Instituto Tecnológico de Costa Rica
Escuela de Computación
Redes GR 2
Resumen 6 y 7
Profesor Gerardo Nereo Campos Araya
Estudiante Ary-El Durán Balestero
Fecha de entrega 8/11/2022

Algoritmos de Clave Simétrica

Usan la misma clave para encriptar y desencriptar.
Estos algoritmos pueden estar hechos en hardware para darle prioridad a la velocidad o en software para que termine siendo más flexible.
Cifrado de bloques: Se agarra un bloque de bits donde se usa llave para cifrarlo.

Caja P: Este dispositivo se encarga de realizar una trasposición de una entrada de 8 bits.

Caja S: Se encarga de realizar la sustitución, se va a reemplzarar los bits originales con bits cifrados.

DES - El Estándar de Encriptación de Datos

Este es un estándar creado por IBM que fue adoptado por estados unidos para el cifrado de información no secreta.

Etapas

- Primeta etapa: Transposición
- Otras etapas: Todas similares pero con parametrización diferente
- Penúltima etapa: Intercambiar las primeros 32 bits con los últimos
- Última etapa: Inverso de la transposición

Pasos

- Cosntruir un número de 48 bits
- Aplica un OR exclusivo
- División de las salidas en ocho grupos de 6 bits
- Se mapean las entradas a la caja S en una salida de 4 bits
- Los bits se pasan atravez de una caja P

Blanqueamiento: Aplicar un OR exclusivo a una clave aleatoria de 64 bits a la entrada y luego otra llave aleatoria de 64 bits en la salida.

Triple DES

Tras controversias causadas por este el DES, se decidió cambiar por uno de tres etapas que usa dos claves.

AES

Rijndael

Soporta longitud y tamaños de 126 a 256 bits de las claves con pasos de 32 bits Utiliza sustitución y permutaciones Pasos

- Las claves se producen por mediante una rotación y usando el OR exclusivo.
- Copiar el texto llano
- Aplicar XOR exclusivo byte por bute
- Girar a la izquierda cada una de las filas
- Mezclar las columnas de manera independiente
- Aplicar OR exclusivo a la clave

Modos de cifrado

El AES tiene el problema de que la misma entrada siempre va a producir la misma salida

Modo de libro de código electrónico

Este se encarga de dividir el texto en bloques y de ahi encriptar lo necesario. El problema en este caso es que se sabe que el programa se encarga de dividir la información en bloques, estos pueden ser reemplazados fácilmente.

Modo de encadenamiento de bloques de cifrado

Este encadena los bloques aplicando un OR exclusivo con el bloque anterior antes de que se encripte.
Al primer bloque se le aplica un OR exclusivo con un Vector de Inicialización que es aleatorio.

Modo de retroalimentación de cifrado

Aquí se aplica un cifrado byte por byte con DES hasta tener los 64 bits para la transmisión y se le aplica un OR al byte que se encuentre más a la izquierda.

Modo de cifrado de flujo

Se encripta un vector de inicialización usando una clave para conseguir un bloque de salida y de ahi se sigue encriptando con más claves, esto es el flujo de claves.

Modo de contador

Este método permite desencriptar los bloques de manera no secuencial Aquí se envreipta el vector de inicialización más una constante y luego se le aplica un OR exclusivo al texto.

Criptoanálisis

Criptoanalisis diferencial: Para atacar cualquier cifrado de bloques. Criptoanálisis lineal: Aplica OR esxclusivos a ciertos bits para encontrar patrones.

Algoritmos de Clave Pública

En este caso los programas de encriptación no usaran la misma clave para la encriptación y la decriptación.

El algoritmo RSA

Este es increiblemnete robusto pero es muy lento ya que necesita llaves de al menos 1024 bits Pasos

- Seleccionar dos números primos cuales sean grandes, estos se van a representar con p y q
- Realizar la formula n = p _ q y z = (p - 1) _ (q - 1)
- d = númoer primo con respecto a z
- Usar un e donde e * d = 1 mod z