ÁREA TECNOLOGÍA E INFORMÁTICA
GRADO DÉCIMO.
TALLER 1 SEGUNDO PERIODO 2023.

LOGRO: Utilizar adecuadamente herramientas de uso de transmisión de datos por medio de las diferentes tipologías de redes.

DBA: Comprende el concepto de redes e Identifica cada una de las tipologías de redes

1. Lea con mucha atención el siguiente texto:

DEFINICIÓN DE RED DE COMUNICACIÓN DE DATOS.

El término genérico "**red**" hace referencia a un conjunto de entidades (objetos, personas, elementos etc.) conectadas entre sí. Por lo tanto, una red permite que circulen elementos materiales o inmateriales entre estas entidades, según reglas bien definidas. Del latín rete, el término red se utiliza para definir a una estructura que cuenta con un patrón característico. Existen múltiples tipos de red, como la red informática, la red eléctrica y la red social, etc.

Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

Puede a su vez dividirse en diversas categorías, según su alcance (red de área local o LAN, red de área metropolitana o MAN, red de área amplia o WAN, etc.), su método de conexión (por cable coaxial, fibra óptica, radio, microondas, infrarrojos) o su relación funcional (cliente-servidor, persona a persona), entre otras.

HISTORIA:
El primer indicio de redes de comunicación fue de tecnología telefónica y telegráfica. En 1940 se transmitieron datos desde la Universidad de Darmouth, en Nuevo Hampshire, a Nueva York. A finales

de la década de 1960 y en los posteriores 70 fueron creadas las minicomputadoras. En 1976, Apple introduce el Apple I, uno de los primeros ordenadores personales.
En 1981, IBM introduce su primer PC. A mitad de la década de 1980 los PC comienzan a usar los módem para compartir archivos con otros ordenadores, en un rango de velocidades que comenzó en 1200 bps y llegó a los 56 kbps (comunicación punto a punto o dial-up), cuando empezaron a ser sustituidos por sistema de mayor velocidad, especialmente ADSL.

POR QUÉ LAS REDES SON IMPORTANTES

Un equipo es una máquina que se usa para manipular datos. Los seres humanos, como seres comunicativos, comprendieron rápidamente porqué sería útil conectar equipos entre sí para intercambiar información.

Una red de comunicación de datos o red informática puede tener diversos propósitos:

- Intercambio de recursos (archivos, aplicaciones o hardware, una conexión a Internet, etc.)
- Comunicación entre personas (correo electrónico, debates en vivo, etc.)
- Comunicación entre procesos (por ejemplo, entre equipos industriales)
- Garantía de acceso único y universal a la información (bases de datos en red)
- Videojuegos de varios jugadores

Las redes también se usan para estandarizar aplicaciones. El término groupware se usa generalmente para referirse a las herramientas que permiten que varias personas trabajen en una red. Por ejemplo, las agendas grupales y el correo electrónico se pueden usar para comunicar de manera más rápida y eficaz. Estas son algunas de las ventajas de dichos sistemas:

- Costos más bajos gracias al uso compartido de datos y de periféricos
- Estandarización de aplicaciones
- Acceso a los datos a tiempo
- Comunicación y organización más eficaces

Actualmente, gracias a Internet, presenciamos una unificación de las redes. Por lo tanto, las ventajas de instalar una red son múltiples, ya sea para una empresa comercial, para uso particular o para uso pedagógico o administrativo en los colegios o universidades.

COMPONENTES BÁSICOS DE LAS REDES

Para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (hosts) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es la de interconectar los componentes hardware de una red, y por tanto, principalmente, las computadoras individuales, también denominados hosts, a los equipos que ponen

los servicios en la red, los servidores, utilizando el cableado o tecnología inalámbrica soportada por la electrónica de red y unidos por cableado o radiofrecuencia. En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea ésta parte de un ordenador, de un conmutador, de una impresora, etc. y sea de la tecnología que sea (Ethernet, Wi-Fi, Bluetooth, etc.)

La red eléctrica, por su parte, es aquella conformada por generadores eléctricos, transformadores, líneas de transmisión y líneas de distribución, que se encargan de llevar la electricidad a los usuarios residenciales. El sistema utiliza diferentes tensiones, donde las más altas se utilizan en las distancias más largas, mientras que las tensiones se van reduciendo a medida que la energía se acerca a las instalaciones del usuario.

En cuanto a la red social, el concepto se refiere a aquella estructura donde diversos individuos mantienen distintos tipos de relaciones (de amistad, comerciales, sexuales, etc.).
La red social ha actualizado su significado en los últimos años, ya que comenzó a utilizarse el término para definir a los sitios de Internet que promueven las comunidades virtuales de acuerdo a intereses. MySpace y Facebook son dos de estas redes sociales que reúnen a millones de usuarios, quienes pueden intercambiar mensajes y archivos con otros miembros de la red.

CLASIFICACÍON DE REDES INFORMÁTICAS:

Si bien existen diversas clasificaciones de redes informáticas, la más reconocida es aquella que las distingue de acuerdo a su alcance. De esta manera los tipos de redes son:
RED DE ÁREA LOCAL o LAN: (Local Área Network). Esta red conecta equipos en un área geográfica limitada, tal como una oficina o edificio. De esta manera se logra una conexión rápida, sin inconvenientes, donde todos tienen acceso a la misma información y dispositivos de manera sencilla.

RED DE ÁREA METROPOLITANA o MAN: (Metropolitan Área Network). Ésta alcanza un área geográfica equivalente a un municipio. Se caracteriza por utilizar una tecnología análoga a las redes LAN, y se basa en la utilización de dos buses de carácter unidireccional, independientes entre sí en lo que se refiere a la transmisión de datos.

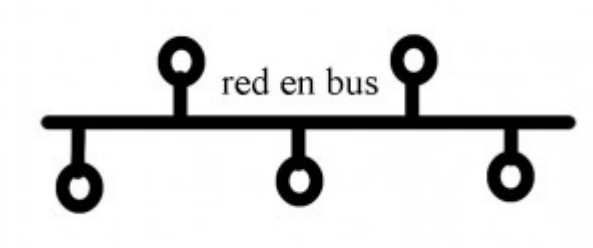
RED DE ÁREA AMPLIA o WAN: (Wide Área Network). Estas redes se basan en la conexión de equipos informáticos ubicados en un área geográfica extensa, por ejemplo entre distintos continentes. Al comprender una distancia tan grande la transmisión de datos se realiza a una velocidad menor en relación con las redes anteriores. Sin embargo, tienen la ventaja de trasladar una cantidad de información mucho mayor. La conexión es realizada a través de fibra óptica o satélites.

RED DE ÁREA LOCAL INALÁMBRICA o WLAN: (Wireless Local Área Network). Es un sistema de transmisión de información de forma inalámbrica, es decir, por medio de satélites, microondas, etc. Nace a partir de la creación y posterior desarrollo de los dispositivos móviles y los equipos portátiles, y significan una alternativa a la conexión de equipos a través de cableado.

RED DE ÁREA PERSONAL o PAN: (Personal Área Network). Es una red conformada por una pequeña cantidad de equipos, establecidos a una corta distancia uno de otro. Esta configuración permite que la comunicación que se establezca sea rápida y efectiva.

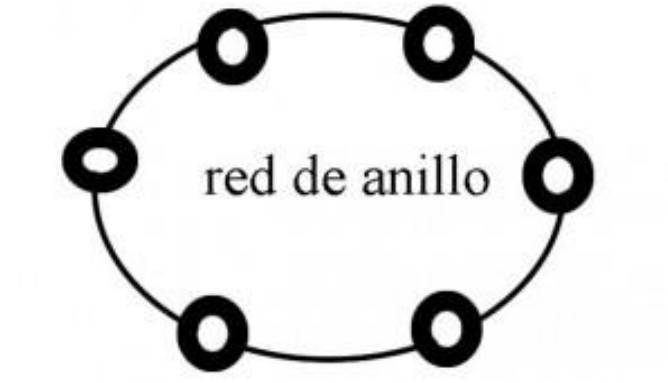
Redes informáticas de acuerdo con su topología o configuración interna, ventajas y desventajas.

1. Bus o en línea



Son aquellas que están conectadas a un mismo tronco o canal de comunicación, a través del cual pasan los datos. Los dos extremos del cable coaxial acaban con un "terminador", que lleva una resistencia que impide la "impedancia". Además, habrá una serie de derivadores T, que son las ramas a las que se conectan los equipos informáticos. Es la más fácil de montar, pero tiene varios inconvenientes: si se rompe el cable, toda la red deja de estar operativa. Además, a medida que añadimos nuevos equipos, con la desventaja de requerir más espacio, la red tiende a degradarse y pierde señal.

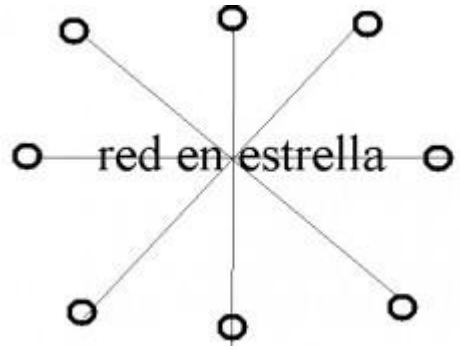
2. Anillo



Es aquella donde un equipo está conectado a otro, y éste al siguiente, en forma de círculo o anillo, hasta volver a conectarse con el primero. Cada estación tiene un transmisor y un receptor. En ocasiones, pueden venir unidas por dos cables, y se llaman de doble anillo.

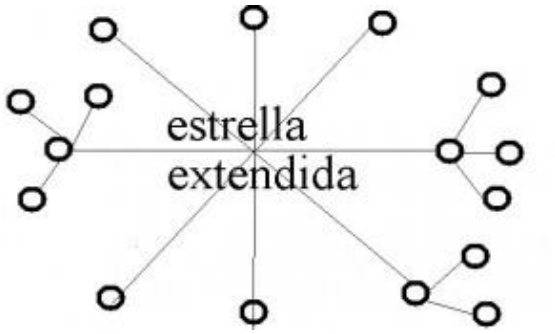
Podemos utilizarla con muchos ordenadores, de manera que no se pierde tanto rendimiento cuando los usamos todos a la vez. Pero el problema una vez más es que un solo fallo en el circuito deja a la red aislada.

3. Estrella



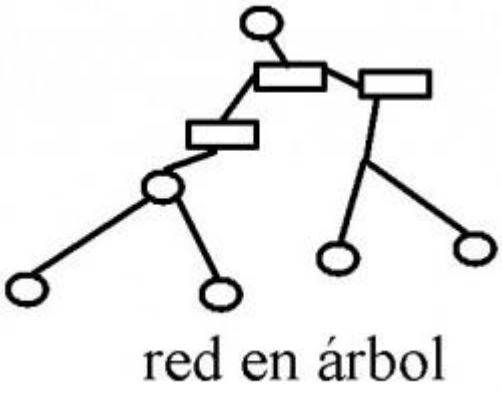
La topología en estrella es donde los nodos están conectados a un "hub". Hablamos de un dispositivo que recibe las señales de datos de todos los equipos y las transmite a través de los distintos puertos.
Tiene la ventaja de que cuando algún cable se rompe, sólo una computadora quedaría aislada de la red y la reparación es más fácil. El repetidor nos permite añadir fácilmente equipos. La única desventaja es el coste (requiere un cable para cada equipo + el hub) y la posibilidad de que falle el hub.

4. Estrella extendida



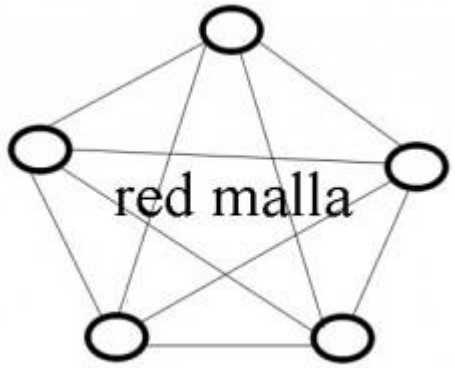
Muy parecida a la anterior, pero en este caso algunas de las computadoras se convierten en el nodo principal o transmisor de datos de otras computadoras que dependen de ésta.

5. Red en árbol



Es muy parecida a la red en estrella, pero no tiene un nodo central. Tenemos varios hub o Switch, cada uno transmitiendo datos a una red en estrella. La principal desventaja es que requiere varios hub y gran cantidad de cable, por lo que resulta más costosa, pero al no estar centralizado, se evita el problema de la interferencia de señales y una mejor jerarquía de la red.

6. En malla



Todos los nodos están interconectados entre sí. De esta forma, los datos pueden transmitirse por múltiples vías, por lo que el riesgo de rotura de uno de los cables no amenaza al funcionamiento de la red. Tampoco requiere de un hub o nodo central y se evita el riesgo de interrupciones e interferencias.
El principal problema, claro está, es que en las redes por cable el coste puede ser muy alto, aunque en temas de mantenimiento daría muchos menos problemas.

2. Responda en hojas de block tamaño carta las siguientes preguntas:

- **a.** Con sus propias palabras elabore una definición de red de comunicación de datos o red informática.
- **b.** ¿Cuáles son los propósitos de una red de comunicación de datos o red informática?
- **c.** ¿Cómo se clasifican las redes de comunicación o redes informáticas? Explique cada una
- **d.** ¿Qué significan las siglas: LAN, WAN, MAN Y WLAN?
- **e.** Explique como es el funcionamiento de las diferentes redes según su tipología y configuración; Realice un esquema o dibujo de cada una.

3. Escoja un esquema de red y haga una maqueta de este tipo de red.

NOTA:

- La maqueta tiene un valor del 50% de la nota final del trabajo; el otro 50% equivale a la resolución del taller escrito.
- El trabajo lo deben presentar escrito a mano.

PROFESOR: LUIS GERMÁN AGUDELO CAMACHO.

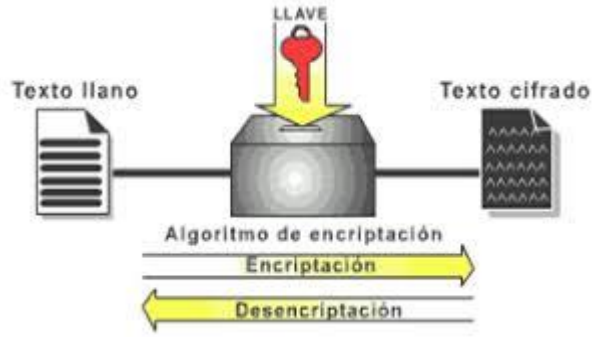
ÁREA TECNOLOGÍA E INFORMÁTICA
GRADO DÉCIMO.
TALLER 2 SEGUNDO PERIODO 2023

DESEMPEÑO: Comprender la importancia de manejar criterios de seguridad con la información que manejamos desde nuestros equipos electrónicos como celulares y computadores

JOVEN ESTUDIANTE:
El texto ¿QUÉ ES LA ENCRPTACIÓN DE DATOS? Es un instrumento donde se nos explica la importancia de proteger la información que constantemente estamos enviando vía internet y que puede ser sujeto de interceptación para mal uso o en ocasiones para la extorsión por eso es importante conocer un poco de que se trata este sistema de seguridad de nuestra información y equipos.

Por favor lea el siguiente texto con mucha atención y responda en el cuaderno las preguntas que se encuentran al final del documento:

¿QUÉ ES LA ENCRIPTACIÓN DE DATOS?



Corresponde a una tecnología que permite la transmisión segura de información, al codificar los datos transmitidos usando una fórmula matemática que "desmenuza" los datos. Asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos.

Para proteger la información almacenada se suele recurrir a las denominadas técnicas de encriptación, la encriptación consiste básicamente en convertir un mensaje en otro de forma tal que el mensaje original solo pueda ser recuperado por un determinado grupo de personas que saben cómo "desencriptar" el mensaje codificado.

El esquema básico de encriptación implica la utilización de un password o clave para encriptar el mensaje de forma tal que solo puedan desencriptar el mensaje aquel que conoce el password utilizado.

CRIPTOGRAFÍA
La encriptación de datos funciona utilizando la criptografía. La criptografía es la ciencia de usar las matemáticas para encriptar y desencriptar datos. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o enviada a través de una red insegura (como Internet) y aun así permanecer secreta. Luego, los datos pueden desencriptarse a su formato original.

Algoritmo criptográfico: Un algoritmo criptográfico, o cifrador, es una función matemática usada en los procesos de encriptación y desencriptación. Un algoritmo criptográfico trabaja en combinación con una llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos.
Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada llave posible El resultado de este cálculo son los datos encriptados.

Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados. La mayoría de los algoritmos modernos del cifrado se basan en una de las siguientes dos categorías de procesos: Problemas matemáticos que son simples pero que tienen una inversa que se cree (pero no se prueba) que es complicada Secuencias o permutaciones que son en parte definidos por los datos de entradas.

Diferencias entre el proceso de encriptación y desencriptación:
La encriptación es el proceso en el cual los datos a proteger son traducidos a algo que parece aleatorio y que no tiene ningún significado (los datos encriptados). La desencriptación es el proceso en el cual los datos encriptados son convertidos nuevamente a su forma original.

LA ENCRIPTACIÓN ABARCA:

- **Consultoría de Seguridad y Gestión del Riesgo**:

Dentro de esta línea están los servicios de consultoría dedicados a la definición de planes directores de seguridad, políticas y planes de seguridad preventiva y planes de contingencia.

- **Arquitecturas de Seguridad:**

Línea dedicada al diseño e integración de soluciones corporativas de seguridad perimetral, de infraestructuras y de sistemas. Entre otras soluciones, en esta línea se encuentran las plataformas de seguridad perimetral (cortafuegos, redes privadas virtuales, etc.), de contenidos, de detección y prevención de intrusiones, de análisis y gestión de vulnerabilidades.

- **Certificación y Firma Electrónica**:

Esta línea se ocupa del despliegue de Infraestructuras de Certificación (PKI) corporativas, desde la definición de Políticas y Prácticas de Certificación hasta el despliegue de servicios avanzados como el Sellado de Tiempo o la Validación. Se incluyen los trabajos de integración de las Tecnologías de Certificación (firma, cifrado, autenticación) en los Sistemas de Información.

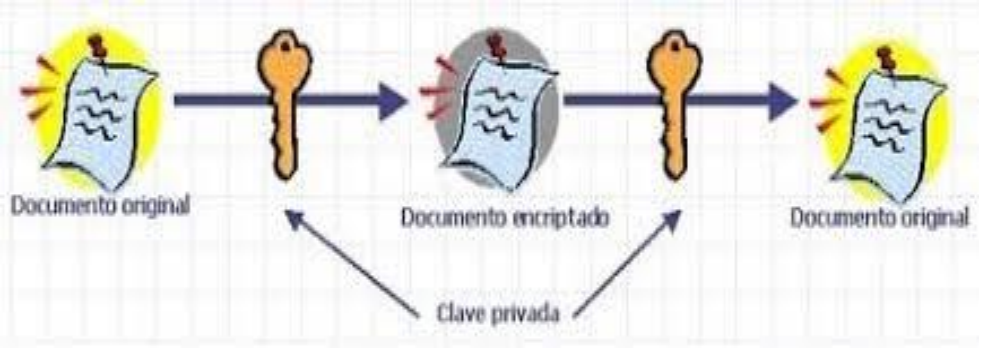
- **Gestión de Identidades**:

Son sistemas de gestión de seguridad corporativa efectivos y alineados con la realidad del negocio. Entre las soluciones de gestión de identidades se pueden destacar los sistemas de gestión de información de seguridad y control de fraude, los Directorios. La seguridad informática Debe garantizar: La Disponibilidad de los sistemas de información. ·

- La Recuperación rápido y completa de los sistemas de información.
- La Integridad de la información.
- La Confidencialidad de la información.

FUNCIONAMIENTO

Para la encriptación de datos se utiliza comúnmente un sistema de clave pública que permite conjuntamente con la firma digital, el aseguramiento de la integridad de los datos transmitidos o almacenados.



La encriptación con algoritmos de clave pública, funciona con un par de llaves, una publica y una privada. Estas claves permiten que el receptor y emisor mantengan una comunicación confiable permitiendo que los datos viajen a través de la red encriptados y que, al llegar al receptor, pueda el mismo recomponer la información fácilmente.

La encriptación de datos se basa en métodos llamados Métodos de encriptación: Para poder Encriptar un dato, se pueden utilizar procesos matemáticos diferentes:

- **Algoritmo HASH:** Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC. Es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor. Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

  Entre los algoritmos de hash más comunes están: SHA-1:

  - Algoritmo de hash seguro. Algoritmo de síntesis que genera un hash de 60 bits. Se utiliza, por ejemplo, como algoritmo para la firma digital. MD2 está optimizado para computadoras de 8 bits. El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el computador (128 bits o 16 bytes) y añadiéndole un checksum. Para el cálculo real, se utiliza un bloque auxiliar 48 bytes y una tabla de 256 bytes que contiene dígitos al azar del número pi.

- **MD4** es un algoritmo de resumen del mensaje (el cuarto en la serie) diseñado por el profesor Ronald Rivest del MIT. Implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes. La longitud del resumen es de 128 bits.
- **MD5** Esquema de hash de hash de 128 bits muy utilizado para autenticación cifrada. Gracias al MD5 se consigue, por ejemplo, que un usuario demuestre que conoce una contraseña sin necesidad de enviar la contraseña a través de la red.

- **Algoritmos Simétricos**: Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. En este modelo, el mensaje original es convertido en un mensaje cifrado que aparentemente es aleatorio y sin sentido. El proceso de encriptación está formado por dos componentes, un algoritmo y una clave. La clave es un valor que es independiente del texto o mensaje a cifrar. El algoritmo va a producir una salida diferente para el mismo texto de entrada dependiendo de la clave utilizada. Una vez cifrado, el mensaje puede ser transmitido. El mensaje original puede ser recuperado a través de un algoritmo de desencriptación y la clave usada para la encriptación.

- **Algoritmos Asimétricos**: (RSA): Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. Los pasos del proceso de encriptación con clave pública son los siguientes:
  - Cada sistema genera un par de claves para ser usadas en la encriptación y desencriptación de los mensajes que envíen y reciban.
  - Cada sistema publica su clave de encriptación (clave pública). La clave de desencriptación relacionada (clave privada) se mantiene en privado.
  - Si Juan desea enviar un mensaje a Martín, encripta el mensaje utilizando la clave pública de Martín.
  - Cuando Martín recibe un mensaje lo desencripta usando su clave privada. Nadie puede desencriptar el mensaje porque solo Bob conoce su clave privada.

- **Algoritmo de encriptación RC4:** Es un algoritmo de Cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 usando remailers anónimos en un grupo de news: sci.crypt. Es usado por diversos programas comerciales como Netscape y Lotus Notes.

- **Firma Digital:** La firma digital permite garantizar algunos conceptos de seguridad que son importantes al utilizar documentos en formato digital, tales como Identidad o autenticidad, integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas.

- **Ventajas Ofrecidas por la Firma Digital:**
  - Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, el receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.

- Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.
- No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Diferencias entre los algoritmos simétricos y los asimétricos:
Los algoritmos simétricos, encriptan y desencriptan con la misma llave. Las principales ventajas de los algoritmos simétricos son su seguridad y su velocidad. Los algoritmos asimétricos encriptan y desencriptan con diferentes llaves. Los datos se encriptan con una llave pública y se desencriptan con una privada, siendo ésta su principal ventaja.

Los algoritmos asimétricos, también conocidos como algoritmos de llave pública, necesitan al menos una llave de 3.000 bits para alcanzar un nivel de seguridad similar al de uno simétrico de 128 bits. Y son increíblemente lentos, tanto que no pueden ser utilizados para encriptar grandes cantidades de información.

Los algoritmos simétricos son aproximadamente 1.000 veces más rápidos que los asimétricos.

Otros:
El protocolo SSL, protege los datos transferidos mediante conexión http, es decir navegación web, utilizando encriptación provista por un Servidor Web de Seguridad. Una llave pública es empleada para encriptar los datos, y una llave privada se utiliza para descifrar o desencriptar la información.

CryptoForge proporciona cuatro robustos algoritmos de encriptación para proteger sus datos: Blowfish (llave de 448 bits) es un algoritmo de encriptación rápido y fuerte. Su creador es Bruce Schneier, uno de los más prestigiosos criptógrafos en el mundo.

Ríndale (llave de 256 bits) es un algoritmo seguro y eficiente. Sus creadores son Joan Daemen y Vincent Rijmen (Bélgica). Ha sido elegido como el nuevo Estándar Avanzado de Encriptación (AES) por el Instituto Nacional de Estándares y Tecnología (NIST) de los EEUU.

Triple DES (llave de 168 bits) es un algoritmo desarrollado por el gobierno de EEUU y ha sido evaluado durante años sin descubrírsele debilidades. Es una configuración de encriptación en la cual el algoritmo DES es usado tres veces con tres llaves diferentes. Gost (llave de 256 bits) es un algoritmo de Rusia y podría ser considerado el análogo ruso al DES. Tiene un diseño conservador y no ha podido ser vulnerado, a pesar de haber sido uno de los más estudiados, durante años, por los mejores expertos en criptoanálisis. Cuando usted ingresa su contraseña en CryptoForge, ésta es procesada con un algoritmo

Hash para generar una huella digital, conocida en inglés como "digest". Encriptar datos en un dispositivo móvil (Smartphone). La importancia de tener nuestros datos a salvo de miradas extrañas o tener un mínimo de privacidad se ha convertido en un tema muy importante.

Los Smartphone son muchas veces usados como pequeñas oficinas portátiles donde se guardan datos de gran valor y donde es de gran importancia tener estos datos protegidos. Muchos usuarios de Smartphone por comodidad no protegen el acceso de inicio con una clave, imagínense en caso de pérdida del aparato o descuido poder dejar estos datos confidenciales en manos ajenas a las nuestras. Para solucionar este problema o tener un cierto grado de seguridad, es muy importante poder cifrar nuestros datos. Encriptación de ficheros Windows nos da una alternativa para poder proteger estos datos y prevenir su pérdida.

El "Encripting File System" (EFS) es el encargado de codificar los ficheros. Estos ficheros sólo se pueden leer cuando el usuario que los ha creado hace "login" en su máquina (con lo cual, presumiblemente, nuestra password será una password robusta). De hecho, cualquiera que acceda a nuestra máquina, no tendrá nunca acceso a nuestros ficheros encriptados, aunque sea un Administrador del equipo. La encriptación es el proceso de codificar datos sensibles usando un algoritmo. Sin la clave del algoritmo correcta los datos no pueden ser desencriptados.

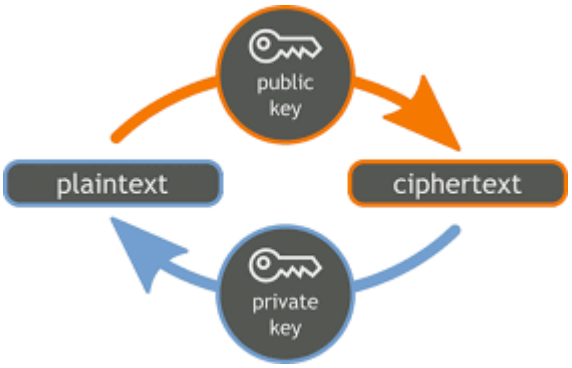
Windows usa encriptación para varios propósitos:

- Ficheros encriptados en un volumen NTFS.
- Datos encriptados enviados entre un cliente web y un servidor usando Security Socket Layer (SSL).
- Encriptando tráfico entre computadores usando VPN.
- Encriptando o firmando mensajes de email.

EFS permite encriptar archivos en un volumen NTFS local (insisto: "local". No es aplicable a volúmenes en red). Esto ofrece un nivel de protección adicional a los permisos NTFS. Recordemos que los volúmenes NTFS pueden ser vulnerables por muchas vías: por ejemplo, instalando otro Windows XP en otra partición y tomando posesión de la partición primitiva, o bien arrancando con utilidades como NTFSDOS. En estos casos, si alguien tiene acceso físico a nuestra máquina, podría llevarse información confidencial.

Este es uno de los motivos por los que se hace imprescindible, sobre todo en equipos portátiles de empresa, el tener encriptada la información sensible. Ante robo o pérdida, los datos serán irrecuperables.

TIPOS DE CIFRADOS:



Cifrado es otro nombre que se le da al proceso de encriptación. El propósito de un cifrado es tomar datos sin encriptar, llamado texto en claro, y producir una versión encriptada de los mismos. Existen dos clases de cifrado: cifrado de flujo de datos y cifrado por bloques.

Cifrado de flujo de datos: En el cifrado por flujo de datos se encripta un bit (o byte) de texto en claro por vez. El ejemplo más simple de cifrado por flujo de datos es el que consiste en combinar los datos, un bit a la vez, con otro bloque de datos llamado pad. Los cifrados por flujo de datos funcionan realmente bien con datos en tiempo real como voz y video.

Cifrado por bloques: operan sobre bloques de tamaño mayor que un bit del texto en claro y producen un bloque de texto cifrado, generalmente los bloques de salida son del mismo tamaño que los de la entrada. El tamaño del bloque debe ser lo suficientemente grande como para evitar ataques de texto cifrado... El de cifrado de flujo de datos puede ser considerado como un cifrado por bloques de tamaño 1 bit.

Tomado de: http://encriptaciondedatos.blogspot.com.co/2007/09/encriptacion-de-datos.html

CONTESTE EN EL CUADERNO LAS SIGUIENTES PREGUNTAS:

1. Realiza un ensayo en el cual se explique la importancia del cifrado de la información.
2. Realiza una lista de las palabras desconocidas y busca su significado en el diccionario.
3. ¿Qué es la criptografía y desde cuando se utiliza?
4. ¿Cuáles son las diferentes formas de cifrar datos?
5. ¿Qué es el cifrado de ficheros?
6. ¿Qué tipos de datos es conveniente cifrar?
7. ¿Qué es la firma digital y qué ventajas tiene su uso?
8. ¿Para qué se usa el protocolo SSL?

PROFESOR: LUIS GERMAN AGUDELO CAMACHO.