

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 es 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 permutaciones 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 (n_0, n_1, \dots, n_n) . 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.

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

<https://knoppia.net/doku.php?id=si:blockci&rev=1727191907>

Last update: **2024/09/24 15:31**

