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 $\xi = (E,D)$ de funciones tales que:

- La función de encriptado $E: K \times M \rightarrow C$ toma una clave K, un texto M y obtiene un texto cifrado c tal que $C=E(k,m)$
- La función de desencriptado $D: K \times C \rightarrow M$ 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 $\xi=(E,D)$ 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 ⊥ 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.
- Shannon es seguro siempre y cuando la clave sea tan larga como el espacio del mensaje, por lo que usando una clave más de una vez no es seguro.
- El teorema de shannon establece que la entropía de la clave debe ser al menos tan grande como la entropía del mensaje por lo que H(k)>=H(m).

Seguridad semántica (SS) y cifrados computacionales

El teorema de shannon nos hace llegar a la conclusión de que la seguridad perfecta es una demasiado fuerte. En la práctica, se insiste que no debería existir un dispositivo computacional que pueda producir más que una pequeña ventaja cuando sus entradas son dos textos cifrados diferentes:

- |P(∅(E(K,m0)))-P(∅(E(K,m0)))|⇐ξ

Este requerimiento suele ser conocido como un juego de ataque entre un atacante y un adversario.

Consecuencia de la seguridad semántica

- Para un cifrado SS es computacionalmente dificil predecir los bits del mensaje
- Para un cifrado SS es computacionalmente difícil para el adversario recuperar el mensaje m del texto cifrado.

Ataques al cifrado SS: si la seguridad semántica de ξ es inferior que e, entonces un ataque de fuerza fruta en ξ tomará un tiempo prporcional a 1/e.

Distribución Cuántica de claves (QKD)

Incluso con OPT par aseguridad perfecta, el secreto es solo posible si las dos partes comparten una clave secreta en común. QKD usa leyes físicas para solucionar este problema:

- La medición del estado de un sistema cuántico, cambia el estado del sistema inevitablemente (Heinserberg uncertainty)
- Teorema del No-Clonado: No se puede hacer una copia exacta de un estado cuántico.

La idea clave es que se puede resolver gracias a las leyes de la mecánica cuántica. El emisor y receptor deben probar que son realmente quienes dicen ser. Gracias al QKD esto se puede hacer dentro de la comunicación secreta sin ningún problema. Existen varios protocolos como E91, COW SARG04…. COW es muy utilizado en comunicaciones cuánticas en la actualidad.

Los computadores cuánticos ponen en riesgo la criptografía clásica ya que pueden resolver problema extremadamente complejos en muy poco tiempo.