Speaker 1 (00 03)

Bienvenidos a esta nueva sesión en la cual vamos a trabajar algunos conceptos nuevos sobre criptografía simétrica y criptografía asimétrica.

Además en esta sesión podremos ver de forma teórica algún ejemplo del uso de herramientas GPG.

Más adelante en otra sesión veremos también un uso práctico de esta herramienta.

Lo que vamos a ver en esta sesión son los tipos de criptografía.

Vamos a recordar rápidamente lo que hay simétrico y qué hay simétrico.

Hablaremos de la criptografía simétrica, hablaremos ya desde dentro de este concepto, hablaremos también de la criptografía simétrica y también dentro de este concepto además hablaremos de algunos tipos de algoritmos enfocados a la parte criptográfica tanto en en el mundo de la criptografía simétrica como en la asimétrica.

Además veremos algunos tipos de operaciones, algún resumen de conceptos y también hablaremos de la herramienta GPG con la cual podremos realizar diferentes operaciones criptográficas de manera sencilla a través de la línea de comandos.

Existen gran cantidad de interfaces gráficas que por encima de GPG proporcionan un entorno un poco más amigable y que también en su determinado momento podríamos estudiar.

Empezamos hablando de la criptografía simétrica a modo de resumen porque esto lo hemos visto en la sesión anterior.

Cuando hablamos de criptografía principalmente hablamos de dos tipos.

Tenemos dos tipos que es la criptografía simétrica y la criptografía asimétrica.

Es importante conocer las diferencias.

Hay muchas diferencias en este tipo de criptografía pero el fin común es el mismo que es la protección de la información tanto en almacenamiento como en tránsito.

La información como digo puede estar almacenada o puede ser protegida, mejor dicho en

almacenamiento o en tránsito o en camino.

Recordamos rápidamente que en almacenamiento es cuando la información está en un disco duro, en una memoria RAM, está almacenada en un sistema 1 base de datos y debe ser protegida para que los usuarios que no están autorizados no puedan visualizarla.

En el caso de proteger la información que se encuentra en tránsito o en camino nos referimos a cuando un dispositivo envía información a través de un canal, ese canal debe estar protegido para evitar que alguien, por ejemplo haciendo ataques de buying, de middle, pueda visualizar esa información.

Bien, cuando hablamos de criptografía de cifrado simétrico nos estamos refiriendo cuando un usuario va a proteger la información con la misma clave con la que después va a poder desprotegerla o descifrarla.

Es decir, la acción de cifrar la información se realiza con una clave y esa misma clave se va a utilizar para realizar el descifrado, es decir, para poder acceder a la información.

La criptografía simétrica nos pone en juego dos conceptos muy importantes en el mundo criptográfico que son el concepto de clave y el concepto de algoritmo.

La clave de cifrado, lógicamente debe ser robusta, debe ser una clave que sea potente y recae sobre ella la seguridad del cifrado.

Se utiliza para transformar algo que es legible, algo que es una información que se puede leer, en algo que no es legible, que va a estar protegido.

Además, con esa misma clave se puede hacer el camino inverso, es decir, podemos obtener de algo que no es legible, descifrarlo y poder convertirlo en información legible.

Cuando hablamos de información legible nos referimos a texto, pero también nos referimos, por ejemplo, a un binario.

Un binario puede estar cifrado y entonces ese binario lógicamente no va a funcionar en el momento que lo desciframos.

El binario pasaría a funcionar sobre el sistema.

El segundo concepto que vemos aquí es el concepto de algoritmo.

Es el paso a paso matemático que realiza el sistema para proteger la información o para acceder a ella.

Así que hay diferentes tipos de algoritmos, algunos los veremos después a modo de ejemplo.

Bien, vamos a pasar al siguiente slide.

Aquí vamos a proponer un ejemplo.

En el siguiente ejemplo tenemos un usuario que va a disponer de una clave de cifrado.

Entendemos que estamos en el concepto de clave cifrado simétrica.

El usuario toma la información, esa información la vemos simbolizada a través de un sobre y lo que hace es cifrar esa información.

Lo que está haciendo es poner una especie de candado.

Nadie puede abrir el sobre, nadie puede ver el contenido de esa carta.

En este ejemplo la información queda protegida y nadie va a poder ver lo que hay dentro del sobre.

Pero esa persona, ese usuario, tiene una clave con la cual puede descifrar, es decir, abrir el candado y poder visualizar lo que hay dentro.

Es decir, se cifrará, se protegerá el sobre con la misma clave que con la que se va a descifrar.

Es decir, cerramos con la misma llave con la que vamos a abrir.

Bien, ahora vamos a trabajar el concepto de la criptografía asimétrica.

La criptografía asimétrica permite que un usuario pueda proteger, el uso principal es el del canal de comunicación, pero puede proteger un canal de comunicación, puede proteger también información que está almacenada.

Se puede utilizar para diferentes cosas.

Es verdad que la criptografía simétrica es una criptografía más lenta que la criptografía

simétrica, eso también tenemos que tenerlo en cuenta.

La fuerza de la criptografía asimétrica es que disponemos de dos claves.

Este es el concepto de las dos clave pública y clave privada.

La clave a por ejemplo, la clave pública va a permitir a un usuario cifrar la información, es decir, proteger la información, pero no va a poder utilizar la clave pública para poder descifrarlo.

Sin embargo tiene que tener una segunda clave que es la clave privada, con esa clave con la que vamos a poder descifrar la información.

Entonces si recapitulamos en el concepto de la criptografía asimétrica, tenemos una clave que nos permite proteger la información y tenemos una segunda clave que nos permite abrir, desproteger, desbloquear, descifrar esa información.

Realmente el tipo de la criptografía simétrica lo que viene es a darnos una solución al problema de distribución de clave.

¿En la criptografía existe un problema que es cómo hago yo para que entre dos máquinas distribuyamos una clave simétrica y podamos utilizar un canal seguro?

Tenemos un problema, es decir, si tenemos dos máquinas y esas máquinas sólo pueden hablarse por un canal no seguro, es decir, un canal que no está protegido, quieren intercambiarse una clave, en este caso simétrica, para poder proteger el canal, pero o conocen la clave antes o no van a poder enviarlo a través de un canal no seguro.

Gracias a la criptografía asimétrica se puede solventar este problema.

El problema de distribución de la clave puede ser solucionado con este tipo de criptografía porque podemos utilizar la clave pública de un extremo para cifrar cierta información y en el otro extremo con la clave contraria, con la clave privada, podemos resolver o descifrar esos datos y poder obtener por ejemplo una clave simétrica.

Esto lo vamos a explicar un poco mejor con algún ejemplo.

Para entenderlo mejor nos venimos a este ejemplo y por ejemplo la conexión HTTPs.

Tenemos un navegador, conectamos contra un servidor HTTPs, un servidor web, el navegador obtiene un certificado, nos conectamos a un servidor, el servidor está por HTTPs, el servidor nos da su certificado, en ese certificado nos vamos a encontrar una clave, con esa clave el navegador puede cifrar la comunicación, el navegador puede cifrar la comunicación con el servidor, el servidor dispone de la otra clave que es la clave contraria, es decir, el servidor en el certificado nos está proporcionando una clave pública. Nosotros como navegador ciframos la comunicación en esa clave pública y el servidor en el extremo, en la clave privada también, porque es su clave privada, él la proporciona su clave pública y ahora está utilizando su clave privada para descifrar lo que el navegador está enviando.

En este instante tenemos un mecanismo para poder enviarnos la información y a partir de aquí podemos generar una clave simétrica utilizando este mecanismo para protegerla y hacer llegar la clave simétrica a los dos extremos.

Puede ser el servidor que la genere puede ser el cliente el que la genere.

De esa forma a partir de entonces la comunicación ya va cifrada con clave simétrica que es más rápido y gracias a la clave asimétrica, al mecanismo de clave asimétrica hemos podido hacer ese intercambio de claves de forma segura.

Es un buen ejemplo porque al final es un buen ejemplo de uso y espero que se entienda.

Vamos a pasar ahora al tema del apartado de los algoritmos.

Aquí hay algunos ejemplos de algoritmos de criptografía simétrica.

He puesto alguno, he puesto Des, he puesto AES.

AES hoy en día 128 bits, es un poco el estándar, es el algoritmo quizás más estandarizado, pero bueno, aparte de Des, AES tenemos idea, tenemos blowfish, hay diferentes algoritmos de criptografía simétrica.

También tenemos aquí algunos algoritmos de criptografía simétrica, puede ser que haya en algunos casos menos cantidad pero pero que son muy importantes, como habéis visto,

son totalmente complementarios.

La criptografía de clave simétrica es importante, la criptografía de clave simétrica es importante y son totalmente complementarias y se pueden utilizar en algunos casos para lo mismo y en algunos casos se complementan para poder, en el problema de la distribución de claves que hemos visto anteriormente, para poder distribuir por ejemplo la clave simétrica.

Bien, aquí tenéis algunos ejemplos, algoritmos y ahora vamos a pasar al apartado de operaciones.

Vamos a hacer un breve resumen de estas dos sesiones de conceptos que hemos ido trabajando.

El cifrado, ya sabemos, hemos visto varias veces que el cifrado es el proceso por el que un usuario convierte un texto, una información legible o binario, o un binario, un ejecutable, una imagen, lo que sea, en algo que no es legible o no entendible o no puede ser ejecutado porque el sistema no lo puede entender.

Entonces podemos decir que es la acción que nos va a permitir proteger la información antes de ser almacenada o antes de ser enviada por un canal no seguro.

El descifrado es la acción contraria por la que un usuario anula la acción descifrado, es decir, desbloquea o descifra, mejor dicho, el contenido.

Entonces digamos que el cifrado es la acción contraria al cifrado.

Como digo, vamos a pasar al siguiente slide.

El descifrado aquí está explicado, como comenta antes, vamos a pasar a la siguiente.

Bien, la clave de cifrado es el elemento utilizado para cifrar matemáticamente una información, es decir, de forma que la información quede protegida.