Resumen 4 y 5

Adriana López Calderón

2019293588

ALGORITMOS DE CLAVE SIMÉTRICA

La criptografía moderna usa las mismas ideas básicas que la criptografía tradicional (la transposición y la sustitución), pero su orientación es distinta. Tradicionalmente, los criptógrafos han usado algoritmos. Hoy día se hace lo opuesto: el objetivo es hacer el algoritmo de encriptación tan complicado y rebuscado que incluso si el criptoanalista obtiene cantidades enormes de texto cifrado a su gusto, no será capaz de entender nada sin la clave.

Los algoritmos de clave simétrica utilizan la misma clave para encriptar y desencriptar, los 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. Los algoritmos criptográficos pueden implementarse ya sea en hardware (para velocidad) o en software (para flexibilidad).

Las transposiciones y las sustituciones pueden implementarse mediante circuitos eléctricos sencillos,caja P (la P significa permutación), que se utiliza para efectuar una transposición de una entrada de 8 bits. Si los 8 bits se designan de arriba hacia abajo como 01234567, la salida de esta caja P en particular es 36071245.

DES—El Estándar de Encriptación de Datos

El DES (Estándar de Encriptación de Datos), se adoptó ampliamente en la industria para usarse con productos de seguridad. Ya no es seguro en su forma original, pero aún es útil en una forma modificada. Ahora explicaremos el funcionamiento del DES.

Una técnica que algunas veces se utiliza para hacer a DES más fuerte se conoce como blanqueamiento (whitening). 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. El blanqueamiento puede eliminarse fácilmente mediante la ejecución de las operaciones inversas (si el receptor tiene las dos claves de blanqueamiento). Puesto que esta técnica agrega más bits a la longitud de la clave, provoca que una búsqueda completa del espacio de claves consuma mucho más tiempo. Observe que se utiliza la misma clave de blanqueamiento para cada bloque (es decir, sólo hay una clave de blanqueamiento).

Triple DES

En 1979, IBM se dio cuenta de que la longitud de la clave DES era muy corta y diseñó una forma de incrementarla de manera efectiva, utilizando cifrado triple. El método elegido, que desde entonces se ha incorporado en el Estándar Internacional 8732, se utilizan dos claves y tres etapas. En la primera etapa, el texto llano se encripta mediante DES de la forma usual con K1. En la segunda etapa, DES se ejecuta en modo de desencriptación, utilizando K2 como la clave. Por último, se realiza otra encriptación DES con K1. La razón para encriptar, desencriptar y luego encriptar de nuevo es la compatibilidad hacia atrás con los sistemas DES de una sola clave.

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, que se llamaría AES (Estándar de Encriptación Avanzada). Las reglas fueron:

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

Los finalistas y sus puntajes fueron los siguientes:

1. Rijndael (de Joan Daemen y Vincent Rijmen, 86 votos).
2. Serpent (de Ross Anderson, Eli Biham y Lars Knudsen, 59 votos).
3. Twofish (de un equipo encabezado por Bruce Schneier, 31 votos).
4. RC6 (de los Laboratorios RSA, 23 votos).
5. MARS (de IBM, 13 votos).

Rijndael

Se basa en la teoría de campos de Galois, la cual da algunas propiedades verificables de seguridad. Sin embargo, también puede verse como código C, sin meterse a las matemáticas. Al igual que el DES, 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. Sin embargo, a diferencia del DES, todas las operaciones involucran bytes completos, para permitir implementaciones eficientes tanto en hardware como en software

Modos de cifrado

El AES (o el DES o, de hecho, cualquier cifrado de bloques) es básicamente un cifrado de sustitución monoalfabética que utiliza caracteres grandes (caracteres de 128 bits para el AES y caracteres de 64 bits para el DES). Siempre que el mismo bloque de texto llano entra en la etapa inicial, el mismo bloque de texto cifrado sale de la etapa final. Si encripta 100 veces el texto llano abcdefgh con la misma clave DES, obtiene 100 veces el mismo texto cifrado. Un intruso puede aprovechar esta propiedad para violar el cifrado.

Modo de libro de código electrónico

Para ver cómo puede utilizarse esta propiedad de cifrado de sustitución monoalfabética para vencer parcialmente el cifrado, utilizaremos el (triple) DES porque es más fácil diseñar bloques de 64 bits que de 128 bits, pero el AES tiene exactamente el mismo problema. 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. Esta técnica se conoce como modo ECB (modo de Libro de Código Electrónico) en analogía con los libros de código pasados de moda en los que se listaba cada palabra de texto llano, seguida por su texto cifrado (por lo general, un número decimal de cinco dígitos).

Modo de encadenamiento de bloques de cifrado

Para frustrar este tipo de ataque, 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. Una forma de encadenar es el encadenamiento de bloques de cifrado.

Modo de retroalimentación de cifrado

El encadenamiento de bloques tiene la desventaja de que requiere la llegada de un bloque completo de 64 bits antes de que pueda comenzar la desencriptación. Este modo no es adecuado para terminales interactivas, en las que se pueden escribir líneas máximo de ocho caracteres y es necesario detenerse a esperar una respuesta. Para la encriptación byte por byte, modo de retroalimentación de cifrado, se utiliza (triple) DES.

La desencriptación con el modo de retroalimentación de cifrado hace lo mismo que la encriptación. En particular, 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 con C10 para obtener P10 sea el mismo al que se le aplicó el OR exclusivo con P10 para generar C10 en primera instancia. Siempre y cuando los dos registros de desplazamiento permanezcan idénticos, la desencriptación funcionará de manera correcta

Modo de cifrado de flujo

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.

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

Un problema que todos los modos tienen, excepto el modo de libro de código electrónico, es que el acceso aleatorio a datos encriptados es imposible. Por ejemplo, suponga que un archivo se transmite a través de una red y después se almacena en disco de forma encriptada. Ésta sería una forma razonable de operar si la computadora receptora fuera una computadora portátil con riesgo de ser robada. Almacenar todos los archivos importantes de forma encriptada reduce en gran medida el potencial daño que se podría sufrir por la información confidencial que se fugaría en caso de que la computadora cayera en las manos equivocadas.

Otros cifrados

DES y Rijndael son los algoritmos criptográficos de clave simétrica más conocidos. Sin embargo, vale la pena mencionar que se han diseñado otros cifrados de clave simétrica. Algunos de ellos están incluidos en varios productos. En la figura 8-16 se listan algunos de los más comunes.

Criptoanálisis

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

- El criptoanálisis lineal (Matsui, 1994). Éste puede descifrar el DES con sólo 243 textos llanos conocidos. Funciona aplicando un OR exclusivo a ciertos bits del texto llano y el texto cifrado en conjunto y buscando patrones en el resultado.
- El 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. Por lo tanto, procesar un 1 gasta más energía eléctrica que procesar un 0.
- El 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

ALGORITMOS DE CLAVE PÚBLICA

En 1976, dos investigadores de la Universidad de Stanford, Diffie y Hellman (1976), 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 (con clave), E, y el algoritmo de desencriptación (con clave), D, tenían que cumplir con los tres requisitos siguientes. Estos requisitos pueden expresarse sencillamente como sigue:

1. D(E(P)) = P.
2. Es excesivamente difícil deducir D de E.
3. E no puede descifrarse mediante un ataque de texto llano seleccionado.

El algoritmo RSA

RSA ha sobrevivido a todos los intentos para romperlo por más de un cuarto de siglo y se le considera muy robusto. Mucha de la seguridad práctica se basa en él. Su mayor desventaja es que requiere claves de por lo menos 1024 bits para una buena seguridad (en comparación con los 128 bits de los algoritmos de clave simétrica), por lo cual es muy lento. Su método se basa en ciertos principios de la teoría de los números. Ahora resumiremos el uso del método; para los detalles, consulte el trabajo original.

1. Seleccionar dos números primos grandes, *p* y *q* (generalmente de 1024 bits).
2. Calcular $n = p \times q$ y $z = (p - 1) \times (q - 1)$.
3. Seleccionar un número primo con respecto a z, llamándolo d.
4. Encontrar *e* tal que $e \times d = 1 \bmod z$

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 (Merkle y Hellman, 1978). La idea aquí es que alguien es dueño de una gran cantidad de objetos, todos con pesos diferentes. El dueño cifra el mensaje seleccionando secretamente un subgrupo de los objetos y colocándolos en la mochila. El peso total de los objetos contenidos en la mochila se hace público, así como la lista de todos los objetos posibles. La lista de los objetos que se metieron en la mochila se mantiene en secreto. 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. El Gamal (1985) y Schnorr (1991) han inventado algoritmos basados en este principio. Existen algunos otros esquemas,

como los basados en curvas elípticas (Menezes y Vanstone, 1993), pero las dos categorías principales son las basadas en la dificultad para factorizar números grandes y calcular logaritmos discretos módulo un número primo grande. Estos problemas se consideran verdaderamente difíciles de resolver porque los matemáticos han estado trabajando en ellos durante años sin adelantos importantes.