COLOMBIA POTENCIA DE LA VIDA

TIC

Módulo 1

LECCIÓN 1

Generalidades de la tecnología blockchain

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Taller de aprendizaje:
Criptografía con algoritmos antiguos y ruptura de cifrados, criptografía con algoritmos modernos.

Tiempo de ejecución: 8 horas

Planteamiento de la sesión:

En este taller los estudiantes deberán aplicar los conocimientos adquiridos en las dos lecciones anteriores, haciendo uso de los recursos aprendidos para usar los métodos de cifrado antiguo, también se propone que los estudiantes practiquen hacer el cifrado manualmente para que interioricen el conocimiento.

Materiales

- Calculadora ROT5
https://calculado.net/rot5-codificador-decodificador-en-linea

- Calculadora ROT13
https://rot13.com/

- Calculadora ROT47
https://rot47.net/

- Calculadora Vigenère
https://es.planetcalc.com/2468/

Desarrollo teórico de la sesión:
Criptografía con algoritmos antiguos
6 horas.

Desarrollo de actividades 1:
Criptografía con algoritmos antiguos.

Tiempo de ejecución: 6 horas

En este taller se van a desarrollar trabajos en pares, los estudiantes tendrán que hacer parejas para resolver las diferentes actividades propuestas.

1. Cada miembro de la pareja debe encriptar una frase de al menos 15 palabras en cualquiera de los métodos de cifrado antiguos vistos en la lección. Posteriormente, debe intercambiar con su compañero el mensaje que está cifrado para que este intente descifrarlo, no se pueden decir cuál fue el método de cifrado que utilizaron. El cifrado y descifrado se debe hacer manualmente, sin el uso de las herramientas en línea.

2. Cada pareja debe intentar descifrar en equipo los siguientes mensajes (no se les dirá cuál es el método de cifrado utilizado):

Texto original	Texto cifrado	Algoritmo
La seguridad e integridad de los datos es uno de los pilares fundamentales en blockchain.	Yn frthevqnq r vagrtevqnq qr ybf qngbf rf hab qr ybf cvynerf shaqnzragnyrf ra oybpxpunva.	ROT13
En el año 2024 estoy haciendo un curso de blockchain.	Ra ry nñb 7579 rfgbl unpvraqb ha phefb qr oybpxpunva.	ROT5 y ROT13
Los algoritmos antiguos no se deben usar en el mundo moderno por su falta de seguridad en los datos.	Ybf nytbevgzbf nagvthbf ab fr qrora hfne ra ry zhaqb zbqreab cbe fh snygn qr frthevqnq ra ybf qngbf.	ROT13

3. Las parejas conformadas ahora deben pensar en un párrafo y cifrarlo manualmente con su algoritmo de elección, una vez verifiquen que está bien redactado y cifrado deberán intercambiar el mensaje con otra de las parejas e intentar descífralo (no deben decir cuál es el algoritmo usado). Esta actividad debe tener un límite de tiempo moderado para poner a prueba las habilidades para descifrar un mensaje.

4. A cada estudiante se le debe asignar un criptograma histórico (por ejemplo, de la Segunda Guerra Mundial) para que investiguen su historia y cómo fue descifrado, ellos pueden elegir cuál van a investigar, no debe repetirse el mismo para dos estudiantes. Posteriormente, deben exponer a los demás compañeros lo que encontró y explicar los métodos usados en dicho criptograma.

5. Para esta actividad se deben formar equipos de al menos 4 personas. Cada equipo se debe dividir en dos, uno de ellos va a ser el grupo emisor y el otro va a ser el receptor. El grupo emisor le debe enviar un mensaje cifrado con el algoritmo que ellos elijan al grupo receptor de manera segura, para esta dinámica el mensaje debe pasar por los demás equipos y ellos tienen que intentar descifrar el mensaje antes de la siguiente iteración, debe haber un límite de tiempo para la posesión de los mensajes. La dinámica finaliza cuando el mensaje llegue a los receptores de cada equipo y estos tienen que descifrar el mensaje en el menor tiempo posible. El equipo que haya descifrado la mayor cantidad de mensajes va a ser el ganador.

6. Para esta actividad se deben formar nuevamente los equipos de al menos 3 personas. A cada equipo se le da un mensaje y un algoritmo de cifrado, cada equipo debe cifrar el mensaje manualmente. Una vez todos los equipos tengan los mensajes listos, cada uno pasará a enseñar el mensaje cifrado y los demás equipos deben intentar descifrarlo en el menor tiempo posible (el algoritmo de cifrado no se debe compartir con los demás equipos) y el primero en lograrlo se lleva un punto. Al final gana el equipo que haya descifrado más mensajes de manera exitosa.

7. Formar grupos de al menos 4 personas y dividirlos en dos grupos Grupo emisor y grupo receptor. Cada equipo debe crear su propia clave de cifrado usando las letras del alfabeto y los números del 0 al 26, por ejemplo:

{'a': 0, 'b': 1, 'c': 2, 'd': 3, 'e': 4, 'f': 5, 'g': 6, 'h': 7, 'i': 8, 'j': 9, 'k': 10, 'l': 11, 'm': 12, 'n': 13, 'ñ': 14, 'o': 15, 'p': 16, 'q': 17, 'r': 18, 's': 19, 't': 20, 'u': 21, 'v': 22, 'w': 23, 'x': 24, 'y': 25, 'z': 26}

Cada equipo define cuáles son los pares clave-valor para poder descifrar el mensaje que se va a enviar. Los mensajes deben pasar por todos los equipos antes de llegar al grupo receptos y debe haber un límite de tiempo para intentar descifrar el mensaje sin conocer la clave usada por el otro equipo. El mensaje debe ser una frase de máximo 15 palabras. Al final gana el equipo que haya logrado descifrar más mensajes.

Desarrollo de actividades 2: Criptografía con algoritmos modernos

Tiempo de ejecución: 2 horas

1. Cada estudiante debe responder cuál es el mejor algoritmo de cifrado para los siguientes casos.

- Un grupo de amigos desea comunicarse de forma segura en línea. Deben intercambiar mensajes privados y asegurarse de que nadie más pueda leerlos. ¿Deberían utilizar cifrado simétrico, asimétrico o una combinación de ambos?

- Una empresa realiza transacciones financieras en línea y desea garantizar la autenticidad de cada transacción. ¿Es más adecuado utilizar cifrado asimétrico, cifrado simétrico o una combinación de ambos para firmar digitalmente las transacciones?

- Un servicio en línea desea almacenar de manera segura las contraseñas de sus usuarios. ¿Deberían utilizar cifrado simétrico, asimétrico, una combinación de ambos para garantizar la seguridad de las contraseñas almacenadas o un hash?

- En un entorno donde los dispositivos de Internet de las cosas (IoT) se comunican entre sí, se busca una forma segura de garantizar la confidencialidad de los datos transmitidos. ¿Es más adecuado el cifrado simétrico, asimétrico o una combinación de ambos para esta comunicación?

2. Una vez hayan respondido a las preguntas deberán exponer sus motivos para elegir los algoritmos que pusieron en sus respuestas. Luego de esto se propone generar un debate en el que todos participen dando sus opiniones de cuál es el mejor cifrado para cada caso.

LISTA DE CHEQUEO DE LO QUE APRENDÍ

Carácter de los desempeños	Indicador por evaluar	Si	Parcialmente	No
• Identificar claves de algoritmos de cifrado antiguos. • Usar herramientas online para generar cifrados César y Vigenère.	Entendí los algoritmos de cifrado antiguos y puedo aplicarlos para codificar mensajes y textos con información relevante.			
	Comprendí cómo usar las herramientas disponibles en línea para cifrar y descifrar mensajes y textos.			
	Entendí cómo se puede crear una clave para cifrar un mensaje y mantener la información segura de otras personas.			
• Identificar las principales diferencias entre los algoritmos de cifrado antiguos y los modernos.	Reconocí los avances tecnológicos que transformaron el mundo de la criptografía para crear los sistemas que se usan actualmente.			
• Comparar los diferentes algoritmos de cifrado modernos. • Determinar el mejor cifrado basado en la necesidad de una aplicación o problemática planteada.	Identifiqué las principales diferencias entre los diferentes tipos de cifrados modernos hechos con sistemas computacionales.			
	Comprendí cómo elegir el cifrado que convenga más según las diferentes situaciones que se pueden requerir, teniendo en cuenta la seguridad, integridad y eficiencia.			