Universidad Autónoma de Chiapas

Facultad de contaduría y Administración Campos 1

Licenciatura en Sistemas Computacionales

Presenta: Charly Aquino Vázquez

Programación de Aplicaciones Web

Lic. Rigoberto Pérez Ovando

Mapa conceptual “Algoritmos de encriptación”

Tarea 12

UNIDAD 4

5°J

Tuxtla Gutiérrez Chiapas a 12 de noviembre del 2023

Algoritmos de encriptación

Rijndael(AES)

La encriptación se realiza con una clave de 128, 192 o 256 bits, lo que garantiza una mayor seguridad contra los ataques de fuerza bruta.

Este método puede utilizarse tanto para el intercambio seguro de claves como para la transmisión de datos con una longitud de 128 o 256 bits.

Un algoritmo de cifrado es un método matemático, según el cual se fundamenta la conversión de los datos.
Password Depot utiliza el algoritmo de encriptación Rijndael o AES (Advanced Encryption Standard) para encriptar sus datos confidenciales.
Este algoritmo de seguridad se explica con más detalle a continuación.

Procedimiento

Rijndael vuelve a generar 10 claves de 128 bits a partir de la clave de 128 bits brindada.
Estos se almacenan en tablas de 4 x 4.
El texto plano también se divide en tablas de 4 x 4 (cada una en trozos de 128 bits).
Cada una de las piezas de texto plano de 128 bits se procesa en un proceso de 10 rondas (10 rondas con claves de 128 bits, 11 en 192, 13 en 256).
Por lo tanto, el código se genera después de la décima ronda.
Cada byte individual es sustituido en una caja S y reemplazado por el recíproco sobre GF (2 8).
Posteriormente, se aplica una matriz de módulo 2 en formato binario y se realiza una operación XOR en el 63.
Las filas de las matrices se ordenan cíclicamente.
Luego las columnas se intercambian por multiplicación de la matriz a través de un campo de Galois (GF) (2 8).
Se aplica un enlace XOR a la subclave para cada ronda.
La seguridad de este método de cifrado aumenta cuando Rijndael se realiza varias veces con diferentes claves circulares.

Blowfish

Blowfish es un codificador de bloques simétricos, diseñado por Bruce Schneier en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado.

Blowfish usa bloques de 64 bits y claves que van desde los 32 bits hasta 448 bits. Es un codificador de 16 rondas Feistel y usa llaves que dependen de las Cajas-S. Tiene una estructura similar a CAST-128, el cual usa Cajas-S fijas.

La función divide las entrada de 32 bits en 4 bloques de 8 bits, y usa los bloques como entradas para las cajas-S. Las salidas deben estar en módulo 232 y se les aplica un XOR para producir la salida final de 32 bits.

Diagrama de la función F de Blowfish
Debido a que Blowfish está en la red Feistel, puede ser invertido aplicando un XOR entre P17 y P18 al bloque texto codificado, y así sucesivamente se usan las P-entradas en orden reversivo.

Generacion de claves:

La generación de claves comienza inicializando los P-arrays y las cajas-S con los valores derivados de los dígitos hexadecimales de pi, los cuales no contienen patrones obvios. A la clave secreta se le aplica un XOR con las P-entradas en orden (ciclando la clave si es necesario). Un bloque de 64 bits de puros ceros es cifrado con el algoritmo como se indica. El texto codificado resultante reemplaza a P1 y P2. Entonces el texto codificado es cifrado de nuevo con las nuevas subclaves, P3 y P4 son reemplazados por el nuevo texto codificado. Esto continúa, reemplazando todas las entradas del P-array y todas las entradas de las cajas-S. En total, el algoritmo de cifrado Blowfish correrá 521 veces para generar todas las subclaves, cerca de 4KB de datos son procesados.

Twofish

Twofish es un método de criptografía simétrica con cifrado por bloques desarrollado por Counterpane Labs y presentado al concurso del NIST que buscaba un sustituto para DES (el concurso AES). El tamaño de bloque en Twofish es de 128 bits y el tamaño de clave puede llegar hasta 256 bits.

Twofish se relaciona con el método de cifrado por bloques anterior Blowfish. Las características distintivas de Twofish son el uso de S-boxes pre-computadas con llaves dependientes, y una llave-horario relativamente compleja. Twofish coge prestados algunos elementos de otros diseños: por ejemplo, el Pseudo-Hadamard transforman (PHT) de la familia SAFER de cifrado. Twofish utiliza la misma estructura de Feistel que el DES.

3DES

DES es un algoritmo de clave simétrica basado en una red Feistel. Como cifrado de clave simétrica, utiliza la misma clave para los procesos de cifrado y descifrado. La red de Feistel hace que ambos procesos sean casi exactamente iguales, lo que da como resultado un algoritmo que es más eficiente de implementar.

En 3DES, el algoritmo DES se ejecuta tres veces con tres claves; sin embargo, solo se considera seguro si se utilizan tres claves separadas.

Usos

Microsoft Office
Firefox
Sistemas de pago EMV

El Instituto Nacional de Estándares y Tecnología (NIST) ha publicado un borrador de propuesta que dice que todas las formas de 3DES quedarán obsoletas en 2023 y no se permitirán a partir de 2024. Aunque es solo un borrador, la propuesta significa el final de una era, por lo que es el momento de pasar a otros algoritmos más seguros.

BIBLIOGRAFIA

- Darmstadt, D-64295. (2023). *¿Cómo funciona el algoritmo de encriptación Rijndael?* Password Depot. https://www.password-depot.de/es/saber-como/blowfish-y-rijndael.htm#:~:text=Un%20algoritmo%20de%20cifrado%20es,con%20m%C3%A1s%20detalle%20a%20continuaci%C3%B3n.
- *¿Qué es el cifrado 3DES y cómo funciona? | Ciberseguridad*. (2022). Ciberseguridad. https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-3des/
- *Wikiwand - Blowfish*. (2021). Wikiwand; Wikiwand. https://www.wikiwand.com/es/Blowfish
- *Wikiwand - Twofish*. (2023). Wikiwand; Wikiwand. https://www.wikiwand.com/es/Twofish