Criptografía

Transcribed on July 7, 2025 at 12:13 PM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión donde vamos a trabajar concepto de la criptografía.

Sabemos que la criptografía es una de las bases de la seguridad de la información porque nos permite o nos va a permitir proteger la información en diferentes ámbitos como iremos viendo durante esta sesión.

A continuación vamos a ver cuál es la agenda que tenemos para esta sesión.

Primero hablaremos un poco de la introducción a la criptografía, hablaremos un poco de su importancia, hablaremos de lo que es, por qué es importante esto de la criptografía y hablaremos también sobre los conceptos básicos antes de próximas sesiones empezar a trabajar de manera práctica sobre los diferentes conceptos que debemos cumplir en este módulo.

La criptografía final es el estudio, podemos verlo como el estudio para proteger la información.

El objetivo va a ser proteger la información para que alguien no pueda visualizarla.

Al final lo que vamos a aplicar son técnicas que van a permitir convertir algo o información que es legible en información que no es legible o es ilegible.

De esta manera estamos protegiendo esa información.

Lo ilegible o lo que no podemos leer debe ser legible en algún momento, es decir, tenemos que tener mecanismos para poder proteger y desproteger esa información en un momento determinado para poder consumir la información.

Al final.

También podemos decir que la criptografía permite traducir algo que es legible o algo que se puede leer en algo que es ilegible o que no podemos leer, pero el camino inverso también nos lo debe proporcionar la criptografía.

Podemos entender también que la criptografía, como he comentado antes, es una de las bases de la ciberseguridad, es algo bastante importante donde sin la criptografía no podríamos proteger, no podríamos asegurar, no podríamos hacer segura la información, ya sea tanto en almacenamiento de esa información como en el tránsito de información cuando viaja por la red, lo que no tendríamos esos mecanismos que nos permiten garantizar la confidencialidad o la integridad de la información.

Es verdad que aquí no hablamos de disponibilidad, recordad que la triada de la seguridad de información sería la confidencialidad, la disponibilidad y la integridad, pero aquí la criptografía la metemos justamente aplicándola sobre la confidencialidad y la integridad de la información.

Además, recordemos que los objetivos, como he comentado, de la ciberseguridad son estos confidencialidad, integridad, disponibilidad información.

Y lógicamente tiene un papel crucial un mapeo directo entre dos de estas tres dimensiones de acción seguria.

En el caso de la criptografía, fijaros en el acto de pasar de algo, de una información que es legible, una información que está en texto plano, a un formato no legible o en un formato que no podemos leer.

Algo que está cifrado.

Eso es precisamente lo que es la criptografía o el cifrado.

El paso contrario al cifrado es el desquizado, es convertir algo que no es legible en algo que podamos consumir, algo que podamos leer, algo que podamos entender como seres humanos, es decir, desproteger esa información.

Al final también podemos decir que la criptografía es el arte con el cual vamos a poder proteger la información.

A través de diferentes técnicas que iremos trabajando en este proceso, la información la vamos a transformar en algo que no vamos a poder leer como seres humanos y que además no debería ser posible entender, porque muchas veces podemos equivocarnos y pensar que la codificación de una serie de caracteres puede ser criptografía y no lo es.

¿Es decir, o luego también podemos decir, bueno, y la ocultación de la información puede ser criptografía?

No lo es, puede ser esta, pero no criptografía.

La criptografía al final son los procedimientos, las técnicas que utilizamos para convertir algo que es legible en algo que no lo va a ser.

Y ya no sea porque esté oculto o ya no sea porque no esté oculto.

¿Bien, por qué es?

Bueno, para acabar esta fase de definición de lo que es la criptografía, también podemos decir que la información va a estar protegida cuando nadie pueda entender lo que está enviando.

También podemos pensar en el almacenamiento, cuando alguien pueda no pueda visualizarlo, porque lo que está en el disco duro está cifrado, por lo que está en memoria está cifrado, por lo que se está transmitiendo a través de la red, este cifrado.

Es decir, si alguien se pone en medio de comunicación, de repente puede visualizar o consumir esa información, pero la información que está llegando porque está en medio del canal está cifrada, por lo cual no puede visualizarlo.

O incluso lo que nos están contando, lo que está contando está cifrado, lo que estamos escuchando no vamos a poder entenderlo.

Entonces, la criptografía es realmente importante, como se puede ver, es una de las bases fundamentales para sentirnos seguros.

Es verdad que a futuro podemos entender que puede haber un problema con la cuántica, con el quantum, ya existen algoritmos criptográficos preparados, post cuánticos que se llaman, pero es verdad que es un reto y es algo también importante a tener en cuenta.

¿Por qué es importante?

¿Por qué es importante la criptografía?

Bueno, yo creo que a estas alturas ya de la sesión entendemos por qué es importante, pero bueno, la información es importante para todos.

La información es uno de los activos más importantes de la organización, debemos protegerlo y abordarse.

Uno de los activos que me permite generar esa actividad de información.

Podemos decir que nuestra información debe ser protegida.

Correcto, sencillo de entender y además existen muchos sitios donde se transmite y se almacena esta información.

Por eso es importante, porque al final tenemos una gran cantidad de sitios en las organizaciones donde tenemos información, tenemos incluso modelos de cloud, tenemos información en el cloud que también debemos proteger, no sólo porque el proveedor de cloud nos pueda decir oye yo protejo la información, sino que nosotros también podemos tener mecanismos extra para proteger nuestra información.

Y luego también el canal es muy importante el canal por el que se transmite la información, que sea un canal seguro.

El concepto de vpn, el concepto de ips, diferentes conceptos, HTTPs, ssh, hay diferentes protocolos y diferentes soluciones para proteger la información, dependiendo un poco también de las necesidades en cada momento.

Lógicamente si montamos un servidor web y debemos hacer que la comunicación esté protegida, nos va a valer con HTTPs, utilizando certificados, necesitamos que una o que una serie de empleados de una empresa se conecten remotamente a recursos internos de la organización, necesitaremos montar una VPN, al final son túneles criptográficos, utilizamos criptografía para proteger esos canales y que la información vaya protegida.

¿Nos tenemos que preguntar dónde tenemos nosotros y dónde transmitimos nuestra información?

Una buena pregunta que que habrá que saber responderse dentro de las organizaciones, tener controlado todo esto.

Bien, vamos a comenzar un poco con conceptos básicos, con la parte de conceptos básicos.

Vamos a empezar por la parte de historia.

Bueno, pues en el año 4000 a.

C.

Los egipcios estaban con jeroglíficos y al final esos jeroglíficos se puede entender como eran elementos criptográficos o podían llegar a ser elementos criptográficos, estaban ahí.

Es verdad que muchas veces no se considera hasta la llegada de Roma, el cifrado César o el cifrado Roth, consiste en rotar, como veremos después, hasta que no llegó este tipo de elementos no se considera un poco el nacimiento de la criptografía, a veces que se considera un poco antes con jeroglíficos, bueno, dependiendo un poco las lecturas que hagamos pues se puede encontrar una serie de cosas u otras.

Después fijaros que siguiente hito, hay muchos más hitos entre medias, pero relevante que he puesto es el del renacimiento en Francia, estamos hablando ya de siglos muy cercanos a los nuestros, donde Blaise de Vigne realizó un trabajo y ahí también estaba sus sus técnicas que son importantes en aquella época de un cifrado que todavía no es un cifrado moderno, no es un cifrado comparable a lo de ahora, pero bueno, se puede ver la evolución y la importancia que el ser humano le ha dado a poder ocultar o hacer no legible la información, incluso aunque caiga en manos tuyas, que tú no puedas tener los mecanismos para poder entender qué es lo que estás leyendo.

Y bueno, pues la importancia se ve incluso hasta en el Renacimiento.

Luego aparecen los trabajos de Cloud Shannon, esos trabajos de Cloudsanon, donde hablaron ya de la modernización de las técnicas de cifrado, se transforman los procesos en matemáticas avanzadas.

Aquí es un paso importante porque ya estamos hablando de metemos una matemática avanzada, hacemos que estos procesos sean más complejos en muchos casos y dándole esa robustez.

Es verdad que en el caso de Villiner, en la Francia del Renacimiento, sí que hablaban ya de robustez en los códigos de cifrado, pero no teníamos esos procesos matemáticos avanzados todavía porque no estábamos en esos momentos.

Si miráis en otras fuentes de información, veréis que la historia tiene muchísimos hitos dentro de la criptografía.

Yo os he dejado estos cuatro porque para mí son bastante relevantes de la importancia que el ser humano le ha dado siempre a proteger su información, pero sobre todo el último, con los trabajos que la abre y luego a la llegada de RSA posteriormente, etc.

Abre la caja de Pandora realmente abre toda esa fuente de investigaciones y de trabajos cristográficos que llegaron después y hasta llegar a la criptografía que tenemos hoy en día, incluso a la criptografía que es la que nos aborda ya en la realidad de manera inmediata.

Bueno, como objetivos, podemos decir que la criptografía tiene varios objetivos.

Esos objetivos pueden ser agrupados en dos grupos principalmente están orientados a la protección de la información y hay otro grupo que está orientado más a la verificación de los usuarios, a poder validar o identificar o hacer el no repudio, por así decirlo, de lo que el usuario ha escrito o comenta.

En el caso de lo que hablamos de la protección de la información, encontramos los siguientes objetivos.

El objetivo de proteger la información, ya lo hemos comentado anteriormente, es la confidencialidad y la integridad.

La confidencialidad podemos decir que son las protecciones que se utilizan para que la información deje de ser legible.

Lo hemos comentado ya varias veces en la sesión de hoy.

Pero además, solamente los usuarios con la capacidad criptográfica para desproteger, para hacer legible otra vez esa información que dejó de serlo, pueden acceder a esa información.

Ese es el objetivo de la confidencialidad.

En el caso de la integridad, es una manera de proteger la información también, pero para ser capaz de verificar que la información no ha sido manipulada, no ha sido modificada.

Es decir, tenemos mecanismos criptográficos que nos permiten validar que la información no ha sido manipulada, ni en tránsito ni en el propio almacenamiento de esa información.

Por ejemplo, en un email, cuando enviamos un email, tenemos mecanismos para saber que ese email, por ejemplo, está firmado y si alguien modificase ese email 1,1 punto o cualquier cosa, nos podríamos dar cuenta de que el mensaje ha sido modificado.

Por ejemplo, con la firma digital se podría validar este tipo de información o con algún tipo de hash también se podría hacer.

En el caso de la verificación de los usuarios encontraremos más objetivos, también tenemos otro tipo de objetivos diferentes a la confidencialidad y a la integridad, pero aquí hablamos, por ejemplo, el no repudio y la autenticidad.

Cuando hablamos de no repudio en esta verificación de los usuarios son que tenemos mecanismos criptográficos que nos permiten validar que un usuario ha realizado una acción o ha hecho algo que no puede rechazar, es decir, ha realizado algo que no podrás decir que no lo has hecho porque está criptográficamente comprobado.

En el caso de autenticidad son los mecanismos criptográficos que se utilizan para verificar que un usuario es quien dice ser.

Por ejemplo, en la identidad, por ejemplo, cuando nos autenticamos contra una entidad, por ejemplo, gubernamental, a través de un certificado ellos pueden validar que nosotros somos esa persona.

Bien, pues esta slide yo creo que es bastante importante porque porque nos da a entender un poco los conceptos básicos y la importancia de la criptografía en sus objetivos.

Bueno, tenemos ahora vamos a hablar dentro de los conceptos básicos metido, quería enseñaros un algoritmo clásico muy sencillo de criptografía que los niños pequeños de siete, ocho, nueve, 10 años pueden utilizar incluso en sus colegios, etc.

Para proteger su información de manera muy sencilla y es el llamado método del César.

¿Esto en qué consiste?

Consiste en rotar n posiciones las letras y aplicar una operación modular sobre el conjunto de las letras.

Vamos a ver un poco un ejemplo, el proceso de cifrado.

Por ejemplo, tenemos la frase Hello, queremos protegerla.

Lo que vamos a hacer es, bueno, si yo tengo el alfabeto a, b, c, d, e, f, g, h, i, j, k, hasta llegar a la z, lo que hago es aplicarle una constante que vamos a llamarlo rot y decimos bueno, mi constante va a ser de cinco.

Claro, esa va a ser mi clave.

Es una clave que me permite rotar las posiciones de las letras cinco posiciones hacia delante.

Lo que ocurre es que, por otro lado, el que reciba el mensaje que no va a ser hello, ahora veremos qué mensaje recibiría, tendrá que hacer la operación inversa, que es restar cinco posiciones a esas letras para recuperar el mensaje.

¿Qué ocurre si, por ejemplo, mi mensaje tuviera la letra z?

La letra z es la posición 26 del alfabeto.

Lo que ocurre es que si sumo cinco seríamos z, la a sería la primera, b, c, d, e, teníamos la e, habíamos dado la vuelta, por eso decimos que es una operación modular, matemáticas discretas.

Entonces, fijaros, sobre el primer carácter, ahí se puede ver, primer carácter h, le sumamos cinco posiciones y obtenemos la m.

Es f g, h i, jklm, cinco posiciones con la e, la j, con la e, pues la l, la q, con la l, la q y con la t, perdón, con la o, la t.

Entonces el mensaje cifrado sería MJQ.

Si tú no conoces cuál es la constante que hay que rotar, desplazar, ya sea hacia adelante o hacia atrás las letras, tenemos un problema, porque claro, al final no tenemos el mecanismo para poder saber qué es lo que están poniendo en esta clase.

Es verdad que hoy en día son algoritmos que no tienen ningún sentido, fácilmente rompibles, muy muy fácilmente rompibles con un criptoanálisis muy básico.

Vamos a ver cómo funcionaba el proceso contrario.

Proceso contrario, el descifrado, el encrypt process, no el decrypt process.

Tenemos la frase mjqt y aplicamos la constante rot y le restamos cinco posiciones.

Entonces fijaos, la m, vamos cinco posiciones atrás y vamos recuperando.

Ahí tenéis una pequeña aplicación que se ha montado ahí en python, donde le pasas una palabra, te hace la rotación, en este caso el rot cinco, la constante cinco y tiene la frase cifrada y la frase sin cifrar.

Si hubiese letras que están hacia el final del alfabeto, no habría problema porque haríamos una operación modular y apareceríamos por el principio del alfabeto.

Al final.

Es como que el alfabeto fuera circular y pudiéramos ir recorriendolo desde el final, llegaríamos al principio.

Bueno, más cosas.

Bueno, la criptografía tiene dos tipos de claves, principalmente tiene dos tipos de claves, los tipos de hacer los cifrados y los descifrados.

Tenemos la forma simétrica y la forma asimétrica.

Esto lo vamos a estudiar en otra sesión en mayor profundidad, pero es muy sencillo.

Al final es importante entender la diferencia entre ambos tipos, ya que al final son diferentes, aunque tienen el mismo objetivo que es proteger la información, aunque también pueden tener otro tipo de usos como se verán más adelante.

Como digo, la información puede ser protegida en diversos modos.

El almacenamiento, cuando la información se encuentra almacenada en disco duro, en memoria, puede estar protegida por cifrado para que los usuarios autorizados no puedan acceder a esa información.

Un ejemplo en disco un buildlocker, un trucrite, firewall, diferentes herramientas criptográficas para proteger particiones, discos duros o incluso GPG.

Por ejemplo, para cifrar carpeta, ficheros EFs en Cred File System de Windows para hacer lo mismo, cifrar carpetas cifrar archivos, podemos hablar de un cifrado de disco, un cifrado de partición o un cifrado a nivel ya de 1 s nivel, que sería un cifrado a nivel de directorio o de archivo.

Y luego tenemos la partición en camino, que hemos hablado ya de ello.

Al final es cuando la información es enviada de un dispositivo a otro.

En ese tránsito, la utilización de protocolos que crean esos túneles criptográficos lógicamente son interesantes en función del ámbito o en función de lo que necesitemos.

Eso lo hemos comentado antes con el ejemplo del servidor web y con el ejemplo de la VPN.

¿Cuándo estamos ante un algoritmo de cifrado seguro?

Es una pregunta que nos tenemos que hacer y que nos hacemos.

¿Cuándo estamos ante un algoritmo de cifrado?

¿Un algoritmo de cifrado seguro?

Bueno, deben cumplir una serie de características.

La primera es que el algoritmo debe ser robusto.

Saber cómo se cifran los elementos no debe ser un problema, es decir, que se sepa cómo funciona el algoritmo no debe ser un problema para garantizar la protección de esa información, por lo cual evitaríamos la seguridad por oscuridad.

Si tengo que proteger cómo funciona el algoritmo, su seguridad por oscuridad y eso significa un mal mecanismo.

Los algoritmos estándar son públicos, la gente puede ver que la matemática está detrás y que al final son procesos complejos matemáticos y sabes cómo funciona el algoritmo, pero no es capaz porque la operación es computacionalmente muy compleja.

La robustez debe consistir en la complejidad matemática.

Es un poco lo que acabamos de comentar.

Un algoritmo de cifrado seguro es cuando se ha cifrado seguro, cuando tardaríamos muchos años en poder descifrarlo, tardaríamos muchísimos años más que en nuestra vida.

Entonces ahí podemos decir bueno, pues el algoritmo es seguro.

Cuando pierde esa nomenclatura, este algoritmo se puede romper en un tiempo asumible.

Entonces esa seguridad del algoritmo, esa robustez se va perdiendo y es lógico con la evolución, la evolución tecnológica, la disrupción ahora del post quantum, todo esto pues lógicamente, o en quantum mejor dicho, todo esto tiene unas implicaciones que afecta lógicamente a la parte de robustez.

Bien, pues llegamos al final de la sesión y lo que hemos estado viendo son los conceptos básicos de criptografía.

Hemos empezado a ver pinceladas.

Primero, por qué es importante la criptografía, hemos estado viendo lo que hay que proteger realmente, hemos estado viendo lo que es la criptografía simétrica y la criptografía asimétrica.

La criptografía asimétrica se utiliza una clave para cifrar y descifrar y en el caso de la simétrica se utiliza una clave para cifrar y otra clave para descifrar.

Un poco el resumen de lo que hemos estado viendo, hemos estado viendo un ejemplo de uso del algoritmo César, muy sencillo.

Luego ha habido evoluciones, el algoritmo de Villenet, o sea, diferentes evoluciones, pero todas hoy en día son simplemente simbólicas a la hora de conocerlas por su historia en la criptografía y sus usos hace cientos o miles, bueno, cientos no, miles de años.

Y luego hemos visto el concepto de simétrica, simétrica, que es un poco lo que hemos comentado.

Así que bueno, esto es una introducción a la criptografía.

Con esto finalizamos la sesión y os espero en la siguiente sesión.