Seguridad de la información

Encriptado

El encriptado es simplemente el proceso de ocultar información en un mensaje de forma que solo el receptor lo pueda leer.

Cifrado de Shannon

Un cifrado de shannon es un par ξ = (E,D) de funciones tales que:

- La función de encriptado E: K x M → C toma una clave K, un texto M y obtiene un texto cifrado c tal que C=E(k,m)
- La función de desencriptado D: K x C → M toma la clave K y un texto cifrado C y obtiene el mensaje m = D(K,C).
- E y D son inversos: para todo K, M: D(K,E(K,M)) = m

Sobre Shannon

- El cifrado de shannon es operacional, no se especifican las funciones de encriptado y desencriptado
- Se asume que el texto cifrado C no ha sido manipulado
- Se asume que K es una clave secreta
- La comunicación solo es segura si es difícil deducir M o C sin saber K. Para comprobar esto tenemos que: P(m=m|c=c) = 1 / |M|+-E debería ser menor que E= 2^-128

Seguridad Perfecta

Hay muchas formas de definir Seguridad de forma rigurosa, en este caso nos centramos en la seguridad perfecta, que es la noción ideal de la seguridad de la comunicación. Si ξ=(E,D) es un cifrado de Shannon, ξ es perfectamente seguro si para todo m0,m1 pertenecientes a M y c perteneciente a C tenemos:

- P(E(K,m0)=C) = P(E(k,m1)=c)

donde K es una clave aleatoria distribuida de forma uniforme.

E(k,m0) y E(k,m1) son equivalentes en distribución, de forma que no se puede distinguir entre m0 y m1 solo mirando el texto cifrado.

Entendiendo la seguridad perfecta

Asumimos que el mensaje m se obtiene de forma uniforme de M y es estadísticamente independiente

de la clave K, entonces:

- ξ es perfectamente seguro si el texto cifrado y el mensaje son estadísticamente independientes, $c \perp m$.
- ξ es perfectamente seguro si no existe un test estadístico que pueda distinguir dos mensajes de sus textos cifrados
- ξ es perfectamente seguri si $I(m;c) = 0$, $H(c|m,k) = 0$, siendo I la información mutua y H la entropía de Shannon.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=si&rev=1725983322

Last update: **2024/09/10 15:48**