­­

Cifrar vs encryptar

Introduction:

Dos tipos de problemas criptográficos:

**Privacidad:** prevenir la extracción no autorizada de información en comunicaciones sobre un canal inseguro. Es necesario compartir una llave que no sea conocida por nadie más. Se hace enviando la llave por un canal seguro como private Courier o email registrado (unrealista). El flujo convencional para privadidad contiene 3 participantes: un transmisor un receptor y un espia. El transmisor emite en mensaje no cifrado P, para comunicarse sobre un canal inseguro. Se encifra con función invertible y llave K C = S\_k(P). La llave es transmitiva al receptor con un canal seguro. Entonces puede aplicar S\_k-1 (C. ) = P para obtener

El objetivo de diseñar el criptosistema. S\_k para hacer las operaciones de desifrado no costosas pero las operaciones exitosas de criptoanalitca sean complejas. Se hace la distinción de **sistemas computacionalmente seguros:** son seguros debido al costo computacional, pero sucumben ante ataque con computo ilimitado. **Incondicionalmente seguro** no sucumbe. El único sistema incondicionalmente seguro es el one time pad.

Se llamará una tarea no factible computacionalmente si su costo en memoria o procesamiento es finito, pero imposiblemente largo. Los sistemas criptográficos pueden ser divididos en dos clases: Stream ciphers y block ciphers. Stream ciphers procesan el texto en pequeños pedazos en cambio Block ciphers actúan de manera que un pequeño cambio implica un mayor cambio en la salida.

Para garantizar la autenticidad de un mensaje la información es añadida por ejemplo fecha y tiempo y enciptando secuencia entera. Los siguientes amenazas que están sujetas (en privacidad o autenticación). **Cipertext only attack**: un ataque criptoanalítico solo contiene ciphertext. Ocurre frecuentemente en la practica. Se analiza con propiedades estadísticas del lenguaje. Si el sistema no resiste a este, se considera totalmente inseguro.

**Known plaintext attack:** contains plaintext and ciphertext. Se considera Seguro un Sistema si se libera a los usuarios de la necesidad de mantener sus mensajes pasados secretos o parafrasearlos.

**Chosen plaintext attach:** puede un numero ilimitado de plaintext y examinar el criptograma resutalnte. IFF attack (Identification friend of foe)

**Criptografia de llave pública:**

Dos alternativas:

* Criptosistema de llave pública:
  + Encriptar y desencriptar esta gobernado por distintas llaves. E y D.
* Systema de distribución de llave pública:
  + Dos usuarios que desean intercambiar una llave que se comunican hata llegar a un acuerdo.

Autenticación

* Para poder tener un reemplazo digital al papel, cada usaurio debe ser posible de producir un mensaje para uatenticación pueda ser revisada por cualquuera (pero no producida por nadie más). Pueder ser visto como un broadcast cipher.
* One w­ay utenthication problema: any public key criptosystem puede ser transformado en un one-way autenthication system
* Problem of trap door.

Autenticacion puede dividirse en:

* Message autenticatoin
* User authentication

Para poder desarrollar grandes y seguras telecumunicaciones se vuelve más dificil, ya que para un potencial de usuarios n, se requiere (n^2 – n)/2 pares potenciales que se quisieran comunicar. No pueden todos tener una forma segura de transmitir la llave. Dos alternativas pueden existir para el problema. **Criptosistemas de llave pública** y **Sistemas de distribución de llave publica**. Los primeros son más poderosos, que llevan consigo la solución de problemas de autenticación.

**Criptosistema de llave publica**. Son pares de familias {E\_k}\_k y {D\_k}\_k de algorigmos que representan transformaciones invertibles. Entonces se difvide en dos, una llave cirfradora E\_k que puede hacerce publica sin comprometer la seguridad. Y una familia decifradora. De esta manera todos pueden encriptar mensajes, pero nadie puede desencriptarlos (excepto el intendent to). Pueden ser vistos como encifradores de multiple acceso.

**Sistema de distribución de llave publica:**  Solamente se requiere una llave para ser inetercambiada. Segundo el esfuerzo criptoanalitico crece exponencialmente en el esfuerzo de usuarios legitimos. Tercero, el uso puede ser atado a un archivo publico de informacion de usuario que sirve par autentificar A to B y viceversa.

**Autenticacion una via**

El problema de autenticación es quizas la barrera más seria para la adopción de telecomunicaciones para transacciones de negocios que el problema de distibucion de llave. La autenticación de una via es algo que permita reconocer si la firma es autentica, pero imposible para otra persona producirla Se aplica una funcion f() tal que es información publica, pero tiene un f-1 dificil. Notar que se está definiendo una funcion que no es invertible desde un punto de vista computacional, pero no necesariamente desde el punto de vista matematico, pero tampoco que sea no degerenara. Pro ejemplo, raices de polinomio. Es facil evaluar, pero dificil encontrar las raices.

**Interrelacion de problema y trap doors**

Un criptosistema que es seguro ante un maintext attack puede ser usado para producir una función de una via. El converse de esto no es necesariamente verdadero. Las funciones de una via son básicas para los cifradores de bloque y los generadores de llaves. Un generador de llave es un pseudo aleatorio generador de bit, que en el output. La llave es usada como semilla que determina la secuencia pseudo aleatoria.

Un cripstosistema de llave publica puede ser utilizado para generar una autenticación de una via.

Un criptosistema trap door puede ser utilizado para producitr un sistema de distribución de llave