www.eysglobal.com

MÓDULO 1
TEMA 12:
REVISIÒN DEL CHECKSUM

REVISIÒN DEL CHECKSUM

Llamada **suma de chequeo** o ***checksum***), , esquema simple de detección de errores, donde cada mensaje transmitido es acompañado con un valor numérico basado en el número de grupo de bits del mensaje. Es decir un algoritmo de corrección de errores.

REVISIÒN DEL CHECKSUM

Es una importante practica, para el mantenimiento e integridad de los datos, a través de diferentes procedimientos y dispositivos como medios de almacenamiento confiables, se usa para verificar que un archivo compartido a un usuario es idéntico bit a bit al publicado en su fuente original .

REVISIÒN DEL CHECKSUM

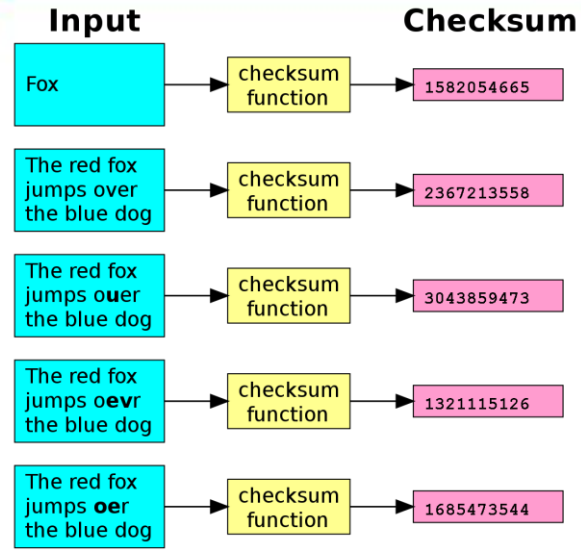
Las funciones de suma de comprobación están relacionadas con funciones hash , huellas digitales , funciones de aleatorización y funciones hash criptográficas . Sin embargo, cada uno de esos conceptos tiene diferentes aplicaciones y, por lo tanto, diferentes objetivos de diseño. Por ejemplo, una función que devuelve el inicio de una cadena puede proporcionar un hash apropiado para algunas aplicaciones, pero nunca será una suma de comprobación adecuada. Las sumas de comprobación se utilizan como primitivas criptográficas en algoritmos de autenticación más grandes. Para sistemas criptográficos con estos dos objetivos de diseño específicos

BYTE DE PARIDAD O PALABRA DE PARIDAD

El algoritmo de suma de control más simple es el llamado control de paridad longitudinal , que divide los datos en "palabras" con un número fijo n de bits, y luego calcula la exclusiva o (XOR) de todas esas palabras. El resultado se adjunta al mensaje como una palabra adicional. Para comprobar la integridad de un mensaje, el receptor calcula la exclusiva o de todas sus palabras, incluida la suma de comprobación; si el resultado no es una palabra que consta de n ceros, el receptor sabe que ocurrió un error de transmisión.

COMPLEMENTO DE SUMA

Una variante del algoritmo anterior es sumar todas las "palabras" como números binarios sin signo, descartando los bits de desbordamiento y anexar el complemento a dos del total como suma de comprobación. Para validar un mensaje, el receptor agrega todas las palabras de la misma manera, incluida la suma de verificación; si el resultado no es una palabra llena de ceros, debe haber ocurrido un error. Esta variante también detecta cualquier error de un solo bit, pero la suma promodular se usa en SAE J1708



SUMA DE COMPROBACIÓN DIFUSA

La idea de la suma de comprobación difusa se desarrolló para la detección de correo no deseado mediante la creación de bases de datos cooperativas de varios ISP de correo electrónico sospechoso de ser spam. El contenido de dicho correo no deseado a menudo puede variar en sus detalles, lo que haría que la suma de comprobación normal fuera ineficaz. Por el contrario, una "suma de comprobación difusa" reduce el texto del cuerpo a su mínimo característico y luego genera una suma de comprobación de la manera habitual. Esto aumenta en gran medida las posibilidades de que los correos electrónicos no deseados ligeramente diferentes produzcan la misma suma de comprobación.

REVISIÒN DEL CHECKSUM

Su funcionalidad está basada en un sencillo algoritmo de verificación que permite crear pequeños **hash** o cadenas de caracteres que luego pueden ser usados para verificar antes o después de una transmisión de datos, la validez de los datos transmitidos. Dicho hash generalmente está ubicado en la parte final del archivo o cadena verificado. Y de esta forma, sirven como una firma que ayudar a verificar la integridad de la información.

HISTORIA DEL CHECKSUM

La aparición de la primeras funciones CheckSum datan de los trabajos iniciales de **William Wesley Peterson**, un científico computacional y matemático que dedicó varios años a la investigación, diseño e implementación de las primeras CheckSum del mundo. Más específicamente, Peterson diseño la primera función CheckSum o de suma de verificación, en el año de 1961, la conocida **CRC** (Verificación por redundancia cíclica), que luego daría vida a estándares industriales como CRC8 o CRC32C, entre otras derivadas de muy amplio uso.

COMO FUNCIONA EL CHECKSUM

La función CheckSum fue creada a partir de la aplicación de un algoritmo sencillo. Este tiene como objetivo utilizar una serie de operaciones matemáticas y lógicas complejas para convertir una la secuencia de datos en una cadena de números fija conocida como **hash de suma de verificación.**

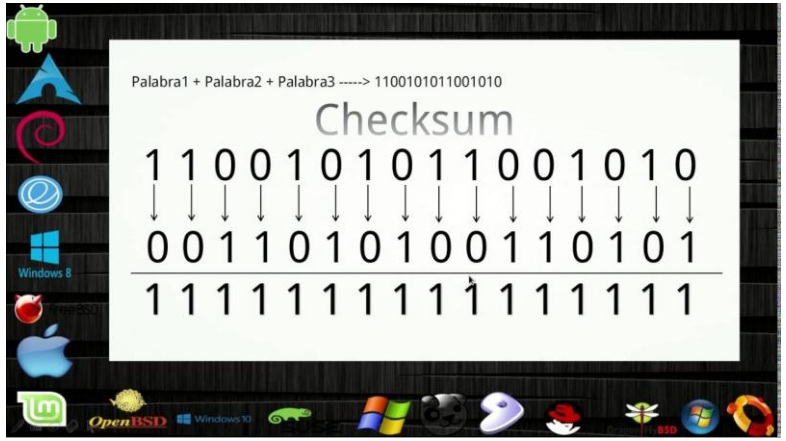
Este pequeño hash se utiliza luego para verificar de forma muy rápida si una determinada data ha sufrido daños. Bien sea por almacenamiento (datos escritos o leídos de forma incorrecta) o por transmisión de los mismo (las redes de transmisión siempre tienen una pérdida relacionada a distintos factores). O inclusive si algun actor malicioso la ha modificado de forma premeditada.

CASOS DE USO DE LA FUNCIÓN CHECKSUM

Los casos de uso de las funciones CheckSum son ampliamente variados. Como ya hemos mencionado son partes muy fundamentales en los aparatos electrónicos y de la informática en general. Pero con el fin de que puedas comprender con mayor claridad el alcance de las mismas veremos a continuación algunos casos de uso reales y muy cotidianos de estas funciones:

TECNOLOGÍA GSM

La tecnología GSM que hace posible que podamos usar la mayoría de nuestros celulares en la actualidad hace un amplio uso de las funciones checksum en sus sistemas de transmisión digital de voz y datos. Recordemos que la información digital que se envía a la red celular va codificada, comprimida y modulada de tal forma que la misma pueda llegar de un punto a otro en la red celular con la menor pérdida de información y calidad.



CUENTAS BANCARIAS

Otro uso muy común de las funciones de checksum es el de verificar que la información de una cuenta bancaria es correcta. Cada vez que vez un número de cuenta bancaria no solo ves un grupo de números que te identifican dentro de ese banco. Sino que también está un dato que les permite verificar que esos números que has entregado son los correctos.

Por ejemplo, en las cuentas bancarias del tipo IBAN, estos números de control o checksum son los primero cuatro dígitos. Los primeros dos indican el país de origen de la cuenta, y los otros dos indican el número de control. Este número de control está relacionado con los últimos 10 números que identifican la cuenta bancaria. Y esto nos garantizan que, no nos equivocaremos al introducir un número de cuenta bancaria.

DIRECCIONES DE CRIPTOMONEDAS

A través de la función CheckSum o suma de verificación usted podrá comprobar rápida y fácilmente que la dirección que está utilizando es la correcta. O si por el contrario, está alterada de alguna manera. Evitando enviar de forma inconsciente sus criptomonedas a una dirección falsa, incorrecta o inexistente.

Aunque, en teoría, sería imposible enviar bitcoins a una dirección que no existe o que este escrita de forma incorrecta. Debido a que estas direcciones cuando son generadas incorporan un código de suma de control. Este dato representa el valor hash de la dirección y los datos de la suma conforman un esquema alfanumérico propio conocido como **Base58Check**.