Implementación de algoritmo de salsa20

Einar Naim Aguilar Santana

Daniel Alejandro Barbosa Ayala

Axel Daniel Macias Heredia

Sebastian Rodríguez Hernández

Reporte de investigación

19 de mayo de 2023

Algoritmos de cifrado

Los algoritmos de cifrado ayudan a prevenir el fraude de datos. Estos algoritmos son parte de los protocolos de gestión de riesgos de cualquier empresa y a menudo se encuentran en aplicaciones de software.

Ayudan en el proceso de transformación de texto sin formato en texto cifrado y luego de vuelta a texto sin formato con el fin de proteger los datos electrónicos cuando se transportan a través de redes.

El cifrado desempeña un papel importante en la protección de muchos tipos diferentes de activos de tecnología de la información El cifrado se usa comúnmente para proteger los datos en tránsito y los datos en reposo.

- **Confidencialidad:** codifica el contenido del mensaje.
- **Autenticación:** verifica el origen de un mensaje.
- **Integridad:** demuestra que el contenido de un mensaje no ha cambiado desde que se envió.
- **No rechazo:** evita que los remitentes nieguen haber enviado el mensaje cifrado.

El objetivo principal del cifrado es proteger la confidencialidad de los datos digitales almacenados en los sistemas informáticos o transmitidos por Internet o cualquier otra red informática.

Tipos de cifrado:

Claves simétricas: datos en reposo

En la criptografía de cifrado simétrico, se utiliza la misma clave de cifrado para cifrar y descifrar los datos.

Claves asimétricas: datos en movimiento

Las claves asimétricas, por otro lado, son un par de claves para el cifrado y descifrado de los datos. Ambas claves están relacionadas entre sí y se crean al mismo tiempo

Por bloques

El cifrado de bloque procesa la entrada de texto claro en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño para cada bloque de entrada

El criptoanálisis es el estudio de métodos para obtener el significado de la información encriptada**,** sin acceso a la información secreta que normalmente se requiere para hacerlo.

Cifrado de Flujo- Salsa20

Es un cifrado de flujo que esta construido por una función pseudo-aleatoria basada en 32-bit, además de una adición bit a bit (XOR) y las operaciones de rotación, que asigna un 256- bit clave, un 64-bit nonce y una posición de corriente de 64-bit a una salida de 512-bit.

Esta elección de las operaciones se evita la posibilidad de ataques de temporización en las implementaciones de software.

El estado inicial se compone de 8 palabras clave, de 2 palabras de la posición de corriente, 2 palabras de nonce, y 4 palabras fijas. 20 rondas de mezcla producir 16 palabras de salida de flujo de cifrado.

Cada ronda consta de cuatro cuartos de vuelta operaciones, realizadas en cualquiera de las columnas o las filas del Estado de 16 palabras, dispuestas como un 4 × 4 matriz. Cada 2 rondas, el patrón se repite. Cada cuarto de vuelta modifica 4 palabras.

Fuentes:

https://ciberseguridad.com/servicios/algoritmos-cifrado/