Tecnológico de Costa Rica
Escuela de Ingeniería en Computación
IC: 7602-Redes - 2 Semestre 2022
2018093728 - Paula Mariana Bustos Vargas

Resumen 6 y 7

8.2 ALGORITMOS DE CLAVE SIMÉTRICA

La primera clase de algoritmos de encriptación que analizaremos en este capítulo se conocen como algoritmos de clave simétrica porque utilizan la misma clave para encriptar y desencriptar.

La primera clase de algoritmos de encriptación que analizaremos en este capítulo se conocen como algoritmos de clave simétrica porque utilizan la misma clave para encriptar y desencriptar. cifrados en bloques, que toman un bloque de n bits de texto llano como entrada y lo transforman utilizando la clave en un bloque de n bits de texto cifrado.

8.2.1 DES—El Estándar de Encriptación de Datos

DES (Estándar de Encriptación de Datos), se adoptó ampliamente en la industria para usarse con productos de seguridad.

La primera etapa es una transposición, independiente de la clave, del texto llano de 64 bits. La última etapa es el inverso exacto de esta transposición. El algoritmo se ha diseñado para permitir que la desencriptación se haga con la misma clave que la encriptación.

La razón para encriptar, desencriptar y luego encriptar de nuevo es la compatibilidad hacia atrás con los sistemas DES de una sola clave.

8.2.2 AES—El Estándar de Encriptación Avanzada

En enero de 1997, los investigadores de todo el mundo fueron invitados a emitir propuestas para un nuevo estándar, se llamaría AES (Estándar de Encriptación Avanzada). Las reglas fueron:

1. El algoritmo debe ser un cifrado de bloques simétricos.
2. Todo el diseño debe ser público.
3. Deben soportarse las longitudes de claves de 128, 192 y 256 bits.
4. Deben ser posibles las implementaciones tanto de software como de hardware.
5. El algoritmo debe ser público o con licencia en términos no discriminatorios.

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 (64 bits) 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.

Modo de encadenamiento de bloques de cifrado

Todos los cifrados en bloques pueden encadenarse de varias formas a fin de que el reemplazo de un bloque de la forma en que lo hizo Leslie cause que el texto llano se desencripte comenzando en el bloque reemplazado que se desechará.

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. Al primer bloque se le aplica un OR exclusivo con un IV (Vector de Inicialización) elegido de manera aleatoria, que se transmite (en texto llano) junto con el texto cifrado

Modo de retroalimentación de cifrado

Se utiliza (triple) DES, AES la idea es exactamente la misma; sólo se utiliza un registro de desplazamiento de 128 bits.

Un problema con el modo de retroalimentación de cifrado es que si un bit del texto cifrado se invierte de manera accidental durante la transmisión, se dañarán los 8 bytes que se desencriptan mientras el byte incorrecto se encuentra en el registro de desplazamiento.

Modo de cifrado de flujo

Existen aplicaciones en las que un error de transmisión de 1 bit que arruina 64 bits de texto llano es demasiado.

Funciona encriptando un vector de inicialización y usando una clave para obtener un bloque de salida. A continuación se encripta este bloque usando la clave para obtener un segundo bloque de salida. A continuación este bloque se encripta para obtener un tercer bloque, y así sucesivamente. La secuencia (arbitrariamente grande) 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,

Modo de contador

El texto llano no se encripta en forma directa. En su lugar, 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, es más fácil desencriptar un bloque en cualquier parte del archivo sin tener que desencriptar primero todos sus predecesores.

8.2.4 Otros cifrados

DES y Rijndael son los algoritmos criptográficos de clave simétrica más conocidos. Tambien se encuentran: Blowfish, DES, IDEA, RC4, RC5, Rijndael, Serpent, Tiple DES, Twolish

8.2.5 Criptoanálisis

Criptoanálisis diferencial (Biham y Shamir, 1993). Esta técnica puede utilizarse para atacar cualquier cifrado en bloques

Criptoanálisis lineal (Matsui, 1994). Éste puede descifrar el DES con sólo 2 43 textos llanos conocidos. Funciona aplicando un OR exclusi- vo a ciertos bits del texto llano y el texto cifrado en conjunto y buscando patrones en el resultado. Al hacerse repetidamente, la mitad de los bits deben ser 0s y la otra mitad 1s.

Análisis del consumo de energía eléctrica para averiguar las claves secretas. Las computadoras por lo general utilizan 3 voltios para representar un bit 1 y 0 voltios para representar un bit 0.

Análisis de temporización. Los algoritmos criptográficos están llenos de instrucciones if que prueban bits en las claves de ronda. Si las partes then y else toman diferentes cantidades de tiempo, reduciendo la velocidad del reloj y viendo el tiempo que tardan en ejecutarse varios pasos, también podría ser posible deducir las claves de ronda. Una vez que se conocen todas las claves de ronda, por lo general puede calcularse la clave original. Los análisis de energía y temporización también pueden utilizarse de manera simultánea para facilitar el trabajo.

8.3 ALGORITMOS DE CLAVE PÚBLICA

Surge el problema de de si un intruso puede robar la clave, el sistema no vale nada no importa lo robusto que sea un criptosistema.

Los criptólogos siempre daban por hecho que las claves de encriptación y desencriptación eran la misma . Pero la clave tenía que distribuirse a todos los usuarios del sistema.

En 1976, dos investigadores de la Universidad de Stanford, Diffie y Hellman , propusieron una clase nueva de criptosistema, en el que las claves de encriptación y desencriptación eran diferentes y la clave de desencriptación no podía derivarse de la clave de encriptación.

En su propuesta, el algoritmo de encriptación , E, y el algoritmo de desencriptación , D, tenían que cumplir con los tres requisitos siguientes. En estas condiciones, no hay razón para que una clave de encriptación no pueda hacerse pública. El algoritmo de encriptación y la clave de Alice se hacen públicos, de ahí el nombre de criptografía de clave pública. Por ejemplo, Alice podría poner su clave pública en su página de inicio en Web.

Utilizaremos la notación EA para denotar el algoritmo de encriptación parametrizado por la clave pública de Alice. De manera similar, el algoritmo de desencriptación parametrizado por la clave privada de Alice es D A. Se supone que tanto la clave de encriptación de Alice, EA, como la clave de encriptación de Bob, EB, están en un archivo de lectura pública. Bob entonces lo desencripta aplicando su clave secreta DB . Nadie más puede leer el mensaje encriptado, E B, porque se supone que el sistema de encriptación es robusto y porque es demasiado difícil derivar DB de la EB públicamente conocida.

Consistentemente nos referimos a estas claves como claves públicas y privadas, respectivamente, y las distinguiremos de las claves secretas usadas en la criptografía convencional de clave simétrica.

8.3.1 El algoritmo RSA

Es conocido por las iniciales de sus tres descubridores (Rivest, Shamir, Adleman): RSA. Ha sobrevivido a todos los intentos para romperlo por más de un cuarto de siglo y se le considera muy robusto.

Su método se basa en ciertos principios de la teoría de los números. Seleccionar dos números primos grandes, p y q . Con estos parámetros calculados por adelantado, estamos listos para comenzar la encriptación. Dividimos el texto llano en bloques, para que cada mensaje de texto llano, P, caiga en el intervalo 0 P < n.

Esto puede hacerse agrupando el texto llano en bloques de k bits, donde k es el entero más grande para el que 2k < n es verdad. Puede demostrarse que, para todos los P del intervalo especificado, las funciones de

encriptación y desencriptación son inversas. Para ejecutar la encriptación, se necesitan e y n. La seguridad del método se basa en la dificultad para factorizar números grandes.

Equipado con el conocimiento de z y de e, puede encontrar d usando el algoritmo de Euclides. Afortunadamente, los matemáticos han estado tratando de factorizar números grandes durante los últimos 300 años, y las pruebas acumuladas sugieren que se trata de un problema excesivamente difícil. 1025 años de tiempo de cómputo utilizando el mejor algoritmo conocido y una computadora con un tiempo de instrucción de 1 μseg. Un ejemplo pedagógico trivial del algoritmo RSA se muestra en la figura 8-17.

El texto cifrado, C, de un mensaje de texto llano, P, se da por la regla C = P3 . El receptor desencripta el texto cifrado de acuerdo con la regla P = C7 . Afortunadamente, los matemáticos han estado tratando de factorizar números gran-des durante los últimos 300 años, y las pruebas acumuladas sugieren que se trata de un problema excesivamente difícil. El receptor desencripta el texto cifrado de acuer-do con la regla P = C7.

Dado que los números primos escogidos para este ejemplo son tan pequeños, P debe ser menor que 33, por lo que cada bloque de texto llano puede contener sólo un carácter. Por tanto, 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 como el AES o el triple DES.

El RSA es demasiado lento para poder encriptar grandes volúmenes de datos, pero se utiliza con amplitud para la distribución de claves.

8.3.2 Otros algoritmos de clave pública

Aunque el RSA se usa ampliamente, de ninguna manera es el único algoritmo de clave pública conocido. El primer algoritmo de clave pública fue el de la mochila . Con ciertas restricciones adicionales, el problema de determinar una lista posible de los objetos a partir del peso dado se consideró no computable, y formó la base del algoritmo de clave pública.

Otros esquemas de clave pública se basan en la dificultad para calcular logaritmos discretos.