Lección 31

Mantener los datos secretos

Lección sin conexión
Ver en Code Studio

Propósito

Los estudiantes tienen una discusión sobre los diferentes niveles de seguridad que desearían para los datos personales. Una vez que la clase ha desarrollado una comprensión de la importancia de la privacidad, aprenden sobre el proceso de cifrado de información codificando una nota para un compañero y descifrando la nota del compañero. La clase concluye con una discusión sobre la importancia de la seguridad física y digital.

Como los estudiantes han estado codificando y decodificando con datos, no han estado preocupados por la seguridad de los datos que están usando. En esta lección, comienzan a pensar en cómo pueden garantizar que solo el destinatario pueda leer los datos que envía. Usarán un cifrado simple para codificar un mensaje. Los estudiantes deben comprender que, para encriptar un mensaje, necesitan tanto un algoritmo como una clave, y que es importante que la clave se mantenga en secreto.

Secuencia para el aprendizaje

Conocimiento inicial (5 min)

Ampliación del conocimiento (40 min)

Transferencia del conocimiento (5 min)

Objetivos

Los estudiantes serán capaces de:

- Aplicar un método de encriptación para garantizar la transmisión segura de datos.
- Usar medidas de seguridad físicas y digitales para proteger los datos.

Recursos

¡Atención!
Por favor, haga una copia de cada documento que planee compartir con los estudiantes.

Para los profesores:

- Mantener el secreto de los datos- guía de actividades – Versión en español.
- Mantener el secreto de los datos- ejemplar

Vocabulario

- **Descifrar**: para cambiar la información para que se muestre su significado oculto.
- **Cifrar**: para cambiar la información de modo que su significado quede oculto.

Estrategia de aprendizaje

El mensaje sirve para iniciar la revisión de lo que alguien necesita en un sistema de codificación. Los estudiantes deben entender que, sin conocer el sistema utilizado para codificar la secuencia en binario, no tienen forma de saber lo que significa.

Conocimiento inicial (5 min)

Muestre la cadena binaria de Code Studio nivel 2.

Dirija a los estudiantes a los Niveles de Code Studio correspondientes a la lección

Preguntar: Aquí hay un ejemplo de un mensaje que alguien podría enviar por Internet a un amigo. ¿Qué necesitas para decodificar este mensaje?

Observaciones: En las últimas actividades, hemos visto muchos tipos de datos diferentes que se pueden codificar en binario. Sin embargo, todos nuestros sistemas de codificación tienen un par de cosas en común.

Revisión: Revise brevemente las características de un sistema de codificación:

1. Necesita ser inequívoco.
2. Todos deben estar de acuerdo.

Permita que los estudiantes intercambien ideas para mantener el mensaje en secreto. En la mayoría de los casos, los estudiantes pueden pensar en usar un código secreto en lugar de uno públicamente disponible. Esto podría funcionar, pero es mucho trabajo hacer un nuevo código para cada tipo de datos, y tendrías que repetir ese trabajo si su código fuera revelado accidentalmente.

Muestra la cadena binaria y la clave de decodificación en Code Studio nivel 3.

Niveles de Code Studio

Dé tiempo a los estudiantes para decodificar la secuencia binaria y discutan lo que creen que significa.

Preguntar: ¿Qué pasaría si quisiera enviar un mensaje secreto, para que sólo mi amigo lo pudiera entender?

Hoy vamos a ver un sistema que nos permitirá mantener todo tipo de mensajes en secreto.

Ampliación del conocimiento (40 min)

Grupo: Pon a los estudiantes en parejas.

Distribuye Mantener el secreto de los datos- guía de actividades (Versión en español) para cada alumno.

Reducir el papel: Esta lección se puede hacer en línea. En lugar de colorear en los cuadros, los estudiantes pueden escribir una “X” en cada cuadro que sería de color negro.

Codificación y decodificación

Observaciones: Este es el mismo sistema que vimos antes, pero

con más emojis. Con tu compañero, decodifica la secuencia binaria y decide qué crees que significa el mensaje.

Permita que los estudiantes compartan lo que han encontrado y sus propias interpretaciones de los emojis.

Cifrado y descifrado

Observaciones: La siguiente cadena binaria utiliza el mismo código emoji que vio antes, pero el remitente no quería que otras personas lo leyeran. Con su pareja, intente descifrar el mensaje.

Permite que los estudiantes intenten descifrar el mensaje. Pueden notar que los códigos binarios no están en el sistema de codificación que se les ha dado.

Observaciones: Este mensaje ha sido encriptado. Eso significa que alguien lo cambió para que no podamos leerlo. Para leer el mensaje, primero debemos descifrarlo.

Vocabulario: Introduce los siguientes términos:

Encriptar: Para cambiar la información de modo que su significado esté oculto

- Alguien ha cifrado el mensaje, por lo que no podemos entenderlo.

Descifrar: Para cambiar la información para que se muestre su significado oculto

- Necesitamos descifrar el mensaje antes de poder leerlo.

Modela el descifrado del primer mensaje.

1. Copie el resto de la cadena binaria en la primera fila del cuadro.

2. Continúe repitiendo la tecla hasta que hayas llegado al final del cuadro. (La última repetición solo tendrá dos bits).

3. Para cada bit en la tercera fila del gráfico, coloree en el cuadrado si y sólo si los dos bits encima son iguales. Por ejemplo, si los dos bits superiores son blancos O ambos negros, coloree en el cuadrado. No coloree en el cuadrado si los dos bits son diferentes.

Una vez que el mensaje ha sido descifrado, permite que los estudiantes lo decodifiquen y hablen sobre lo que piensan que significa.

Recorrer la sala: Apoye a los estudiantes mientras descifran el mensaje en la segunda página.

Los estudiantes pueden no entender la diferencia entre la codificación / decodificación y el cifrado / descifrado. Lo principal para que los estudiantes entiendan es que las intenciones entre los dos son muy diferentes.
La codificación se usa para cambiar la forma de los datos, no para ocultar su significado a los demás.
Por ejemplo, ASCII se utiliza para codificar caracteres en binario, pero la intención es que todos puedan decodificar la información. El objetivo es facilitar la tarea de almacenar y procesar información. El cifrado se utiliza para garantizar que solo el destinatario de la información pueda leerlo, Se usa para seguridad y privacidad.

En este sistema de encriptación, el método de cifrado y descifrado es idéntico y utiliza la misma clave. En la mayoría de los sistemas de encriptación, ese no es el caso. Esta vez ha sido elegido por el mismo de simplicidad.

Para compartir el mensaje en línea, los estudiantes pueden escribir “B” para cada cuadrado negro y “W” para cada cuadrado blanco en la fila.

Encripta tu propio mensaje

Los estudiantes crean sus propios mensajes emoji y claves, luego los codifican y los encriptan.

Los estudiantes deben publicar sus mensajes encriptados públicamente, mientras mantienen en secreto sus mensajes y claves no encriptados. Permita que los estudiantes miren los mensajes de sus compañeros de clase e intenten descifrarlos sin una clave.
Indicación: Todos han compartido sus datos encriptados. ¿Crees que podrías descifrar los datos de alguien sin la clave? ¿Cómo? ¿Qué lo hace difícil?

Junte diferentes grupos y pida que intercambien claves secretamente. Deberían poder descifrar el mensaje del otro grupo. Permita que cada uno de los grupos comparta el mensaje emoji que descifraron y lo que creen que significa.

El objetivo de esta discusión es resaltar el valor de cifrado, y que incluso con el conocimiento de algoritmo, es difícil descifrar un código sin la clave. Permita a los estudiantes la oportunidad de compartir sus ideas sobre cómo descifrar este código y probarlo. Luego, pídales a los estudiantes que digan qué es lo que lo dificulta.

Reflexión

Indicación: ¿Cómo mantuviste tu llave segura al dársela a tu pareja?

El alumno debería compartir cómo se aseguraron de que nadie más pudiera ver la clave que usaban para encriptar sus datos.

Observaciones: Utilizaste la seguridad física para mantener tu llave segura, asegurándote de que nadie pudiera acceder físicamente a ella.

Inducir: ¿De qué manera utiliza la seguridad física para mantener seguros sus datos en línea?

Permita que los estudiantes discutan las preguntas con sus compañeros antes de compartirlos con la clase.

Observaciones: Para mantener nuestros datos seguros, debemos prestar atención a la seguridad digital y física. La seguridad digital incluye el uso de encriptación o protección de cosas con contraseñas. La seguridad física mantiene nuestros dispositivos y contraseñas físicamente seguros.

El objetivo de la primera discusión es introducir la idea de la seguridad física, que incluye todo lo que hacemos en el mundo físico, como la prevención del acceso físico a computadoras y contraseñas.
Los estudiantes deben entender que la seguridad física es tan importante como la seguridad digital cuando salvaguardan la información. Algunas cosas que pueden hacer los estudiantes para mantener su información segura puede ser guardar las contraseñas en un lugar seguro (o evitar escribirlas por completo) y mantener los dispositivos bloqueados cuando no estén en uso.

Transferencia del conocimiento (5 min)

Indicación: Cuando las personas se comunican en Internet, no pueden confiar en la seguridad física para mantener sus claves seguras. Trata de pensar en una forma en que todavía puedan comunicarse de forma segura, incluso si alguien pudiera leer todo lo que le enviaron.

Permita que los estudiantes realicen una lluvia de ideas, luego compartan sus ideas con un compañero de clase.

Sugerencias para evaluar

Se sugieren los siguientes indicadores para evaluar formativamente los aprendizajes:

- Aplican varios métodos de encriptación para modelar la transmisión segura de información
- Identifican los derechos propios como los de los otros, y aplican estrategias de protección de la información en ambientes digitales.