Block Ciphers

Es un cifrado determinístico, utilizando un algoritmo de encriptado y otro de desencriptado. El algoritmo recibe una entrada que es una instancia de cierto número de bits y la salida tiene exactamente el mismo tamaño, pero cifrado, en resumidas cuentas: el input y el output del algoritmo deben ser del mismo tamaño.

Computacionalmente indistinguible

El cifrado de bloques no tiene memoria. Un cifrado de bloque se puede tomar como una caja negra que toma un valor y lo encripta o lo desencripta. Este sistema es seguro si la función de encriptado es computacionalmente indistinguible de cualquier otra operación computacional.

El adversario tiene que determinar si el challenger está utilizando un algoritmo matemático o si está usando una funcionalidad cualquiera para encriptar un texto. El adversario tiene que intuir si la salida está encriptada o si es solo ruido. Si el adversario no es capaz de adivinar si una salida está encriptada o no, entonces, nuestro sistema es seguro.

Implicaciones

- Un block cipher es impredecible
- El ser impredecible implica seguridad contra la recuperación de claves. Tratar de recuperar la clave es computacionalmente muy difícil.
- si E ε seguro contra una recuperación de clave, entonces el espacio de la clave debe ser muy grande.

Permutaciones aleatorias

Cuando el challenger elige una permutación aleatoria, la toma de un espacio enorme. En la práctica las permitaciones aleatorias pueden ser implementadas fácilmente en Lazy Mode.

Block ciphers para encriptado directo

Supongamos que tenemos un block cipher seguro. Queremos encriptar una cadena de bits muy larga, dividimos dicha cadena en bloques del mismo tamaño que el block cipher, de forma que vamos cifrando la cadena en secuencias de bloques (n0, n1,….nn). Cada bloque es encriptado con la misma clave secreta. Usar block cipher de esta manera es un proceso sin memoria ya que a pesar de que se usa la misma clave, cada bloque cifrado es diferente. Esto es conocido como Electronic CodeBook mode (ECB). En resumidas cuentas consiste en dividir una cadena en bloques e irlos encriptando uno a uno. A pesar de su seguridad, no es semánticamente seguro ya que un atacante puede distinguir unos mensajes de otros.

Data Encryption Standard (DES) & Advanced Encryption Standard (AES)

DES es un block cipher que usa claves y bloques con un input de 64 bits y una salida de 64 bits y una clave de cifrado de 56 bits. Lo malo es que en la actualidad ya no es lo suficientemente seguro, siendo retirado en 2021. Existe una variante de DES llamada 3DES que utiliza una clave de 168 Bits. AES utiliza claves de 128 o 256 bits, mucho más grandes que las de DES. Si bien no hay pruebas científicas de que las encriptaciones anidadas sean más seguras, pero en el sector informático parecer ser que si es más seguro, aunque no hay pruebas contundentes de esto.

AES tiene un bloque de input y 10 rondas diferentes que realizan cada una una clave y transforma cada una la entrada que reciben. Este es un cifrado iterado y destaca por su velocidad en hardware. Generalmente el AES se aplica en hardware y no en software. El input se organiza como un array en una matriz.

Rondas

En cada ronda se realizan las siguientes operaciones:

1. La primera operación en cada ronda es la de mover filas varias posiciones.
2. El segundo paso en cada ronda es la de mezclar las columnas mediente el uso de multiplicaciones matriciales con una operación aritmética específica
3. La tercera operación divide la clave en múltiples piezas y aplica la clave para cifrarlas.

Seguridad de DES y AES

- DES es vulnerable a ataques de búsqueda de clave. Se pudo romper en menos de 13 días en 2007. En cambio, en AES esto llevaría 10^20 años si el ataque fuera de fuerza bruta.
- Con los medios actuales la seguridad mínima recomendable es de 128 bits, aunque se recomienda que la clave sea de 256 bits.