Facultad de Ciencias de la Universidad
Nacional Autónoma de México

Reporte Sistemas mixtos

Criptografía y Seguridad

Oscar Andrés Rosas Hernandez

19 de noviembre de 2019

0.1. Sistemas mixtos

La criptografía híbrida es un método criptográfico que usa tanto un cifrado simétrico como un asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando su propia clave privada, luego el mensaje cifrado se envía al destinatario. Ya que compartir una clave simétrica no es seguro, ésta es diferente para cada sesión.

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento.

El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

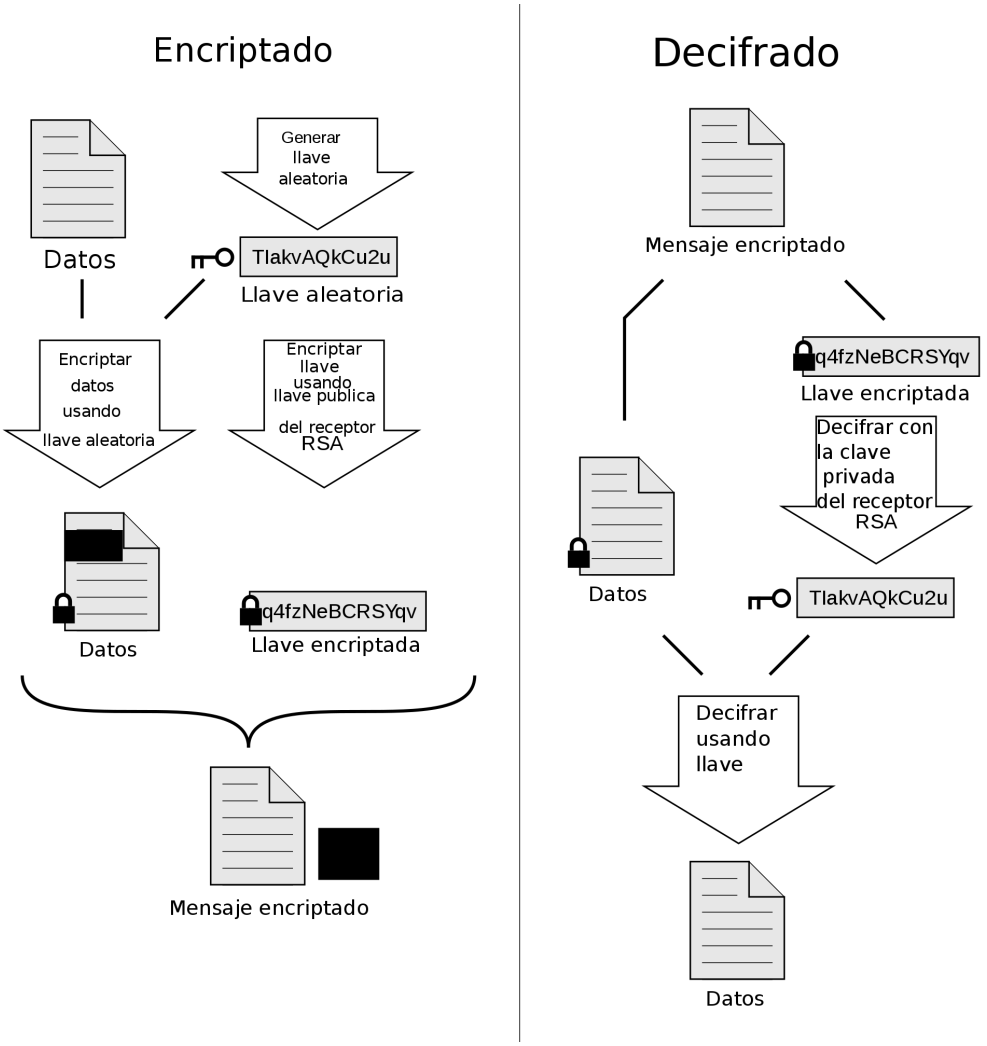
Generar una clave pública y otra privada (en el receptor). Cifrar un archivo de forma síncrona. El receptor nos envía su clave pública. Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor. Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

0.2. Ejemplos de los mismos

Tanto PGP como GnuPG usan sistemas de cifrado híbridos. La clave de sesión (clave simétrica) es cifrada con la clave pública del destinatario, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un solo paquete. El destinatario usa su clave privada para descifrar la clave de sesión (clave simétrica) y acto seguido usa ésta para descifrar el mensaje.

Un sistema de cifrado híbrido no es más fuerte que el de cifrado asimétrico o el de cifrado simétrico de los que hace uso, independientemente de cuál sea más débil. En PGP y GnuPG el sistema de clave simétrica es probablemente la parte más débil de la combinación. Sin embargo, si un atacante pudiera descifrar una clave de sesión, sólo sería útil para poder

leer un mensaje, el cifrado con esa clave de sesión. El atacante tendría que volver a empezar y descifrar otra clave de sesión para poder leer cualquier otro mensaje.



0.3. Firmas digitales

PGP ofrece autenticación de mensajes y la comprobación de su integridad. Esta última es usada para descubrir si un mensaje ha sido cambiado luego de ser completado (la propiedad de integridad del mensaje), y la anterior para determinar si realmente fue enviado por la persona/entidad que reclama ser el remitente (una firma digital). En PGP, estas operaciones son

usadas por defecto junto con la codificación o cifrado del mensaje, pero pueden ser aplicadas a texto simple también. El remitente usa PGP para crear una firma digital para el mensaje con algoritmos de firma RSA o DSA. Para hacer esto, PGP calcula un condensado (también llamado resumen o - en inglés - "hash"del mensaje) del texto simple, y luego crea la firma digital de aquel condensado usando las llaves privadas del remitente.