Nombre de alumno:

Teresa Méndez Pérez

Nombre del profesor:

Mireya del Carmen García Alfaro

Nombre del trabajo:

Ensayo

Materia:

Redes de computadoras III

Grado: 7 cuatrimestre

Comitán de Domínguez Chiapas a 29 de septiembre del 2021

INTRODUCCION

En este ensayo se abordaran cinco temas relacionados al tema de “algoritmos de claves simétricas”, pero ¿qué quiere decir este término? Se dice que es una clave segura si se sabe utilizarla, también se sabe que es muy utilizada para cifrar una gran cantidad de información sin riesgo de ser vista, actualmente en uso son cifrados de bloque: esto significa que cifran los datos bloque por bloque.

Se abordara el tema DES (Algoritmo de Encriptación Estándar) un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. Puede decirse que es una de las versiones más anteriores y con el paso del tiempo se necesitó otro tipo de cifrado con mayor seguridad.

También se tratara el siguiente tema AES, se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloque de datos de 16 bytes, que se repiten varias veces. Lo que en la actualidad se dice que es el mejor sistema de cifrado incapaz de ser descifrado, lo que ha llevado a ser utilizado por bancos e incuso la NASA.

Otro tema importante son los modos de cifrado, pero ¿Qué es un modo de cifrado? Los algoritmos de cifrado de bloque como DES o AES separan el mensaje en pedazos de tamaño fijo, por ejemplo de 64 o 128 bits. La forma en que se gestionan estos pedazos o bloques de mensaje, se denomina “modo de cifrado”.

Con respecto a los dos últimos temas, los dejare en suspenso para poder investigar un poco, ya que no tengo una idea clara sobre estos temas, se relacionan entre sí, pero prefiero buscar una definición concreta de estos temas y puntos a tratar.

Procederemos a la investigación de los temas antes mencionados, esperando que la información que posteriormente se presentara sea del agrado y comprensión de todos, pasare a la explicación de los temas.

ALGORITMOS DE CLAVES SIMETRICAS

2.1 DES- EL ESTANDAR DE ENCRIPTACION DE DATOS

El principio central de DES se basa en la operación matemática XOR. Conocemos una propiedad básica de la operación XOR A XOR B = C; C XOR B = A. Esta función es muy similar al proceso de cifrado y descifrado. A se cifra con la clave secreta B para obtener C y C se descifra con la clave secreta B para obtener A.

DES se basa en el cifrado de bloques de datos. Divide los datos que se van a cifrar en varios bloques de datos en unidades de 64 bits. Luego dos iteraciones:
La iteración de la capa externa es la iteración entre bloques de datos. Los métodos de iteración incluyen ECB, CBC, etc. Este artículo se centra en CBC.

La iteración interna se realiza a través de la red Feistel.
El proceso iterativo de cifrado y descifrado de bloques de datos basados en CBC se muestra en la figura anterior. El proceso de cifrado y descifrado de cada bloque de datos depende del bloque de datos anterior. Una vez que haya un error en un bloque de datos, habrá un "efecto de avalancha".

Antes de que comience la iteración de Feistel, el bloque de datos de 64 bits se divide en 32 bits izquierdo y derecho, y luego se realiza el proceso iterativo como se muestra en la figura anterior, un total de 16 iteraciones. La subclave de cada iteración es diferente. Cada proceso de iteración utiliza el procesamiento de funciones redondas (cifrado) en la mitad derecha del bloque de datos. Por lo tanto, aquí hay dos cuestiones involucradas: 1. Cómo generar la subclave, 2. Cómo implementar la función de ronda

En términos generales, la lógica de implementación de la generación de subclases y la lógica de implementación de la función redonda es más complicadas, consulte mi código para la implementación.

2.2 AES- EL ESTANDAR DE ENCRIPTACION AVANZADA

AES no es precisamente Rijndael (aunque en la práctica se los llama de manera indistinta) ya que Rijndael permite un mayor rango de tamaño de bloques y longitud de claves; AES tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado.

AES opera en una matriz de 4×4 bytes, llamada state (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state).

Hasta 2005, no se ha encontrado ningún ataque exitoso contra el AES. La Agencia de Seguridad Nacional de los Estados Unidos (NSA) revisó todos los finalistas candidatos al AES, incluyendo el Rijndael, y declaró que todos ellos eran suficientemente seguros para su empleo en información no clasificada del gobierno de los Estados Unidos.

Funcionamiento

Pseudocódigo

- Expansión de la clave usando el esquema de claves de Rijndael.
- Etapa inicial:

1. AddRoundKey

- Rondas:

1. SubBytes — en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.
2. ShiftRows — en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.
3. MixColumns — operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.

4. AddRoundKey — cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.

- Etapa final:

1. SubBytes
2. ShiftRows
3. AddRoundKey

Conforme el paso del tiempo la tecnología ha estado avanzando enormemente y con ello la necesidad de proteger la información delicada, ya que conforme se encontró nuevos métodos para ocultar información de terceros, también se encontraba la manera de descifrar y obtener dicha información. Es de gran importancia el avance logrado en la seguridad de los datos, la creación de este algoritmo AES tomó mucho tiempo y trabajo para los criptólogos. Aunque el riesgo de que exista un fallo en la seguridad del algoritmo existe según el paso del tiempo se ha demostrado como sigue siendo un cifrado altamente seguro.

2.3 MODOS DE CIFRADO

Los algoritmos de cifrado de bloque como DES o AES separan el mensaje en pedazos de tamaño fijo, por ejemplo de 64 o 128 bits. La forma en que se gestionan estos pedazos o bloques de mensaje, se denomina "modo de cifrado".

ECB ha sido estandarizado por el NIST (U.S. National Institute for Standards and Technology). Este modo de cifrado es el más simple de todos, pues se limita a partir el mensaje en bloques y cifrarlos por separado.

Entre las ventajas de este método destaca la posibilidad de romper el mensaje en bloques y cifrarlos en paralelo o el acceso aleatorio a diferentes bloques.

Sin embargo, las desventajas de este modo de cifrado son enormes, por lo que se usa cada vez menos. El hecho de cifrar los bloques por separado implica que cuando se cifre un bloque con cierto valor, siempre se obtendrá el mismo resultado. Esto hace posible los ataques de diccionario.
Además, cuando se cifran varios bloques y se envían por un canal inseguro, es posible que un adversario elimine ciertos bloques sin ser detectado, o que capture algunos bloques y los reenvíe más adelante.

CBC ha sido estandarizado por el NIST (U.S. National Institute for Standards and Technology). Este modo de cifrado es una extensión de ECB que añade cierta seguridad. El modo de cifrado CBC divide el mensaje en bloques y usa XOR para combinar el cifrado del bloque anterior con el texto plano del bloque actual. Como no se dispone de un texto cifrado con el que combinar el primer bloque, se usa un vector de inicialización IV (número aleatorio que puede ser públicamente conocido). El uso del vector de inicialización es importante, pues de no usarlo, podría ser susceptible de ataques de diccionario. También es necesario que el IV sea aleatorio y no un número secuencial o predecible.

Entre las desventajas de este modo de cifrado destaca la necesidad de realizar el cifrado de forma secuencial (no puede ser paralelizado). También hay que tener en cuenta la posibilidad de realizar ataques de reenvío de un mensaje entero (o parcial).

Mientras que **ECB y CBC** son modos basados en bloques, CTR simula un cifrado de flujo. Es decir, se usa un cifrado de bloque para producir un flujo pseudo aleatorio conocido como keystream. Este flujo se combina con el texto plano mediante XOR dando lugar al cifrado.
Para generar el keystream se cifra un contador combinado con un número aleatorio mediante ECB y se va incrementando. El valor del contador puede ser públicamente conocido, aunque es preferible guardarlo en secreto. Es necesario que el valor de nonce+contador lo conozcan ambos lados de la comunicación.

Entre las ventajas de CTR destaca la posibilidad de pre calcular el keystream (y/o trabajar en paralelo), el acceso aleatorio al keystream o que revela poquísima información sobre la clave.

Como desventajas hay que tener en cuenta que reutilizar un contador en la misma clave puede ser desastroso, pues se generará de nuevo el mismo keystream.
Modificar bits en el texto plano es muy sencillo, pues modificando un bit del cifrado se modificará el bit del texto plano correspondiente .Por lo que es adecuado usar este modo de cifrado junto con una verificación de la integridad del mensaje.

OFB ha sido estandarizado por el NIST (U.S. National Institute for Standards and Technology). Como CTR es otro cifrado de flujo. En este caso el keystream se genera cifrando el bloque anterior del keystream, dando lugar al siguiente bloque. El primer bloque de keystream se crea cifrando un vector de inicialización IV. OFB comparte muchas de las características de CTR, pero CTR tiene beneficios adicionales, por lo que OFB se usa bastante poco.
En OFB se pueden pre calcular los keystream (aunque no se puede realizar en paralelo) y a diferencia de CTR no da problemas al ser usado con cifrados de bloque de 64 bits. Además, como en el caso de CTR, revela muy poca información sobre la clave.

También comparte con CTR sus desventajas: reutilizar un contador en la misma clave puede ser desastroso y permite Bit-flipping attacks.

CFB ha sido estandarizado por el NIST (U.S. National Institute for Standards and Technology) y es muy similar a OFB. Para producir el keystream cifra el último bloque de cifrado, en lugar del último bloquedel keystrema como hace OFB.

Como en OFB reutilizar un contador en la misma clave puede ser desastroso y permite Bit-flipping attacks. En CFB el cifrado no puede ser paralelizado, pero el descifrado si. Igual que en el caso anterior, es preferible usar CTR.

2.4 OTROS CIFRADOS

Cifrado por transposición o permutación

Cada letra (o carácter) se intercambia por otra del mensaje, reordenando de algún modo las letras, pero no *disfrazándolas*. Para este tipo de cifrado se usan multitud de métodos, como colocar las letras en una matriz de una manera y *sacarlas* de otra manera diferente.

Cifrado Vernam

Según el principio de Kerkhoff todos los algoritmos de cifrados y descifrados deben ser públicos y conocidos por todos, lo único secreto es la clave del algoritmo, esta clave se convierte en la piedra angular del algoritmo.
Basándose en este principio, el cifrado perfecto (el cifrado Vernam) debe ser público con su clave en secreto y ésta debe tener la misma longitud del mensaje, ser generada aleatoriamente y solamente puede ser usada una sola vez.
Para cifrar el mensaje se realiza una operación XOR *(or exclusivo)* entre el mensaje y la clave.
Como se puede observar este método sería perfecto de no ser porque cada clave generada aleatoriamente debería ser generada también aleatoriamente e idéntica a la del emisor, por el receptor del mensaje, algo que en principio es muy difícil.

2.4 CRIPTOANALISIS

Es la ciencia opuesta a la criptografía quizás no es muy afortunado hablar de ciencias opuestas, sino más bien de ciencias complementarias, ya que si ésta trata principalmente de crear y analizar criptosistemas seguros, la primera intenta romper esos sistemas, demostrando su vulnerabilidad: dicho de otra forma, trata de descifrar los criptogramas. El término descifrar siempre va acompañado de discusiones de carácter técnico, aunque asumiremos que descifrar es conseguir el texto en claro a partir de un criptograma, sin entrar en polémicas de reversibilidad y solidez de criptosistemas.

En el análisis para establecer las posibles debilidades de un sistema de cifrado, se han de asumir las denominadas condiciones:

- El criptoanalista tiene acceso completo al algoritmo de encriptación
- El criptoanalista tiene una cantidad considerable de texto cifrado
- El criptoanalista conoce el texto en claro de parte de ese texto cifrado. También se asume generalmente el Principio de Kerckhoffs, que establece que la seguridad del cifrado ha de residir exclusivamente en el secreto de la clave, y no en el mecanismo de cifrado.

Objetivos de sistemas

Aunque para validar la robustez de un criptosistemas normalmente se suponen todas las condiciones del peor caso, existen ataques más específicos, en los que no se cumplen

todas estas condiciones. Cuando el método de ataque consiste simplemente en probar todas y cada una de las posibles claves del espacio de claves hasta encontrar la correcta, nos encontramos ante un ataque de fuerza bruta o ataque exhaustivo. Si el atacante conoce el algoritmo de cifrado y sólo tiene acceso al criptograma, se plantea un ataque sólo al criptograma; un caso más favorable para el criptoanalista se produce cuando el ataque cumple todas las condiciones del peor caso; en este caso, el criptoanálisis se denomina de texto en claro conocido. Si además el atacante puede cifrar una cantidad indeterminada de texto en claro al ataque se le denomina de texto en claro escogido; este es el caso habitual de los ataques contra el sistema de verificación de usuarios utilizado por Unix, donde un intruso consigue la tabla de contraseñas generalmente /etc/passwd y se limita a realizar cifrados de textos en claro de su elección y a comparar los resultados con las claves cifradas a este ataque también se le llama de diccionario, debido a que el atacante suele utilizar un fichero `diccionario' con los textos en claro que va a utilizar. El caso más favorable para un analista se produce cuando puede obtener el texto en claro correspondiente a criptogramas de su elección; en este caso el ataque se denomina de texto cifrado escogido

Algoritmo de cifrado

El algoritmo de cifrado, para ser considerado seguro, ha de soportar todos estos ataques y otros no citados; sin embargo, en la criptografía, como en cualquier aspecto de la seguridad, informática o no, no debemos olvidar un factor muy importante: las personas. El sistema más robusto caerá fácilmente si se tortura al emisor o al receptor hasta que desvelen el contenido del mensaje, o si se le ofrece a uno de ellos una gran cantidad de dinero; este tipo de ataques (sobornos, amenazas, extorsión, tortura...) se consideran siempre los más efectivos

Utilidades

Criptoanálisis también se utiliza para referirse a cualquier intento de sortear la seguridad de otros tipos de algoritmos y protocolos criptográficos en general, y no solamente el cifrado. Sin embargo, el criptoanálisis suele excluir ataques que no tengan como objetivo primario los puntos débiles de la criptografía utilizada; por ejemplo, ataques a la seguridad que se basen en el soborno, la coerción física, el robo, el keylogging y demás, aunque estos tipos de ataques son un riesgo creciente para la seguridad informática, y se están haciendo gradualmente más efectivos que el criptoanálisis tradicional

El criptoanálisis es el arte de descifrar comunicaciones encriptados sin conocer las llaves correctas. Existen muchas técnicas criptoanalíticas. Algunas de las más importantes se describen a continuación

Esta es la situación en la cual el atacante no conoce nada sobre el contenido del mensaje, y debe trabajar solo desde el texto cifrado. En la práctica es muy probable hacer tantas conjeturas acerca del texto plano, como cantidad de tipos de mensajes tengan un encabezado similar
Incluso las cartas y los documentos ordinarios comienzan de una manera muy previsible. Por ejemplo, muchos ataques clásicos utilizan análisis frecuencial del texto cifrado, sin embargo, no funciona bien contra los cifrados modernos
Los criptosistemas modernos no son débiles contra ataques de texto cifrado, aunque algunas veces son considerados con el agregado de que el mensaje contiene "tendencia" estática

El atacante conoce o puede adivinar el texto de alguna parte del texto cifrado. La tarea es desencriptar el resto del bloque cifrado utilizando esta información. Esto puede ser hecho determinando la clave utilizada para encriptar la información, o a través de algún atajo
Uno de los mejores ataques modernos de texto plano conocido es el criptoanálisis lineal contra cifradores de bloques

El atacante puede tener cualquier texto encriptado con una llave desconocida. La tarea es determinar la llave utilizada para encriptar. Un buen ejemplo de este ataque es el criptoanálisis diferencial que puede ser aplicado a cifradores de bloques y, en algunos casos, a funciones Hash
Algunos criptosistemas, particularmente el RSA, son vulnerables a estos ataques. Cuando tales algoritmos son utilizados, se debe tener cuidado en el diseño de la aplicación (o protocolo) de forma tal que un atacante no pueda obtener el texto encriptado

Este ataque es relevante para las comunicaciones criptográficas y los protocolos de intercambio de llaves. La idea es que cuando dos partes, A y B, están intercambiando llaves por comunicaciones seguras por ejemplo utilizando Diffie-Hellma, un adversario intruso se posiciona entre A y B en la línea de comunicación. El intruso intercepta las señales que A y B se envían, y ejecuta un intercambio de llaves entre A y B. A y B

terminaran utilizando llaves diferentes, cada una de las cuales es conocida por el intruso. El intruso puede luego desencrespar cualquier comunicación de A con la llave que comparte con A, y luego reenviarla a B encrestándola nuevamente con la llave que comparte con B. Ambos A y B pensarán que se están comunicando en forma segura pero de hecho el intruso está escuchando todo.

Como Prevenir

La forma habitual de prevenir este ataque es utilizar un sistema de clave pública capaz de proveer firmas digitales.

- Por configuración, las partes deben conocer de antemano la clave pública de cada una de ellas.
- Después de que han sido generadas, las partes se envían firmas digitales.
- El hombre de por medio falla en el ataque a causa de que no es capaz de falsificar las firmas sin conocer las llaves privadas utilizadas para generar las firmas.
- Este medio es suficiente si existe también una manera segura de distribuir claves públicas. *Una forma es la jerarquía de certificados como X.509. Es utilizado por ejemplo en IP Sec.

La correlación entre la clave secreta y la salida del criptosistema es la fuente principal de información para el criptoanálisis. En el caso más simple, la información sobre la llave secreta es filtrada por el criptosistema. Casos más complicados requieren estudios sobre la correlación básicamente, cualquier relación que no sería esperada entre la información observada o tomada de los criptosistemas y la información de la llave adivinada

Teorías

Por ejemplo, en ataques lineales contra bloques cifrados el criptoanálisis estudia el texto plano conocido y el observado. Adivinando algunos bits del criptosistema el analista determina, por correlación entre el texto plano y el cifrado, si el "adivinó bien". Esto se puede repetir y tiene muchas variantes.
El criptoanálisis diferencial introducido por Eli Biham y Adi Shamir en los '80 fue el primer ataque que utilizó completamente esta idea contra los bloques cifrados. Más tarde Eli Biham y Adi Shamir introducen el criptoanálisis lineal que fue aún más efectivo contra el DES. Más recientemente, se han desarrollado nuevos ataques que utilizan ideas

similares.
La idea correlacionar es fundamental para la criptografía y muchas investigaciones han tratado de construir criptosistemas que sean seguros contra tales ataques. Por ejemplo, Knudsen y Nyberg han estudiado esta seguridad contra el criptoanálisis diferencial.

Se han aplicado ideas similares a una gran variedad de algoritmos y dispositivos. Es así necesario que los dispositivos criptográficos sean diseñados para ser altamente resistentes a fallas y contra introducciones maliciosas de fallas por criptoanálisis

CONCLUCION

Para finalizar este trabajo, menciono que gran parte de la información la obtuve de la antología y otras de internet, las páginas que visite las dejare hasta abajo para poder corroborar la información y veracidad de este trabajo.

Como en un principio mencione en los primeros temas, tenía un poco de idea de la criptologia ya que sé, que en ocasiones es muy difícil de extraer la información y si se extrae en algunas ocasiones no tenemos toda la información completa y en otros casos toda la información es perdida por lo que no se puede acceder a ella.

En el tema de modos de cifrados existen diferentes tipos y cada uno de ellos tiene diferente utilidad algunas van de la mano pero con diferente función que en la actualidad se utilizan y la mayoría de las personas no sabíamos.

En el tema otros cifrados solo existen dos, y al comprar la información de la antología y en internet es lo mismo por eso no hubo que explicar y para mi si resulto un pequeño inconveniente puesto a que no sabía mucho sobre el tema y más si la información coincidía no había mucho de donde buscar.

Y con el último tema sobre el criptoanálisis, si resulto un tema muy amplio y no sabía exactamente que temas abordar, pero sobre todo me fui guiando de los temas que coincidían con la antología para no estar muy fuera de tema, por eso trate de relacionarlo, sinceramente si aprendí algo nuevo y sobre todo algo que es de suma importancia ya que es lo que prácticamente veré a lo largo de la carrera dentro y fuera de clases, de donde surgen estos problemas y con esta información ya podre dar respuesta a ciertas cosas

que nos ocurren en nuestros equipos y n sabemos cómo resolverlos, pero con esta información será un poco más fácil de resolverlo.

Sin más por agregar espero que este trabajo cumpla con las expectativas.

- www.elcodigok.com.ar
- www.ibiblio.org
- www.segu-info.com.ar
- www.cryptography.com