|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DATOS DE LA ACTIVIDAD | | | | | | | |
| No. de Actividad: | **3.3** | **Investigación** | **Actividad 3.3 Cuadro comparativo entre: Algoritmos hash MD5, SHA-n y HMAC Algoritmos de cifrado (DES, 3DES, AES y otros)** | | | | |
| Unidad: | Unidad 3: Configuración de SSH y VPN | | | | | | |
| Carrera: | Tgo. en Desarrollo de Software | | | | | | |
| Materia | SEGURIDAD EN INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN | | | | | Clave | **18MPEDS0835** |
| Profesor: | Andrés Figueroa Flores | | | | | | |
| Alumno: | Esmeralda Itzel Rodríguez Guareño | | | | | Registro: | 19100256 |
| Alumno: | Juan Carlos Villarroel Capetillo | | | | | Registro: | 19100309 |
| Institución: | **Centro de Enseñanza Técnica Industrial plantel Colomos** | | | | | | |
| Semestre: | 8 | Grupo: | B1 | Período: | Ago-Dic 2022 | Fecha: | 03/11/2022 |
| Compet. Genéricas | | 4.1, 4.5, 5.2, 5.5 | | Compet.. Profesional | | 12 | |

**Propósito u objetivo:**Identificar los principales Algoritmos HASH y Algoritmos de cifrado.

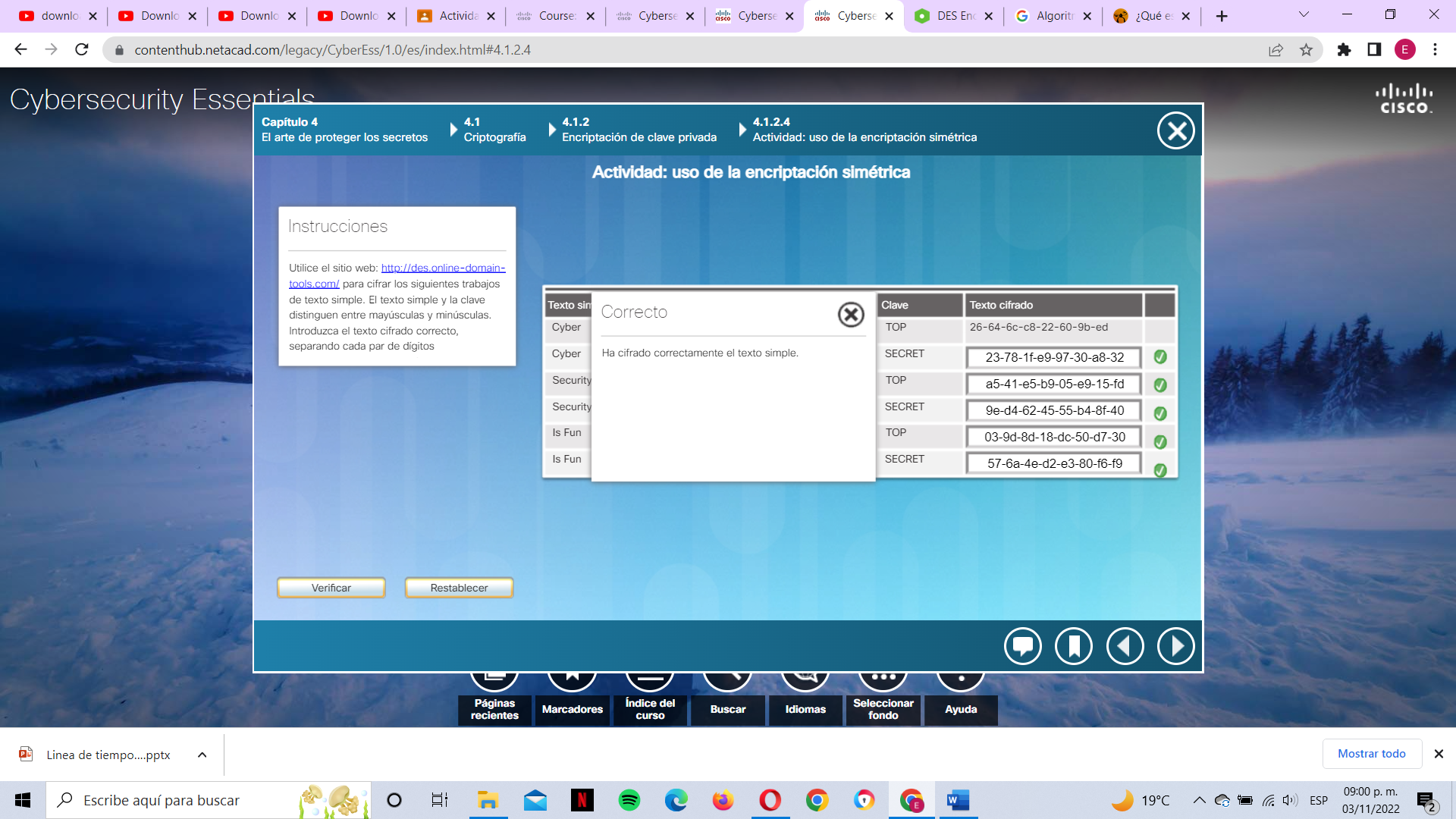
**Instrucciones**:  
  
1. Investigar la información sobre Algoritmos HASH y Algoritmos de cifrado.  
  
2. Elaborar un cuadro comparativo de las características de los algoritmos Hash MD5, SHA-n y HMAC y entre los Algoritmos de cifrado (DES, 3DES, AES y otros).  
  
3. Leer el tema 4.1 Criptografía y 5.1 Tipos de controles de integridad de datos, en el curso Cybersecurity Essentials, <https://www.netacad.com/>  
  
4. Responder las siguientes actividades, tomar impresión de pantalla completa (con sus nombre) de cada actividad correcta y subir en la misma actividad (en el archivo de WORD junto con el cuadro comparativo):  
4.1.2.4 Actividad: uso de la encriptación simétrica  
4.1.3.3 Actividad: uso de la encriptación asimétrica  
4.1.4.4 Actividad: comparar la encriptación simétrica con la encriptación asimétrica  
5.1.1.9 Actividad: identificar la terminología de hash  
  
5. Usar el archivo de ejemplo de actividades en WORD, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.  
  
6. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

**Cuadro Comparativo**

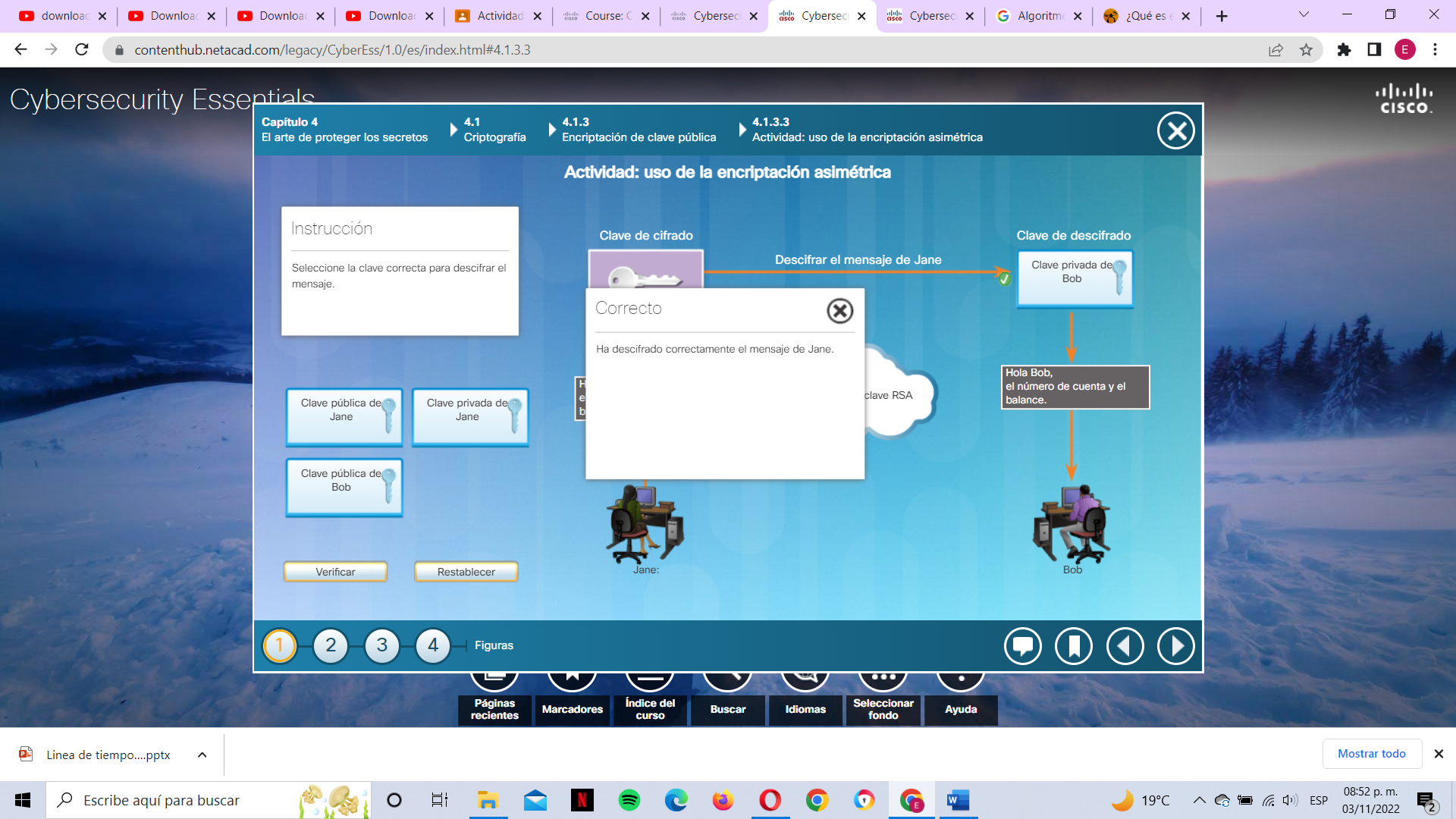
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Hash MD5 | SHA-n | HMAC | Algoritmo Des | Algoritmo 3DES | Algoritmo AES |
| MD5 es una función unidireccional que facilita el cálculo de un hash de datos de entrada dados, pero dificulta el cálculo de los datos de entrada con un solo valor hash.  MD5 produce un valor hash de 128 bits. El malware Flame comprometió la seguridad de MD5 en 2012. Los creadores del malware Flame utilizaron una colisión MD5 para forjar un certificado de firma de códigos de Windows. | Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos desarrolló SHA, el algoritmo especificado en el Estándar de hash seguro (SHS). NIST publicó SHA-1 en 1994. SHA-2 reemplazó a SHA-1 por cuatro funciones de hash adicionales para componer la familia SHA:   * SHA-224 (224 bits) * SHA-256 (256 bits) * SHA-384 (384 bits) * SHA-512 (512 bits)   SHA-2 es un algoritmo más sólido y reemplaza a MD5. SHA-256, SHA-384 y SHA-512 son los algoritmos de próxima generación. | Los HMAC utilizan una clave secreta adicional como entrada a la función de hash. El uso de HMAC va un paso más allá de garantizar la integridad al incorporar la autenticación. Un HMAC utiliza un algoritmo específico que combina una función de hash criptográfica con una clave secreta.  Solo el emisor y el receptor conocen la clave secreta y el resultado de la función de hash ahora depende de los datos de entrada y la clave secreta | Es un algoritmo a bloques. El algoritmo DES, cuyas siglas representan el nombre de Data Encryption Standard, fue desarrollado en 1976 en Estados Unidos por las organizaciones IBM (International Business Machines) y NSA (National Security Agency).  El algoritmo DES (Data Encryption Standard) fue desarrollado con la intención de resistir un [ataque de día cero](https://keepcoding.io/blog/que-es-un-ataque-de-dia-cero-en-ciberseguridad/) que había descubierto la NSA. Sus características de seguridad son las siguientes:  Tamaño del bloque: 64 bits  Tamaño de la clave: 56 bits  El número de claves posibles de este algoritmo puede calcularse elevando dos a la cincuenta y seis, lo cual da un número total de opciones que un ordenador sería capaz de probar en un ciberataque. De hecho, esto fue comprobado en 1998 con el desarrollo de la máquina [EEF DES Cracker](https://www.eff.org/es/press/releases/eff-des-cracker-machine-brings-honesty-crypto-debate), la cual es capaz de romper este código en cuestión de días. | Debido a lo fácil que era romper la versión original, se creó una modificación del algoritmo DES, que se conoce como 3-DES o Triple DES. Esta nueva versión vino con la capacidad de encriptar tres veces consecutivas los datos de entrada del bloque, con tres claves diferentes de 56 bits. El algoritmo Triple DES utiliza también bloques de 64 bits, pero cuenta con características adicionales que aumentan su seguridad:  Tamaño del bloque: 64bits  Tamaño de la clave: 168bits  Bits de seguridad: 112bits | El algoritmo AES, también conocido como Rijndael, es un algoritmo creado en Bélgica que fue adoptado por el gobierno de Estados Unidos como estándar, después de que ganara el concurso llamado Advanced Encryption Standard. El premio se creó con el fin de reemplazar el algoritmo DES y su versión mejorada 3-DES. Desde que se eligió el algoritmo Rijndael, se le conoce oficialmente como AES y ha sido el estándar más utilizado desde el año 2001.  El algoritmo AES (Advanced Encryption Standard) cuenta con las siguientes características:  Tamaño de bloque: 128bits  Tamaño de la clave: 128/192/256 bits |

Actividades de Cisco

4.1.2.4



4.1.3.3



4.1.4.4

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

5.1.1.9

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Reflexión

En esta actividad se compararon las diferentes características de los algoritmos de seguridad como el hash, md5, des, 2des, aes. Confirmando que el algoritmo más seguro actualmente es el aes. Pero también fue bueno ver los demás para entender cómo fue su evolución y las fallas que tenían.

# Bibliografía

Cisco. (s.f.). *Cecurity Esscentials.* Obtenido de Cisco: https://contenthub.netacad.com/legacy/CyberEss/1.0/es/index.html#5.1.1.9

Keep Coding. (25 de 07 de 2022). *¿Qué es el algoritmo DES?* Obtenido de Keep Coding : https://keepcoding.io/blog/que-es-el-algoritmo-des/#Que\_es\_un\_algoritmo\_de\_cifrado\_por\_bloques