
CRIPTOGRAFIA

Universidad Tecnológica
Centroamericana

Como comienza todo

- Supondremos que un emisor desea enviar un mensaje a un receptor.
 - El emisor quiere asegurarse que un intruso no pueda leer el mensaje
 - La solución : **criptografía**
-

Definiciones

- **Texto claro (plaintext)**

- Mensaje

- **Encriptar (encrypt)**

- Proceso de encubrir un mensaje para que no se conozca su contenido

- **Texto cifrado (cyphertext)**

- Mensaje encriptado
-

Definiciones

- **Decriptar (decrypt)**

- Proceso de convertir texto encriptado a texto claro

- **Criptografía**

- Arte y ciencia de mantener seguros los mensajes. Practicada por criptólogos

- **Criptanálisis**

- Arte y ciencia de romper texto encriptado
-

Definiciones

- Si M es el mensaje (datos binarios), el texto encriptado es C , la función de encriptamiento $E(M) = C$
 - $D(C) = M$
 - Por lo tanto, $D(E(M)) = M$
-

Seguridad vs. Oscuridad

- Existen dos clases de criptografía:
 - La que no deja que tu hermanita lea tu “libro negro”
 - La que no deja que la CIA ni la KGB ni la DNI lean tu “libro negro”.
 - Nosotros hablaremos sobre esta última, debiendo notar la diferencia entre seguridad y oscuridad
-

Oscuridad

- Si yo tomo una carta, la meto en una caja fuerte, luego escondo la caja fuerte en algun lugar de toda Centroamérica y le pido que lea la carta, eso es oscuridad
-

Seguridad

- Ahora bien, si yo pongo la carta en una caja fuerte, y luego le doy:
 - La caja fuerte, con los planos de diseño
 - Cien cajas fuertes iguales a esta, con todo y las combinaciones
 - Cien expertos en cajas fuertes, para que estudien el diseño
 - Y si aún así no puede leer la carta...
-

Seguridad

- Esta clase de seguridad solo estaba disponible para los militares (CIA, KGB, Mossad)
 - En los últimos veinte años se ha hecho tanta investigación en criptografía, que es posible para cualquier persona usar técnicas de seguridad a nivel de las agencias de inteligencia militar
-

Es necesaria tanta seguridad?

- Dependencia en la información por parte de las empresas comerciales
 - Protección intelectual
 - Acoso del gobierno
 - Derecho a la privacidad
 - Anonimidad (votaciones, HIV)
 - Paranoia
-

Que más se puede hacer?

- Autenticación

- Verificación de quien ha enviado un mensaje que fue recibido

- Integridad

- Verificar que el mensaje no fue modificado mientras estuvo en transito

- Afirmación de origen

- Evitar la repudiación de mensajes
-

Algoritmos criptográficos

- Un algoritmo criptográfico es una función matemática usada para encriptar y decriptar
 - Si la seguridad se basa en mantener secreto el algoritmo, se denomina restringido
 - Problemas
 - Si un usuario se va, debe cambiarse
 - No hay control de calidad
-

Algoritmos restringidos

- A pesar de los problemas, estos algoritmos son muy populares
 - No saben
 - No les importa
 - Existe solución?
-

Llaves

- Una llave K es un valor, escogido de un conjunto muy grande, llamado *espacio de llaves*
 - Ahora $E(M, K) = C$ y $D(C, K) = M$
 - Algunos algoritmos usan dos llaves así:
 $E(M, K_1) = C$ y $D(C, K_2) = M$
 - La seguridad depende de las llaves, no de los algoritmos
-

Aparte: valores grandes

- Probabilidad diaria de que le caiga un rayo: 1 en 9,000,000,000 (2^{33})
 - Probabilidad de ahogarse: 1 en 59,000 (2^{16})
 - Cuanto falta para la siguiente Edad de Hielo: 14,000 años (2^{14})
 - El sol se convierte en nova: 2^{30} años
 - Edad del universo: 2^{34} años
 - Atomos en el planeta: 2^{170}
 - Atomos en el sol: 2^{190}
 - Atomos en la galaxia: 2^{223}
 - Si el universo es abierto, faltan 2^{216} años para que toda la materia se vuelva líquida a 0 Kelvin
-

Algoritmos basados en llaves

- Simétricos (llave secreta)
 - Se utiliza la misma llave para encriptar y decriptar. La seguridad se basa totalmente en esta llave, y si se pierde o se compromete el sistema falla
 - Existen dos clases : stream opera un bit a la vez y block opera sobre bloques de bits
-

Algoritmos basados en llaves

■ Llave pública

- ❑ Se tiene una llave para encriptar y otra para decriptar
 - ❑ La llave de decripción no puede calcularse en base a la de encripción
 - ❑ La llave de encripción puede publicarse, solamente quien tenga la llave privada puede leer el mensaje
-

Criptanálisis

- La ciencia de recuperar mensajes encriptados
 - Un criptanálisis se denomina *ataque*
 - La secretividad debe depender solamente de la llave
 - Existen varios tipos de ataque
-

#1: Solo texto encriptado

- El analista tiene el texto encriptado de varios mensajes que han usado el mismo algoritmo
 - Dado $C_1 = E(P_1, K)$, $C_2 = E(P_2, K), \dots$
 - Deducir P_1, P_2, P_n o K o un algoritmo para inferir P_{i+1} de $C_{i+1} = E(P_{i+1}, K)$
-

#2: Texto claro conocido

- El analista tiene mensajes cifrados y el texto claro de estos
 - Dado P_1 , $C_1 = E(P_1, K)$, etc.
 - Deducir: K o un algoritmo para inferir P_{i+1} de $C_{i+1} = E(P_{i+1}, K)$
-

#3: Texto claro escogido

- El analista tiene mensajes cifrados, textos claros y además puede escoger el mensaje que se encripta
 - Esto es muy poderoso, porque el analista puede escoger mensajes específicos que pueden proveer más información
-

Criptografía simétrica

- Dos entidades se comunican de manera segura de la siguiente forma:
 - A y B acuerdan un algoritmo
 - A y B acuerdan una llave K
 - A envía $C = E(M, K)$
 - B recibe C y hace $M = D(C, K)$
-

Problemas

- K debe permanecer secreta, antes, durante y después
 - A puede dar copia de K a un tercero
 - Si un tercero ataca exitosamente el sistema, puede leer mensajes o falsificarlos
 - Si hay n usuarios, se requieren $n(n-1)/2$ llaves
-

Funciones no invertibles

- Estas funciones son importantes para la criptografía de llave pública
 - Son fáciles de calcular, pero difíciles de invertir
 - Difícil = algo que tomaría al computador más rápido del mundo millones de años
 - Suena bien, pero no se ha demostrado su existencia
-

Funciones no invertibles con trampa

- Son FNI con un “secreto” que permite calcular la inversa fácilmente
 - Ejemplo: desarmar un reloj
-

Criptografía de llave pública

- Usa dos llaves: una pública y otra privada
 - Concepto de caja fuerte versus buzón
 - A puede encriptar con la llave pública de B, pero solamente B puede decriptar el mensaje con su llave privada
 - Matemáticamente: FNI con trampas
 - La trampa? La llave privada
-

Problemas con PKC

- PKC es lento
 - PKC es vulnerable a ataques de texto claro escogido
 - Solucion: usar PKC para encriptar llaves aleatorias de sesión que serán usadas en un algoritmo simétrico
-

Firmas digitales

- Una firma a mano tiene las siguientes características (ideales):
 - Es auténtica
 - No falsificable
 - No es reusable
 - El documento firmado es inalterable
 - La firma no se puede repudiar
 - Podemos hacer esto con computadoras?
-

Firmas digitales con PKC

- Para firmar un documento digitalmente usando criptografía de llave pública, se realizan los siguientes pasos:
 - A encripta M con su llave privada (firma)
 - A envía el documento a B
 - B decripta el documento con la llave pública de A, verificando la firma
-

Divirtiéndonos con la firma

- B podría reutilizar el documento firmado. Qué importa una copia más de un contrato?
 - Pero... ¿ y si lo firmado es un cheque digital ?
 - Solución: timestamps
-

Como experimentar

- PGP es un paquete completo de criptografía, basado en llaves públicas
 - Se puede conseguir en Internet
 - Usar la version internacional
-

Preguntas ó Comentarios

- Ahora mismo
- Por e-mail
 - efutch AT gmail DOT com