

# bluray

## como funciona

pequeñas anotaciones del funcionamiento del sistema de encriptación:

- DECRYPT = MediaKey + VolumeID
- VolumeID = Host Certificate + Private Key
- Media Key = Processing Key

## como se hackea

Al parecer, el soft existente tiene claves no revocadas así:

- VolumeID → MKB v14
- MediaID → MKB v10
- MKB = es la revisión/versión del sistema de criptografía usado en BluRay

A medida que sacan versiones nuevas de MKB van revocando Media Key - porque están «hackeados» o no son de confianza para el sistema.

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/criptografia:bluray>

Last update: **24/11/2012 04:28**

