Criptografía simétrica.

Ejemplos, inconvenientes y alternativas.

***Fuente**: Wikipedia (https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica)*

Ejemplos

Como ejemplo de sistema simétrico está **Enigma**. Éste fue un sistema empleado por **Alemania** durante la **Segunda Guerra Mundial**, en el que las claves se distribuían a diario en forma de **libros de códigos**. Cada día, un operador de **radio**, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el **tráfico** enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.

Inglaterra usó máquinas para descifrar las claves durante aquella guerra y aunque el citado sistema alemán, Enigma, estaba provisto de un amplio abanico de claves, los ingleses diseñaron máquinas de cómputo especializado, los **Bombes**, para comprobar las claves de modo mecánico hasta que la clave del día era encontrada. Esto significaba que algunas veces encontraban la clave del día pocas horas después de que ésta fuera puesta en uso, pero también que otros días no podían encontrar la clave correcta. Los Bombes no fueron máquinas de cómputo general, sino las precursoras de los **ordenadores (computadoras)** actuales.

******** SE RECOMIENDA ….

La siguiente película estrenada el 1 de enero del 2015, nos relata cómo Alan Turing (Criptógrafo británico) hizo posible la derrota del ejército nazi en la Segunda Guerra Mundial por ser (en teoría) el responsable de descifrar los códigos secretos del ejército alemán transmitidos por la máquina Enigma.

**** **The Imitation Game (Descifrando Enigma)**

Para saber más:

http://www.sensacine.com/peliculas/pelicula-198371/

****

Inconvenientes

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio/distribución de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del **espacio de claves**.

Otro problema es el número de claves que se necesitan. Si tenemos un número *n* de personas que necesitan comunicarse entre sí, se necesitan en total $n(n-1)/2$ claves para todas las parejas de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Para solucionar estos problemas se podrían tener **centros de distribución de claves simétricas**. Esto podría funcionar por ejemplo para organizaciones militares. Aunque siempre habría un riesgo a posibles fugas de información de que claves son usadas en ciertas comunicaciones. Sin embargo su uso en el sector privado llevaría consigo inevitables fugas, atascos burocráticos y una constante amenaza de filtraciones.

Alternativas

Para solucionar este problema existen la **criptografía asimétrica** y la **criptografía híbrida**.