Encriptación asimétrica vs Encriptación simétrica

Emilio Cabo Gomis

Analiza el significado de clave simétrica y asimétrica.

El mecanismo de encriptación mediante clave simétrica emplea una misma clave para encriptar y des-encriptar los datos.
Debemos compartir la clave mediante un método seguro. Si el mecanismo mediante el que compartimos la clave no es seguro el mensaje puede ser des-encriptado con facilidad.

El mecanismo de encriptación mediante clave asimétrica. Se emplea una clave pública para cifrar los datos y una clave pública para descifrarlos.
Para implementar claves públicas debemos emplear algoritmos que estén diseñados con este propósito. Cómo AES.

Los algoritmos de claves simétricas son mucho más rápidos que los de claves asimétricas.

```
[dave@hal9000 ~]$ openssl speed aes-128-cbc
Doing aes-128 cbc for 3s on 16 size blocks: 26126940 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 64 size blocks: 7160075 aes-128 cbc's in 3.00s
...
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
aes-128 cbc     139343.68k   152748.27k   155215.70k   155745.61k   157196.29k
```

```
[dave@hal9000 ~]$ openssl speed rsa2048
Doing 2048 bit private rsa's for 10s: 9267 2048 bit private RSA's in 9.99s
Doing 2048 bit public rsa's for 10s: 299665 2048 bit public RSA's in 9.99s
...
                  sign    verify    sign/s verify/s
rsa 2048 bits 0.001078s 0.000033s    927.6  29996.5
```

¿Podrías poner algunos ejemplos dónde se disponga típicamente claves simétricas y asimétricas?

Los algoritmos de claves simétricas los empleamos cuándo encriptamos los archivos contenidos en un disco duro.

Los algoritmos de claves asimétricas se emplean en servicios como SSH. En el que tenemos que compartir una clave pública con el cliente.

¿Cómo es que siendo una clave pública en el cifrado asimétrico es más seguro que el cifrado simétrico?

La encriptación mediante algoritmos asimétricos no es inherentemente más segura que la encriptación mediante algoritmos simétricos.
El problema de los algoritmos simétricos es que en el proceso de compartir la clave privada esta se vea vulnerada. Este problema no lo tiene
Pero pongamos que encriptamos un disco y no tenemos que compartir la clave con nadie.
Esta encriptación es tan segura cómo el número de bits que se emplee para encriptar.

Bibliografía

What is the performance difference of pki to symmetric encryption? - Stack Overflow

Cifrado simétrico vs. asimétrico: ¿cuál es la diferencia? (mailfence.com)

Criptografía: Algoritmos de clave simétrico y asimétrico explicados (redeszone.net)

What is asymmetric encryption? | Asymmetric vs. symmetric encryption | Cloudflare