Martinez Orozco Victor Manuel

Investigación 06

Serialización

¿Qué es y para qué sirve la serialización?

Primeramente, la serialización es un proceso fundamental en la programación que permite convertir datos o estructuras de datos

Una de las principales utilidades de la serialización es la comunicación entre sistemas distribuidos

Esto permite transferir datos de manera eficiente entre diferentes sistemas o aplicaciones en diferentes lugares geográficos, con arquitecturas heterogeneas o que utilicen diferentes lenguajes de programación

Además, la serialización se utilica para el almaceramiento de datos en medios persistentes. Permíte guardar objetos o estructuras de datos en archivos en disco, para así su posterior recuperación, procesamiento o analisis.

La serialización también se utilica en aplicaciones en tiempo real, donde la transmisión y el procesamiento de datos son críticos, como en sistemas de mensajería o aplicaciones de procesamiento de datos en directo

Martínez Orozco Víctor Manuel

Tipos de serialización

Binaria: Esta serialización convierte los datos en una representación como su nombre lo menciona "binaria". Esta usualmente es utilizada por los terminos de eficiencia que implica, pues no incluye etiquetas o marcas de formato y portanto el espacio y tiempo de procesamiento es eficiente.

Se utiliza en aplicaciones cuando el tamaño o velocidad de procesamiento se consideran importantes.

Detexto: Este convierte los datos en un formato más amigable con lo humanos. Por obvias razones, este serializado es más grande y menos eficiente que el binario. Practicamnte hace lo contrario al binario, pues incluye etiquetas y marcas de formato para representar los datos.

Martinez Orozco Victor Manuel

Serialización en formato de archivo:

Este tipo de serialización almacena los datos en un formato de archivo en específico. Esto para que, posterior a su serializado de formato, pueda ser procesado/leído por aplicaciones que entiendan tal formato de archivo especificado. Usualmente se recurre a este serializado cuando se usan aplicaciones que requieren almacenamiento y recuperación de datos en disco.

De protocolo: Tal cual como su nombre lo dice; los datos se serializan en un formato especifico que cumple con un protocolo de comunicación acordado. Practicamente se utiliza en sistemas que requieren comunicación entre diferentes componentes.

¿Cuál es la necesidad de crear algoritmos de encriptacion?

- Privacidad: Garantiza que nadie puede leer las comunicaciones o datos excepto el destinatario o el propietario legítimo de los datos.

Martinez Orozco Victor Manuel

Seguridad: Previene la fuga de datos, ya que si un equipo/dispositivo se pierde o es robado y el disco donde se almacena información importante esta encriptado correctamente, nadie más que el propietario puede descifrarlos.

En otras palabras, protegen la confidencialidad, integridad, privacidad de la información entre la comunicación entre redes.

- Algoritmo cesar

Un poco de su historia: Este cifrado recibe su nombre en honor a Julio Cesar, un politico y militar romano de Siglo I antes de Cristo, quien usaba el algoritmo con un desplazamiento de 3 espacios para proteger sus mensajes importantes de contenido militar.
"Esto es, si tenía que decir algo importante, lo escribía usando el cifrado, cambiando el orden de las letras del alfabeto para que ninguna palabra pudiera entenderse. Si alguien quería decodificarlo, tenía que sustituir la cuarta letra del alfabeto, es decir, la D por la A y así hasta terminar el texto.

Éste algoritmo entonces fue creado/ conocido desde el siglo I AC.

Se conoce tambien como cifrado por desplazamiento, código Cesar o desplazamiento Cesor. Como su nombre lo menciona, sustituye una letra reemplazando por otra letra que se encuentra un número fijo de posiciones más adelante

Para codificar un mensaje simplemente se debe buscar cada letra de la línea del texto original y escribir la letra correspondiente a la línea codificada, o sea, la letra ubicada X lugares antes o después, claro que para decodificarla se hace el mismo procedimiento de codificación empleado pero al revés.

Algoritmo Xor

El cifrado Xor o cifrado Vernam, es una tecnica de cifrado que se basa en la operación Xor entre un mensaje y una clave secreta para producir un mensaje cifrado.

Esta técnica fue inventada por Gilbert Vernam, un ingeniero de la empresa AT&T

El cifrado XOR es un cifrado de flyo, lo que significa que cifra un flyo continuo de datos en lugar de bloques de datos fijos. Para cifrar un mensaje, el algoritmo toma cada bit del mensaje y lo combina con el bit correspondiente de la clave secreta utilizando la operación XOR

Operación XOR

Esta es una operación lógica binaria que se utiliza en muchos campos. Toma dos bits como entrada y produce un bit de salida

Entrada A	Entrada B	Salida
0	0	0
0	1	1
1	0	1
1	1	0

El resultado entonces es el bit cifrado correspondiente en el mensaje cifrado. Para descifrar el mensaje, se aplica la misma operación XOR utilizando la misma clave secreta

Bibliografía

- colaboradores de Wikipedia. (2023). Cifrado César. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar
- González, A. (2020, 27 octubre). ¿Qué es el cifrado César y cómo funciona? Ayuda Ley Protección Datos. https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/
- KeepCoding, R. (2023, 20 marzo). ¿Qué es el cifrado XOR? | KeepCoding Bootcamps. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-el-cifrado-xor/
- EcuRed. (s. f.). Cifrado Xor - EcuRed. https://www.ecured.cu/Cifrado_Xor
- Gewarren. (2023, 15 febrero). Serialización: .NET. Microsoft Learn. https://learn.microsoft.com/es-es/dotnet/standard/serialization/
- KathleenDollard. (2023, 15 febrero). Serialización - Visual Basic. Microsoft Learn. https://learn.microsoft.com/es-es/dotnet/visual-basic/programming-guide/concepts/serialization/