Introducción Criptografía Simétrica

Características y uso

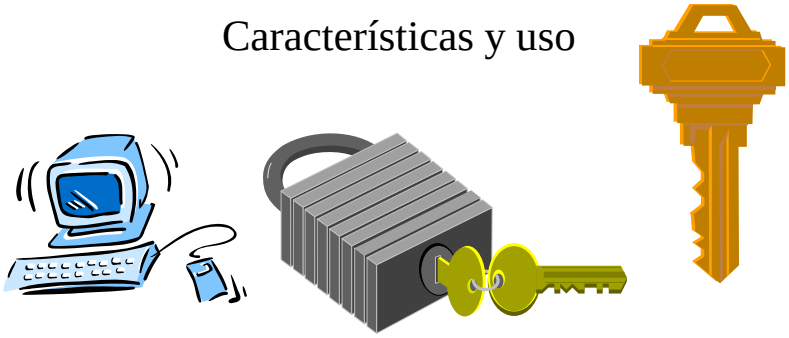


Lámina 1

Roberto Gómez C.

Recordando

- La criptografia define una función de transformación de un mensaje con base a un elemento base o llave, para obtener un nuevo mensaje nuevo e inteligible.
- El mensaje *m* es un elemento de un universo M que es el conjunto de las combinaciones de posibles mensajes aunque no sean semanticamente correcto.

Lámina 2

Roberto Gómez C.

Encriptando con una computadora

- La computadora "*maneja*" números en lugar de letras
  - solo números binarios (digitos binarios = bits)

a = 1100001
! = 0100001
& = 0100110

- La encripción se realiza bajo mismo principio de substitución y transposición
  - elementos del mensaje son substituidos por otros elementos, o sus posiciones son intercambiadas o ambas

Lámina 3 Roberto Gómez C.

Transposición en la computadora

- Convertir mensaje a ASCII

Texto claro:
HELLO = 1001000 1000101 1001100 1001100 1001111

- Transposición: intercambiar las letras en un orden predeterminado

Texto claro:
HELLO = 1001000100010110011001001100111 1
Criptograma:
LHOEL = 1001100100100010011111000101100 1100

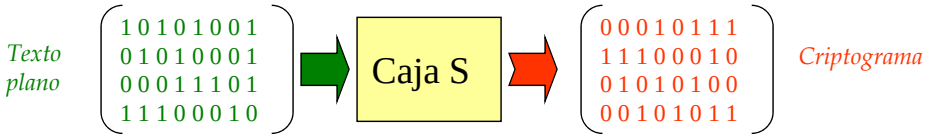
- La transposición puede darse a nivel de bits

Letra original: 1001000 Letra encriptada: 0010010

Lámina 4 Roberto Gómez C.

Substitución en la computadora

- Conjunto de bits es sustituido por otro conjunto de bits.
- El mapeo se efectúa a través de una tabla (p.e. caja S) o una operación matemática (que cuenta con una inversa) sobre el conjunto original de bits (p.e. pseudo transformada de Hadamard)



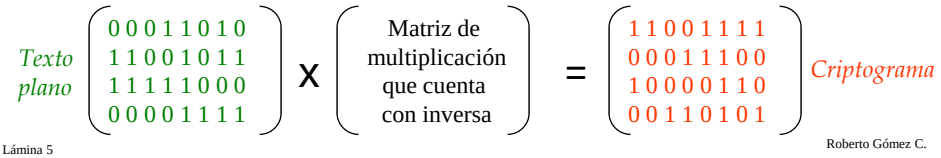


Lámina 5
Roberto Gómez C.

Utilizando una llave: la función xor

- Es posible utilizar una llave para transformar los bits.
- Por ejemplo supongamos el uso de la llave DAVID.

DAVID = 1000100 1000001 1010110 1001001 1000100

- Para encriptar/decriptar sumamos la llave al mensaje original, (suma binaria: xor)

Texto claro:	HELLO
Texto ASCII:	1001000100010110011001001100100111 1
Llave:	1000100100000110101101001001100010 0
Criptograma:	0001100000010000110100000101000101 1

Lámina 6
Roberto Gómez C.

Encriptado Vernam

- Representa caso límite cifrado de Vigenere
- Emplea alfabeto binario
- Operación aritmética es suma modulo 2
  - recuperación: sumar nuevamente la secuencia
- llave: secuencia binaria aleatoria de la misma longitud que el texto claro
- Ejemplo:

Mensaje:	00011 01111 01101 00101 10011 01111
Llave:	11011 00101 01011 00110 10110 10101
Criptograma:	11000 01010 00110 00011 00101 11010

Lámina 7
Roberto Gómez C.

Condiciones secreto perfecto

- Definida por Shanon a partir hipótesis:
  - la llave secreta se utilizará una vez
  - la llave es del mismo tamaño que el mensaje
  - el enemigo criptoanalista solo tiene acceso al criptograma
- Referencia:
  - C. E. Shannon. Communication theory of secrecy systems. Bell System Technical Journal, 28-4:656--715, 1949
- Un ejemplo de secrecia perfecta es conocido como One-time Pad de Vernam
  - descrito por primera vez en 1917
  - usado en telégrafos

Lámina 8
Roberto Gómez C.

Métodos Criptográficos

- Métodos Simétricos
  - llave encriptado coincide con la de descifrado
  - la llave tiene que permanecer secreta
  - emisor y receptor se han puesto de acuerdo previamente o existe un centro de distribución de llaves
  - criptografía clásica o criptografía de llave secreta
- Métodos asimétrico
  - llave encriptado es diferente a la de descriptado
  - corresponden a la criptografía de la llave pública, introducida por Diffie y Hellman en 1976

Lámina 9
Roberto Gómez C.

Características encripción llave secreta

- Los mejores algoritmos ofrecen confidencialidad casi perfecta
- Cada entidad debe asegurar a la otra parte que mantendrá en secreto la llave compartida
- Util en redes donde el número de usuarios es reducido
- Debe existir un administrador encargado de la generación, asignación y almacenamiento de las llaves

Lámina 10
Roberto Gómez C.

Criptosistema llave secreta

- M: conjunto de mensajes que se pueden enviar dos usuarios
  - A: Alicia, B: Beto
- K todas las posibles llaves que pueden utilizar
- Criptosistema llave secreta:
  - par de funciones D_k (E_k para cada llave k de K)
  - $E_k : m \rightarrow c$
  - $D_k : c \rightarrow m$

para cada mensaje m de M
$D_k (E_k(m)) = m)$

Lámina 11
Roberto Gómez C.

- Los usuarios A y B se ponen de acuerdo y eligen secretamente una llave *k* de K.
- Si A desea enviar un mensaje m de M a B, encripta mensaje por medio función E_k

$$E_k (m) = c$$

- Envía resultado c a B,
- En la recepción B decripta el texto encriptado, c, por medio de la función D

$$D_k (c) = D_k (E_k (m)) = m$$

Lámina 12
Roberto Gómez C.

- Funciones E_k D_k deben ser “fáciles” de calcular para los usuarios y “difíciles” de calcular para alguien que escuchara c, de modo que no pudiera recuperar ni *m* ni k.
- Termino fácil indica que el cálculo se puede llevar a cabo en un período corto de tiempo.
- Termino difícil implica que no se puede calcular en un tiempo aceptable.

Lámina 13
Roberto Gómez C.

La llave k del universo K

- El tamaño de K debe buscarse los suficientemente grande para evitar romper el algoritmo (encontrar la llave k usada) con los recursos de computo con que se cuente en ese momento

Lámina 14
Roberto Gómez C.

Esquema general encripción llave secreta

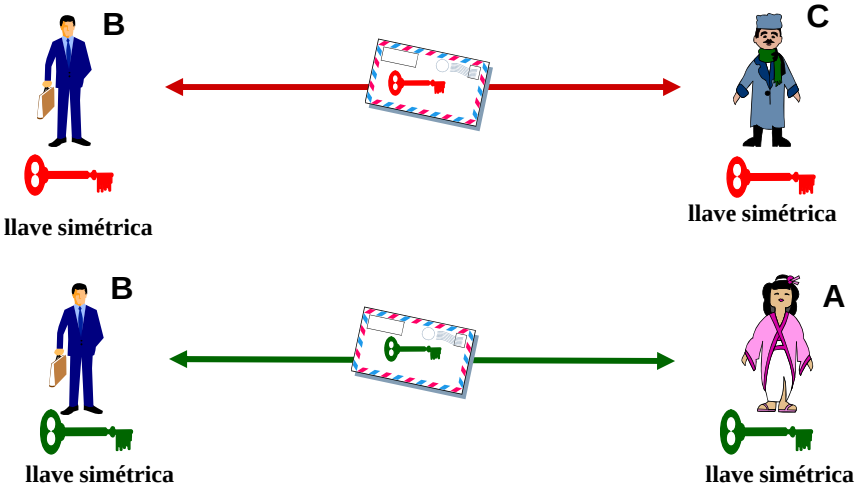


Lámina 15 Roberto Gómez C.

Encripción llave secreta

3. Bob asegura la caja con la llave de la caja fuerte.

5.Alice desasegura la caja con un duplicado de la llave de la caja fuerte.

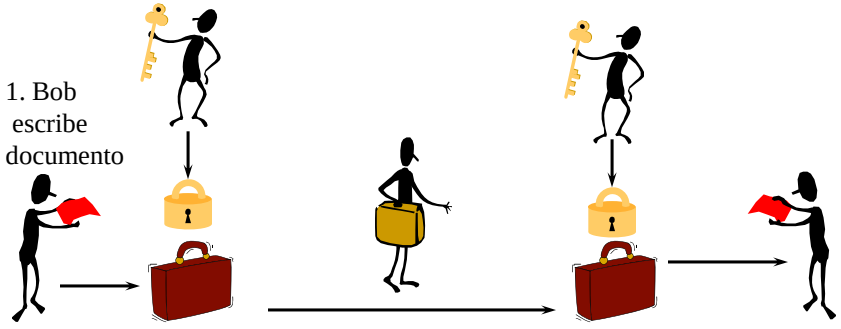


Lámina 16 Roberto Gómez C.

Introducción Criptografía Simétrica

Características y uso

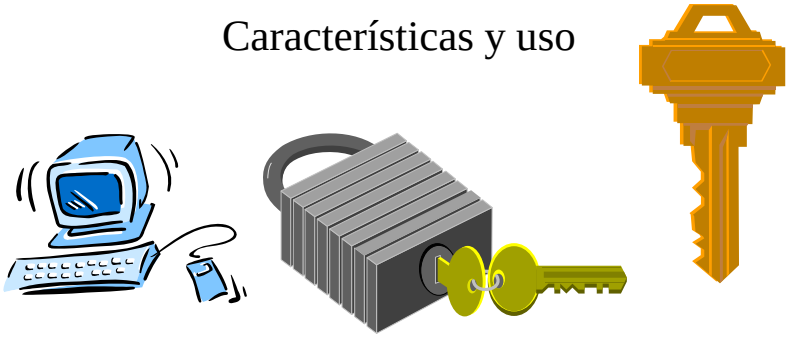


Lámina 17

Roberto Gómez C.

Difusión y confusión

- En criptografia simétrica, la seguridad depende de un secreto compartido por emisor y receptor.
- La principal amenaza criptoanalítica proviene de la alta redundancia de la fuente.
- Shannon sugirió por ello dos métodos básicos para frustrar un criptoanálisis estadístico:
  - la confusión: modificación de los símbolos del mensaje original
  - la difusión: ocultar las estadísticas que puedan aparecer en ese mensaje
- Por si solas, ni confusión ni difusión constituyen buenas técnicas de cifrado.

Lámina 18

Roberto Gómez C.

La difusión

- Como E depende de (k,M) para generar C, se dice que E es función de (k,M)
- El propósito de la difusión consiste en anular la influencia de la redundancia de la fuente sobre el texto cifrado.
- La difusión consiste en distribuir la influencia de cada bit por todo el mensaje, de forma que cambiar un bit en el mensaje en claro, provoque un gran cambio en el mensaje cifrado.

Lámina 19
Roberto Gómez C.

Consiguiendo difusión

- Hay dos formas de conseguirlo.
  - La primera, conocida como transposición, evita los criptoanálisis basados en las frecuencias de las n-palabras.
  - La otra manera consiste en hacer que cada letra del texto cifrado dependa de un gran número de letras del texto original.

Lámina 20
Roberto Gómez C.

La confusión

- El objetivo de la confusión consiste en ocultar la relación entre el mensaje en claro, el mensaje cifrado y la llave, de forma que sea difícil establecer relaciones entre los tres.
  - crear confusión de acerca que (k,M) viene de C
- De esta forma las estadísticas del texto cifrado no estén muy influidas por las del texto original.
- Esto se consigue normalmente con la técnica de la sustitución.

Lámina 21
Roberto Gómez C.

Algoritmos producto

- En principio la confusión sería suficiente si almacenamos suficientes pares de bloque en claro y bloque cifrado (todos los posibles), pero esto resulta inviable en cuanto nuestro tamaño de bloque crece, así que lo que se hace es mezclar la confusión con patrones pequeños con la difusión.
- Los algoritmos que hacen esto se denominan *algoritmos de producto.*

Lámina 22
Roberto Gómez C.

Entropía

- Cantidad de información promedio por símbolo que emite una fuente.
  - puede ser interpretada como el número medio de símbolos necesarios para representar cada valor de los elementos de una secuencia aleatoria
- La entropía nos indica el límite teórico para la compresión de datos.
- También es una medida de la información contenida en el mensaje

Lámina 23
Roberto Gómez C.

Definición formal entropia

- La definición normal esta dada por

$$H(x) = \sum_{i=1}^{n} p(i)\left(\frac{1}{p(i)}\right)$$

- Donde
  - H es la entropía,
  - p son las probabilidades de que aparezcan los diferentes simbolos y
  - n el número total de simbolos
  - habitualmente el logaritmo en base 2

Lámina 24
Roberto Gómez C.

Ejemplo entropia

- Texto escrito en español, codificado como una cadena de letras, espacios y signos de puntuación
- Estadísticamente, algunos caracteres no son muy comunes (por ejemplo, 'y'), mientras otros sí lo son (como la 'a'), la cadena de caracteres no es tan "aleatoria" como podría llegar a ser.
- Obviamente, no podemos predecir con exactitud cuál será el siguiente carácter en la cadena y eso la haría aparentemente aleatoria; pero es la entropía la encargada de medir precisamente esa aleatoriedad

Lámina 25
Roberto Gómez C.

Funciones y relaciones lineales

- Función matemática polinomial de primer grado de la forma:

$$y = mx + c$$

  - donde m y c son constantes
- Las variables en una expresión lineal:
  - no pueden tener exponentes
  - no pueden multiplicarse o dividirse uno a otra
  - no pueden encontrarse dentro un signo de raíz
- Biunívoca
- Para todo valor en el dominio existe uno en el codominio

Lámina 26
Roberto Gómez C.

Ejemplos

- Estos son ejemplos de expresiones lineales
  - x + 4
  - 2x +4
  - 2x + 4y
- Estos no son expresiones lineales
  - x^2
  - 2xy + 4
  - 2x / 4y
  - $\sqrt{x}$

Lámina 27
Roberto Gómez C.

Clasificación métodos encripción simetricos

- Encripción en flujo

- Encripción en bloques

Lámina 28
Roberto Gómez C.