Guía de trabajo autónomo #8

Nombre del docente: Daniel Chaves Ureña

Taller Exploratorio: Tecnologías de la Información y la Comunicación

Unidad de estudio: Herramientas para la gestión y análisis de la información

Nivel: Décimo Año.

Horario de atención: A distancia lunes a viernes 7:00 a.m. – 4:30 p.m. (Según horario establecido)

Centro educativo: lunes a viernes 7:00 a.m. – 4:30 p.m. (Según horario establecido).

Escenario: 1 ( ) 2 ( ) 3 ( ) 4 ( )

Período establecido para el desarrollo de la guía:

II Parte. Planificación Pedagógica

Espacio físico, materiales o recursos didácticos que voy a necesitar: **(Importante considerar la situación de cada uno de los estudiantes)**	• Cuaderno de la subárea de Programación. • Lápiz o lapicero, según su preferencia, lápices de color de ser necesario. • Espacio cómodo, según la preferencia de cada estudiante y las posibilidades en el hogar o lugar de residencia.
Indicaciones generales:	Dicha GTA la encontraras en Microsoft Teams en el grupo de trabajo establecido para su respectiva sección, y en la Página del Colegio
Fecha de Entrega máxima:	8 de Noviembre del 2021

Detalle de la planificación de las actividades que realiza el estudiante.

Resultado (s) de aprendizaje/Objetivo (s):

Marco teórico Herramientas para la gestión y análisis de la información

El arte de proteger los secretos…

Criptografía: Básicamente, la criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario, así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

entre otras finalidades, para:

- autentificar la identidad de usuarios
- autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias
- proteger la integridad de transferencias electrónicas de fondos

Criptografía y Seguridad informática

Un mensaje codificado por un método de criptografía debe ser privado, o sea, solamente aquel que envió y aquel que recibe debe tener acceso al contenido del mensaje. Además de eso, un mensaje debe poder ser suscrito, o sea, la persona que la recibió debe poder verificar si el remitente es realmente la persona que dice ser y tener la capacidad de identificar si un mensaje puede haber sido modificado.

Los métodos de criptografía actuales son seguros y eficientes y basan su uso en una o más llaves. La llave es una secuencia de caracteres, que puede contener letras, dígitos y símbolos (como una contraseña), y que es convertida en un número, utilizada por los métodos de criptografía para codificar y decodificar mensajes.

Claves Simétricas y Asimétricas

Las claves criptográficas pueden ser básicamente de dos tipos:

Simétricas: Es la utilización de determinados algoritmos para descifrar y encriptar (ocultar) documentos. Son grupos de algoritmos distintos que se relacionan unos con otros para mantener la conexión confidencial de la información.

Asimétricas: Es una fórmula matemática que utiliza dos llaves, una pública y la otra privada. La llave pública es aquella a la que cualquier persona puede tener acceso, mientras que la llave privada es aquella que sólo la persona que la recibe es capaz de descifrar.

Actualmente, los métodos criptográficos pueden ser subdivididos en dos grandes categorías, de acuerdo con el tipo de llave utilizado: criptografía de llave única y la criptografía de llave pública y privada.

Métodos Criptográficos

Criptografía de llave única: La criptografía de llave única utiliza la misma llave tanto para codificar como para decodificar mensajes. A pesar de que este método es bastante eficiente en relación al tiempo de procesamiento, o sea, el tiempo que gasta para codificar y decodificar mensajes, tiene como principal desventaja la necesidad de utilización de un medio seguro para que la llave pueda ser compartida entre personas o entidades que deseen intercambiar información criptografiada.

Criptografía de llaves pública y privada: La criptografía de llaves pública y privada utiliza dos llaves distintas, una para codificar y otra para decodificar mensajes. Con este método cada persona o entidad mantiene dos llaves: una pública, que puede ser divulgada libremente, y otra privada, que debe ser mantenida en secreto por su dueño. Los mensajes codificados con la llave pública solo pueden ser decodificados con la llave privada correspondiente.

Como ejemplo, José y María quieren comunicarse de manera sigilosa. Entonces, ellos tendrán que realizar los siguientes procedimientos:

José codifica un mensaje utilizando la llave pública de María, que está disponible para el uso de cualquier persona.

Después de criptografiarlo, José envía el mensaje a María, a través de Internet.

María recibe y decodifica el mensaje, utilizando su llave privada, que es sólo de su conocimiento.

Si María quisiera responder el mensaje, deberá realizar el mismo procedimiento, pero utilizando la llave pública de José.

A pesar de que este método tiene un desempeño muy inferior en relación al tiempo de procesamiento, comparado al método de criptografía de llave única, presenta como principal ventaja la libre distribución de llaves públicas, no necesitando de un medio seguro para que llaves sean combinadas con antelación.

¿Qué es firma digital?

La firma digital consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda verificar si el remitente es quien dice ser e identificar cualquier mensaje que pueda haber sido modificado.

De esta forma, es utilizado el método de criptografía de llaves pública y privada, pero en un proceso inverso al presentado en el ejemplo anterior.

Si José quisiera enviar un mensaje suscrito a María, él codificará un mensaje con su llave privada. En este proceso será generada una firma digital, que será añadida al mensaje enviado a María. Al recibir el mensaje, María utilizará la llave pública de José para decodificar el mensaje. En este proceso será generada una segunda firma digital, que será comparada con la primera. Si las firmas fueran idénticas, María tendrá certeza de que el remitente del mensaje fue José y que el mensaje no fue modificado.

Es importante resaltar que la seguridad del método se basa en el hecho de que la llave privada es conocida sólo por su dueño. También es importante resaltar que el hecho de firmar un mensaje no significara un mensaje sigiloso. Para el ejemplo anterior, si José quisiera firmar el mensaje y tener certeza de que sólo María tendrá acceso a su contenido, sería preciso codificarla con la llave pública de María, después de firmarla.

Ejemplos de criptografía de llave única y de llaves pública y privada

Ejemplos que combinan la utilización de los métodos de criptografía de llave única y de llaves pública y privada son las conexiones seguras, establecidas entre el browser de un usuario y una web, en transacciones comerciales o bancarias vía Web.

Estas conexiones seguras vía Web utilizan el método de criptografía de llave única, implementado por el protocolo SSL (Secure Socket Layer). El browser del usuario necesita informar a la web cual será la llave única utilizada en la conexión segura, antes de iniciar una transmisión de datos sigilosos.

Para esto, el browser obtiene la llave pública del certificado de la institución que mantiene la web. Entonces, utiliza esta llave pública para codificar y enviar un mensaje a la web, contiendo la llave única a ser utilizada en la conexión segura. La web utiliza su llave privada para decodificar el mensaje e identificar la llave única que será utilizada.

A partir de este punto, el browser del usuario y la web pueden transmitir informaciones, de forma sigilosa y segura, a través de la utilización del método de criptografía de llave única. La llave única puede ser cambiada a intervalos de tiempo determinados, a través de la repetición de procedimientos descritos anteriormente, aumentando así el nivel de seguridad de todo el proceso.

.

Actividades de aprendizaje para la implementación de la mediación pedagógica en educación combinada	Evidencias
1- Explique el concepto de Criptografía. 2- ¿Qué relación tiene la evolución de las computadoras con el avance en la criptografía? 3- ¿Cuáles son las 3 finalidades de la criptografía? 4- ¿Porque un mensaje enviado a una persona debe de ser suscrito, y esto que significa? 5- Mencione los dos tipos de claves criptográficas, y su concepto 6- ¿Cuáles son los Métodos criptográficos y su concepto? 7- ¿Cuál es la diferencia entre la llave Única, y la llave pública o privada? 8- ¿Que se entiende por Firma Digital? 9 – Realice una pequeña explicación o ensayo, de la importancia de la seguridad criptográfica en el ámbito informático, y la repercusión de su desconocimiento por la gente.	**Tipo de evidencia:** **Conocimiento** **Ilustrar los procedimientos para la protección e integridad de los datos mediante el uso de tecnologías.**

Instrumento de Evaluación de las Evidencias			
Indicadores o criterios de desempeño/competencias del aprendizaje esperado			
Evidencias	**Aún no logrado**	**En Proceso**	**Logrado**
Ilustrar los procedimientos para la protección e integridad de los datos mediante el uso de tecnologías			

Rúbrica

Criterio	Puntaje	Descripción
Aún no logrado	1	El estudiante desconoce los conceptos, procedimientos, operaciones necesarias para obtener la evidencia solicitada.
En proceso	2	El estudiante conoce algunos de los conceptos, procedimientos, operaciones necesarias para obtener la evidencia solicitada, pero no llega a obtenerla del todo.
Logrado	3	El estudiante demuestra que logra obtener la evidencia solicitada.