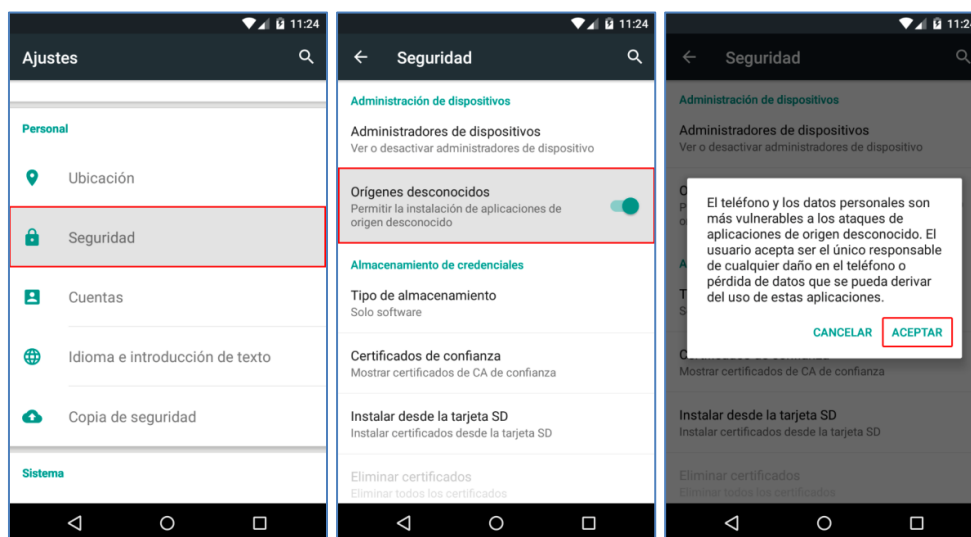


Figura 1. Proceso de instalación

3. CONFIGURACIÓN DE LA APLICACIÓN

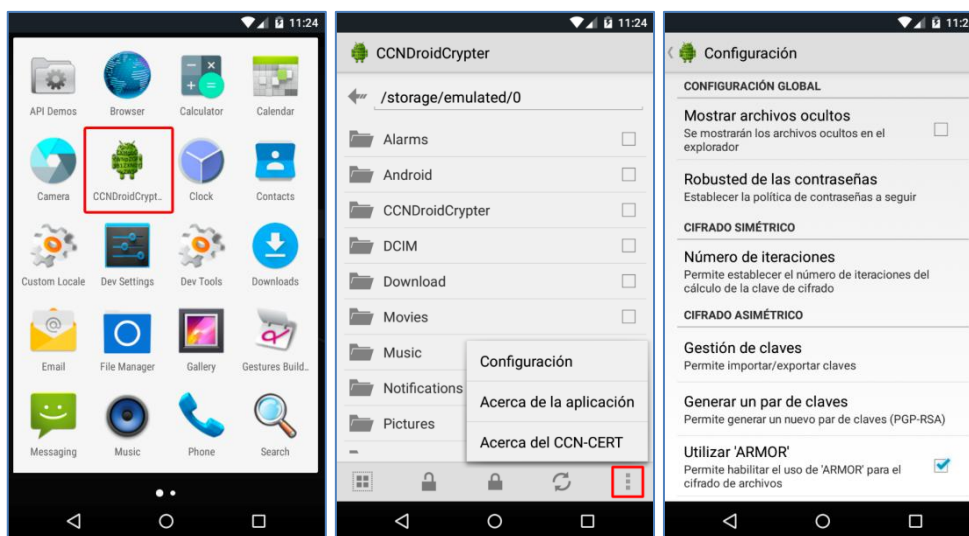


Figura 2. Inicio de la aplicación y pantallas principales

Una vez instalada la aplicación, al iniciarla aparecerá un explorador de archivos. Dentro de las opciones del menú contextual se podrá acceder tanto a una descripción de la aplicación (donde se indica la versión instalada) y del CCN-CERT, como a la configuración de la misma.

La configuración de la aplicación permite:

1. Habilitar la visualización de los archivos ocultos en el explorador interno.
2. Establecer la política de contraseñas que tendrá que cumplir cualquier contraseña que se genere en la aplicación (para el cifrado simétrico o la generación de claves RSA). Permite personalizar la longitud mínima exigida (por defecto son 8 caracteres) y si la contraseña ha de contener números, mayúsculas y/o caracteres especiales (por defecto únicamente requiere que las contraseñas contengan al menos un número).

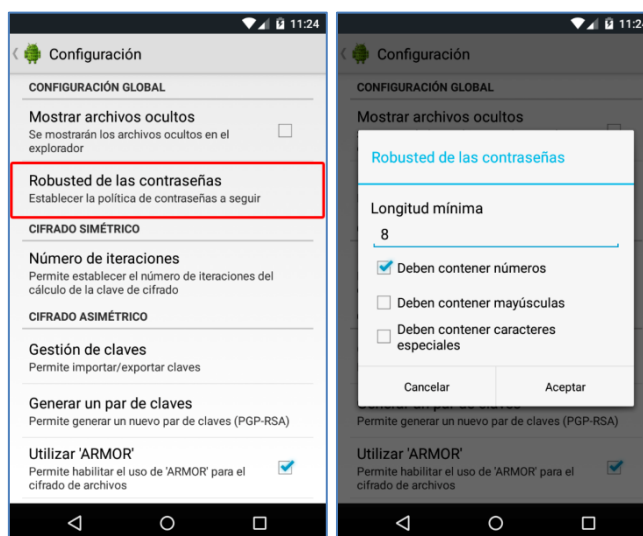


Figura 3. Política de robustez de las contraseñas

3. Establecer el número de iteraciones que se realizarán en el proceso de cálculo de la clave de cifrado. Cuanto mayor sea el valor más tiempo requerirá el proceso de cifrado (el valor por defecto configurado es el mínimo, es decir, 50.000 iteraciones).

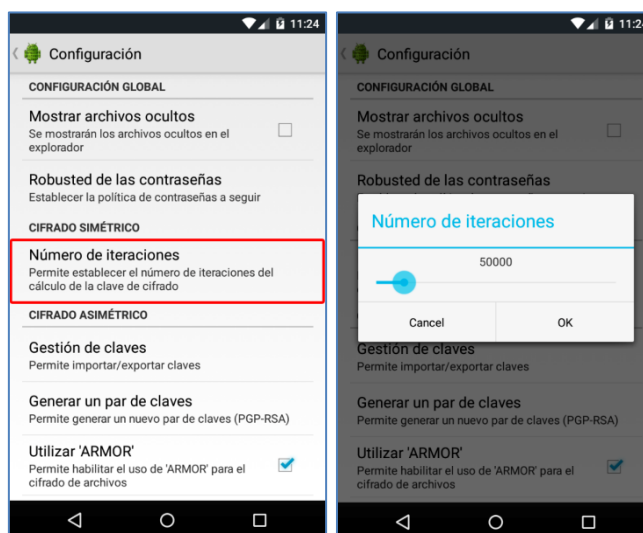


Figura 4. Configuración del número de iteraciones del cálculo de clave (AES)

4. En el panel de gestión de claves es posible visualizar todas las claves PGP importadas (RSA-ELG) o creadas por la aplicación (RSA 4096 bits), apareciendo resaltadas aquellas que sean claves privadas. Además también permite importar nuevas claves y exportar o eliminar alguna de las existentes (pública o privada). Al hacer clic sobre la opción de "importar claves" se abrirá un visor de ficheros para seleccionar las claves a importar.

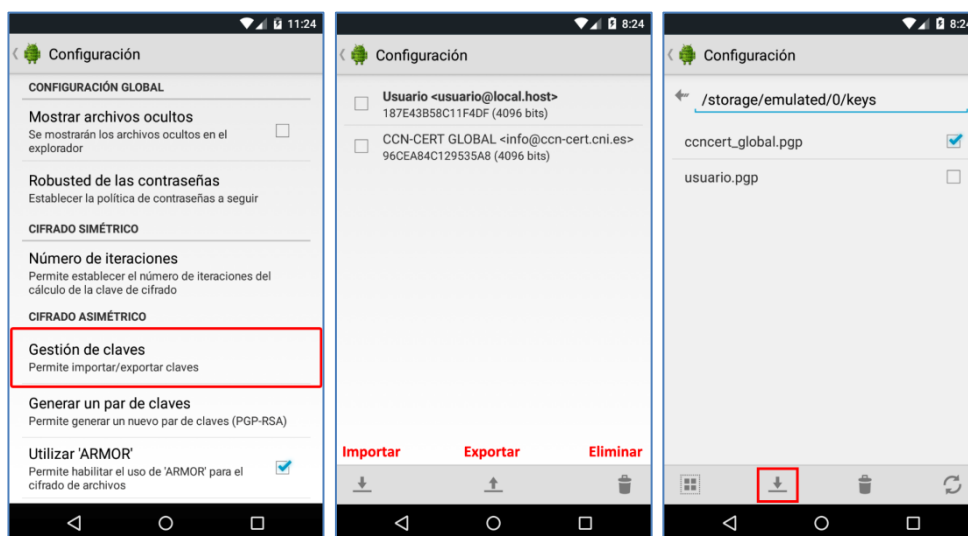


Figura 5. Gestión de claves PGP (importar, exportar, eliminar)

5. En la aplicación es posible la creación de un nuevo par de claves (PGP-RSA-4096). Tanto la identidad (nombre del usuario de la clave) como la contraseña son campos obligatorios mientras que el email asociado es opcional (por norma general también será un dato a cumplimentar). Es posible exportar las claves generadas desde el panel de gestión de claves (punto anterior).
6. Habilitar el uso de la característica "ARMOR" para el cifrado PGP. Durante el proceso de cifrado, si está habilitada esta característica el texto aparecerá con la estructura clásica de PGP (se utiliza el valor estático "GnuPG v2").

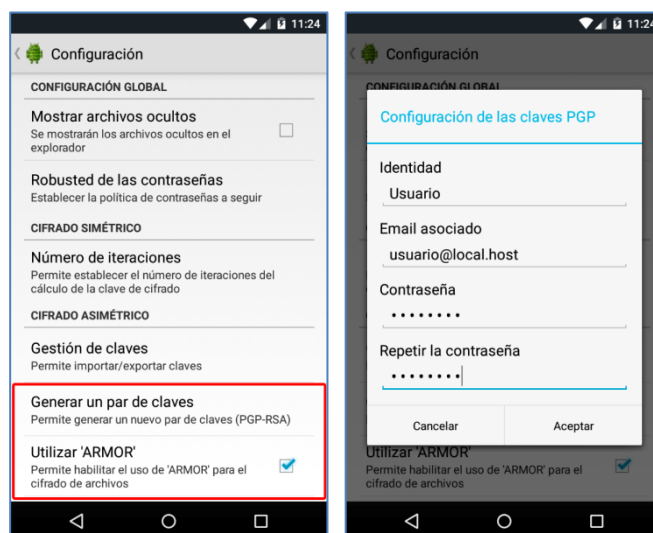


Figura 6. Gestión de claves PGP (importar, exportar, eliminar)

4. USO DEL EXPLORADOR DE ARCHIVOS

El explorador de archivos permite desplazarse por el árbol de directorios del dispositivo (tanto almacenamiento interno como SDCARD) haciendo clic sobre las carpetas o, para ir al directorio anterior, en la flecha localizada en la esquina superior izquierda de la interfaz.

El menú contextual inferior permite seleccionar todos los ficheros y directorios de la carpeta actual, mientras que para seleccionar elementos de forma independiente es necesario hacer clic sobre los ficheros o el selector (carpetas; en caso contrario nos desplazaríamos a dicho directorio en vez de seleccionarlo). El resto de entradas del menú permiten actualizar el contenido del directorio actual (pudiendo editar manualmente la ruta superior para desplazarse a un directorio específico) o iniciar el proceso de cifra.

Si se seleccionan múltiples ficheros, la aplicación generará un ZIP (solicitará el nombre al usuario) y será el contenedor el que se cifre en vez de cada fichero individualmente.

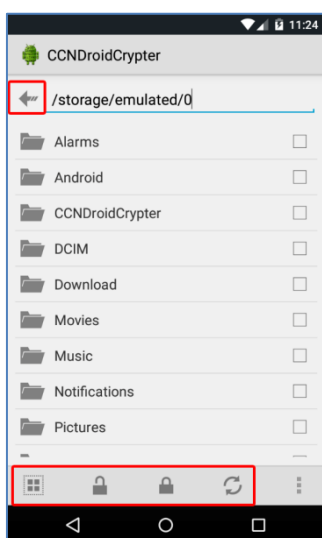


Figura 7. Menú contextual y botón 'atrás'

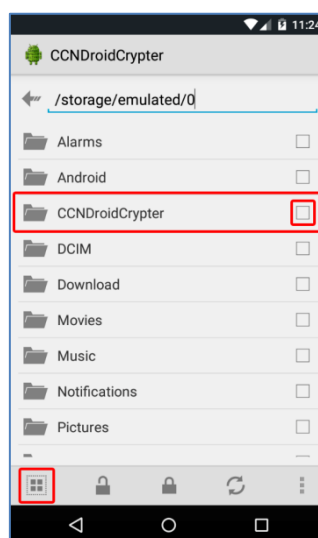


Figura 8. Seleccionar ficheros y directorios

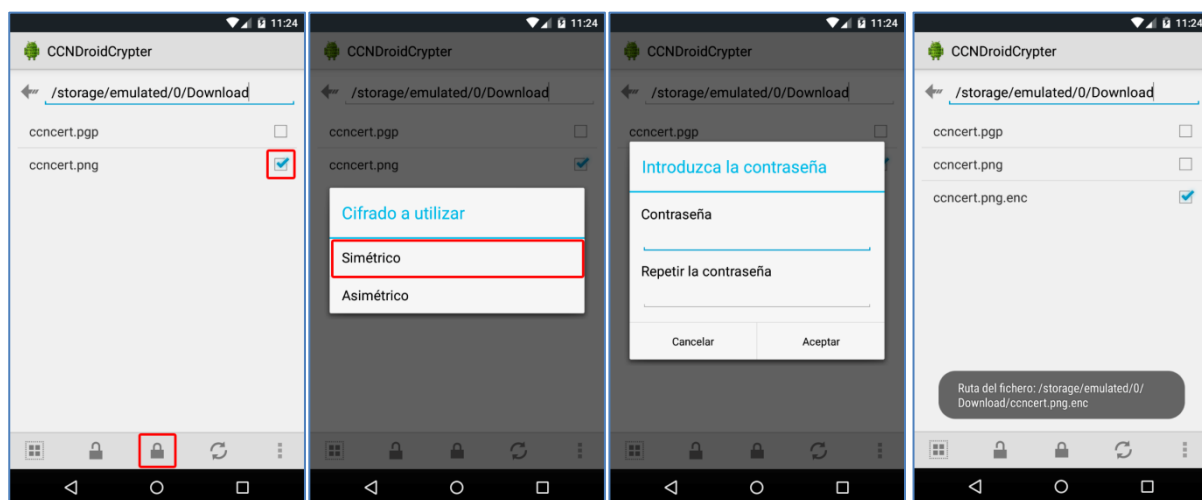


Figura 9. Cifrado AES

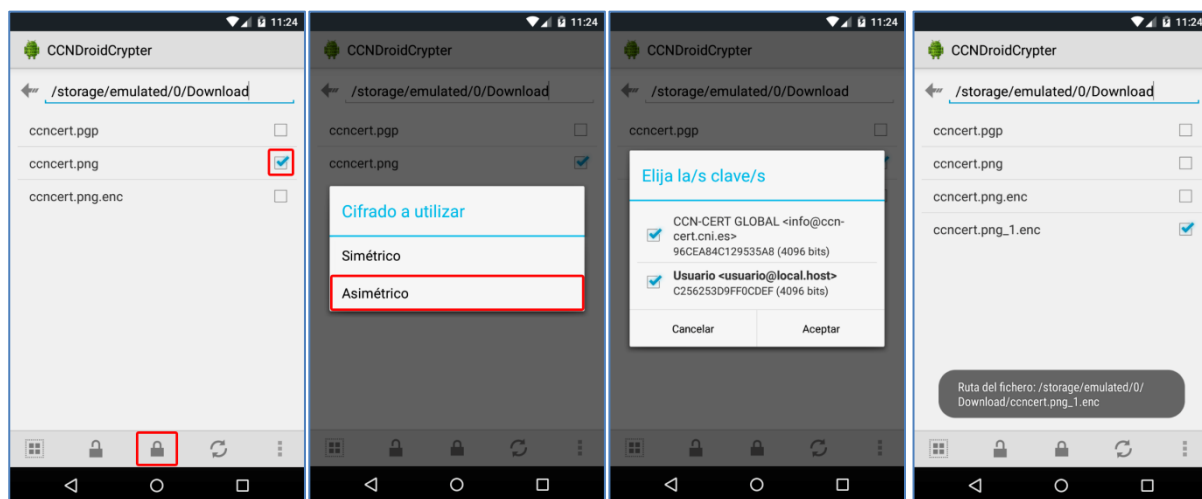


Figura 10. Cifrado PGP

La aplicación es capaz de detectar si un fichero está cifrado con PGP por lo que, en esos casos, el proceso de descifrado no requiere que se indique el tipo de cifrado a utilizar (simétrico o asimétrico, ver paso 2 de la Figura 7 u 8). En ambos casos se solicitará la clave con la que se ha cifrado el fichero (AES) o de la respectiva clave privada (PGP).

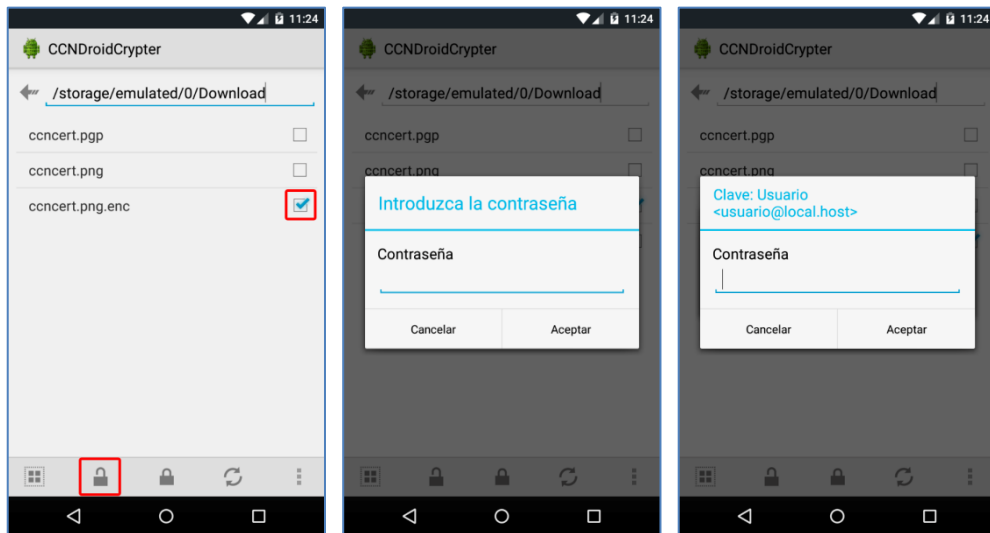


Figura 11. Solicitud de las claves de descifrado (AES & PGP)