Tecnológico de Costa Rica.

Escuela de Ingeniería en Computación.

IC: 7602-Redes - 2 Semestre 2022.

2018086509 - Jocxan Sandí Batista.

Resumen #6 y #7

Capítulo 8

8.2 Algoritmos de Clave Simétrica

Estos algoritmos utilizan la misma clave para encriptar y desencriptar.

8.2.1 DES—El Estándar de Encriptación de Datos

Se utilizó ampliamente en la industria para usarse con productos de seguridad. Y actualmente no es seguro en su forma original, pero aún es útil en una forma modificada.

El funcionamiento: El texto llano se encripta en bloques de 64 bits, produciendo 64 bits de texto cifrado. El algoritmo, que se parametriza mediante una clave de 56 bits, tiene 19 etapas diferentes.

Blanqueamiento (whitening): Una técnica que algunas veces se utiliza para hacer a DES más fuerte que consiste en aplicar un OR exclusivo a una clave aleatoria de 64 bits con cada bloque de texto llano antes de alimentarla al DES y después aplicar un OR exclusivo a una segunda clave de 64 bits con el texto cifrado resultante antes de transmitirla.

8.2.2 AES—El Estándar de Encriptación Avanzada

Rijndael utiliza sustitución y permutaciones, así como múltiples rondas. El número de rondas depende del tamaño de clave y del tamaño de bloque, y es de 10 para las claves de 128 bits con bloques de 128 bits y aumenta hasta 14 para la clave o el bloque más grande. La función rijndael tiene tres parámetros: plaintext, un arreglo de 16 bytes que contiene los datos de entrada; ciphertext, un arreglo de 16 bytes a donde se regresará la salida cifrada, y key, la clave de 16 bytes.

Pasos:

- El arreglo state se inicializa al texto llano y se modifica en cada paso en el cálculo.
- El código inicia expandiendo la clave en 11 arreglos del mismo tamaño que el estado.
- Se copiael texto llano en el arreglo state a fin de poder procesarlo durante las rondas.
- se aplica OR exclusivo ark[0] dentro de state, byte por byte.
- Se gira a la izquierda cada una de las cuatro filas. La fila 0 se gira 0 bytes, la fila 1 se gira 1 byte, la fila 2 se gira 2 bytes y la fila 3 se gira 3 bytes.

- Se mezcla cada una de las columnas independientemente de las demás.
- Por último, se aplica OR exclusivo a la clave de esta ronda dentro del arreglo state.

8.2.3 Modos de cifrado

Modo de libro de código electrónico

La forma directa de utilizar el DES para cifrar una pieza grande de texto llano es dividirla en bloques consecutivos de 8 bytes y encriptarlos después uno tras otro con la misma clave. La última pieza de texto llano se rellena a 64 bits, en caso de ser necesario. Esta técnica se conoce como Modo de Libro de Código Electrónico.

Modo de encadenamiento de bloques de cifrado

Funcionamiento: A cada bloque de texto llano se le aplica un OR exclusivo con el bloque anterior de texto cifrado antes de ser encriptado. En consecuencia, el mismo bloque de texto llano ya no corresponde con el mismo bloque de texto cifrado, y la encriptación deja de ser un enorme cifrado de sustitución monoalfabética.

Modo de retroalimentación de cifrado

Para la encriptación byte por byte, modo de retroalimentación de cifrado, se utiliza (triple) DES, sólo se utiliza un registro de desplazamiento de 128 bits. La desencriptación con el modo de retroalimentación de cifrado hace lo mismo que la encriptación. El contenido del registro de desplazamiento se encripta, no se desencripta, a fin de que el byte seleccionado al cual se le aplica el OR exclusivo.

Modo de cifrado de flujo

La secuencia de bloques de salida, llamada flujo de claves, se trata como un relleno de una sola vez y se le aplica OR exclusivo con el texto llano para obtener el texto cifrado.

Funcionamiento:

- Funciona encriptando un vector de inicialización y usando una clave para obtener un bloque de salida.
- Se encripta este bloque usando la clave para obtener un segundo bloque de salida.
- Este bloque se encripta para obtener un tercer bloque, y así sucesivamente.

La desencriptación se realiza generando el mismo flujo de claves en el lado receptor. Puesto que el flujo de claves depende sólo del IV y de la clave, no le afectan los errores de transmisión en el texto cifrado.

Modo de contador

Solución al acceso aleatorio a datos encriptados.

Funcionamiento: Se encripta el vector de inicialización más una constante, y al texto cifrado resultante se le aplica un OR exclusivo con el texto llano. Al incrementar en 1 el vector de inicialización por cada nuevo bloque.

8.2.5 Criptoanálisis

Criptoanálisis diferencial

Esta técnica puede utilizarse para atacar cualquier cifrado en bloques; empieza con un par de bloques de texto llano que difieren sólo en una cantidad pequeña de bits y observando cuidadosamente lo que ocurre en cada iteración interna a medida que avanza la encriptación.

Criptoanálisis lineal

Funcionamiento: Aplica un OR exclusivo a ciertos bits del texto llano y el texto cifrado en conjunto y buscando patrones en el resultado.

8.3 Algoritmos de Clave Publica

Clase de criptosistema, en el que las claves de encriptación y desencriptación son diferentes y la clave de desencriptación no puede derivarse de la clave de encriptación.

8.3.1 El algoritmo RSA

Se requiere alguna forma de encadenamiento para la encriptación de datos. Sin embargo, en la práctica la mayoría de los sistemas basados en RSA usan criptografía de clave pública principalmente para distribuir claves de sesión de una sola vez para su uso con algún algoritmo de clave simétrica.

Bibliografía

> Tanenbaum, A. (2003). Computer Networks (4ta edición ed.). NJ: Prentice Hall.