Escuela de Ingeniería en Computación

Redes IC-7602

Resumen #6-7 Cap 8.2, 8.3

Profesor: Nereo Campos

Estudiante: Mario Fernández Robert - 2018163975

Algoritmos de clave simétrica (Cap 8.2)

- Transposición(Permutación) y Sustitución como principales ideas de la criptografía moderna.
- Utilizan la misma llave para encriptar y desencriptar.
- Cifrados de bloques:
    - Input: Bloques de n bits de texto.
    - Output: Bloques de n bits de texto cifrado.
- Se puede hacer un cifrado de producto que consiste en una secuencia en cascada de permutaciones y sustituciones.
- Existen diferentes estándares de encriptación.

DES (Cap 8.2.1)

- Ya no es seguro en su forma original.
- En su momento se adoptó ampliamente.
- Especificaciones del algoritmo:
    - El texto se encripta en bloques de 64 bits.
    - Se parametriza mediante una llave de 56 bits.
    - Tiene 19 etapas distintas.
    - La primera etapa es una transposición.
    - La última etapa es el inverso exacto de esta transposición.
    - La penúltima etapa intercambia los 32 bits de la izquierda con los 32 bits de la derecha.
    - Las 16 etapas restantes son funcionalmente idénticas

Triple DES

- Especificaciones del algoritmo:
    - Consta de dos claves y tres etapas.

    - Se encripta el texto con DES y la llave K1.
    - Se desencripta el texto con DES y la llave K2.
    - Se vuelve a encriptar el texto con DES y la llave K1.

AES (Cap 8.2.2)

- Al acercarse DES al fin de su vida útil se decidió promover un concurso para que investigadores de todo el mundo emitieran propuestas para un nuevo estándar.
- Las reglas definidas 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 discriminatorios
- Se realizaron 15 propuestas y gano la de Rijndael (de Joan Daemen y Vincent Rijmen) con 86 votos.
- Especificaciones del algoritmo:
    - Las claves y los bloques tienen un tamaño de 128 a 256 bits en pasos de 32 bits
    - Se copia por columnas el mensaje en un arreglo denominado state
    - Las claves de ronda(rk[num]) se calculan mediante una rotación repetida y aplicado OR exclusivo a varios grupos de bits de clave.

Modos de cifrado (8.2.3)

- A pesar de la complejidad de AES y DES tienen una falla, si encripta 100 veces el texto llano abcdefgh con la misma clave DES, obtiene 100 veces el mismo texto cifrado.

Modo de libro de código electrónico

- Se divide un texto en grupos bloques de n bytes
- Se cifra cada uno con la misma clave

Modo de encadenamiento de bloques de cifrado

- A cada bloque de texto llano se le aplica un OR exclusivo con el bloque anterior de texto cifrado antes de ser encriptado.
- Al primer bloque se le aplica un OR exclusivo con un vector de inicialización de forma aleatoria, este se transmite en texto llano con el texto cifrado.

Modo de retroalimentación de cifrado

- Realiza la encriptación byte por byte
- Se utiliza un vector de inicialización

Modo de cifrado de flujo

- Usado cuando un error de transmisión de 1 bit arruina 64 bits de texto llano.

- Funciona encriptando un vector de inicialización y usando una clave para obtener un bloque de salida.
- El bloque se encripta, usado la clave para tener un segundo bloque de salida. Y así sucesivamente.
- Llamado flujo de claves, se trata como un relleno de una vez y se aplica un XOR con el texto llano para obtener el texto cifrado.

Modo de contador

- Desencripta bloques de manera no secuencial
- Se utiliza un vector de inicialización

Criptoanálisis (8.2.5)

Existen 2 tipos de criptoanálisis:

- Diferencial: puede utilizarse para atacar cualquier cifrado en bloques.
- Lineal: puede descifrar DES con solo 2 a la 43 textos llanos conocidos.
- Se puede realizar un análisis del consumo de energía para obtener información.
- Se puede realizar un análisis del tiempo que dura en procesar las claves de ronda para obtener información.

Algoritmos de clave pública (8.3)

- Utiliza una llave pública y una privada
- La llave pública puede ser conocida por un atacante sin ocasionar problemas
- Los usuarios encriptan con la llave pública y desencriptan con la llave privada.

El algoritmo RSA (8.3.1)

- Existe desde hace más de un cuarto de siglo.
- Extremadamente seguro.
- Su mayor desventaja es el tamaño de sus claves, 1024 bits.
- Se basa en la teoría de números.

Otros algoritmos de clave pública (8.3.2)

- Algoritmo de Mochila
    - Un dueño tiene una gran cantidad de objetos con pesos diferentes.
    - El dueño cifra el mensaje seleccionando secretamente un subgrupo de los objetos y los coloca en la mochila.
    - El peso total de los objetos en la mochila se hace público y la lista de todos los posibles objetos.
- Basados en calcular logaritmos discretos.
- Basados en curvas elípticas.