# Introducción a la criptologia y a la esteganografia

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://campus.cem.itesm.mx/ac/rogomez



## Definición y componentes

- *Criptología*.- Ciencia que estudia los aspectos y contenidos de información en condiciones de secrecía.
- Del griego: *criptos* oculto y *logos* tratado
- La Criptología se divide en:
  - *Criptografía.*
  - *Criptoanálisis.*

## Criptografía

- Es el *arte* de construir códigos secretos.
- Es el conjunto de técnicas o procedimientos que alteran los símbolos de información sin alterar el contenido, convirtiendo a la información modificada en un conjunto de símbolos sin contenido para las partes que no disponen de las técnicas.

Lámina 3
Roberto Gómez C.

## Criptoanálisis

- Metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico, sin conocer *"a priori"* la técnica utilizada para la criptografia.

Codemakers vs Codebreakers


Lámina 4
Roberto Gómez C.

## Los actores

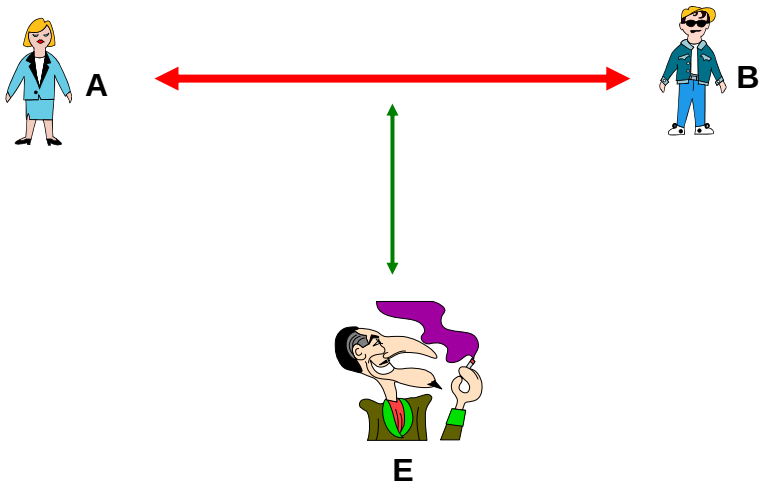



Lámina 5

Roberto Gómez C.

## Esteganografia

- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos, dentro de información considerada como válida.
- La información puede esconderse de cualquier forma
  - diferentes métodos se han ido desarrollando

Lámina 6

Roberto Gómez C.

## Stegoanálisis

- Arte de descubrir y convertir los mensajes en no útiles.
- Ataques y análisis de información oculta pueden tomar diferentes formas:
  - detección
  - extracción
  - confusión (alteración, introducción)
  - deshabilitación de la información oculta
- Muchos casos requieren contar con porciones del objeto encubierto (stego-object) y posibles porciones del mensaje.
  - resultado: el stego-object

Lámina 7
Roberto Gómez C.

## Criptosistemas

- Es el conjunto de procedimiento que garantizan la seguridad de la información y utilizan técnicas criptográficas.
- El termino en inglés es cipher.
- El elemento fundamental de un Criptosistema es la *"llave"*.
- En algunas referencias a la llave se le conoce como *clave*.

Lámina 8
Roberto Gómez C.

## Proceso encripción/decripción

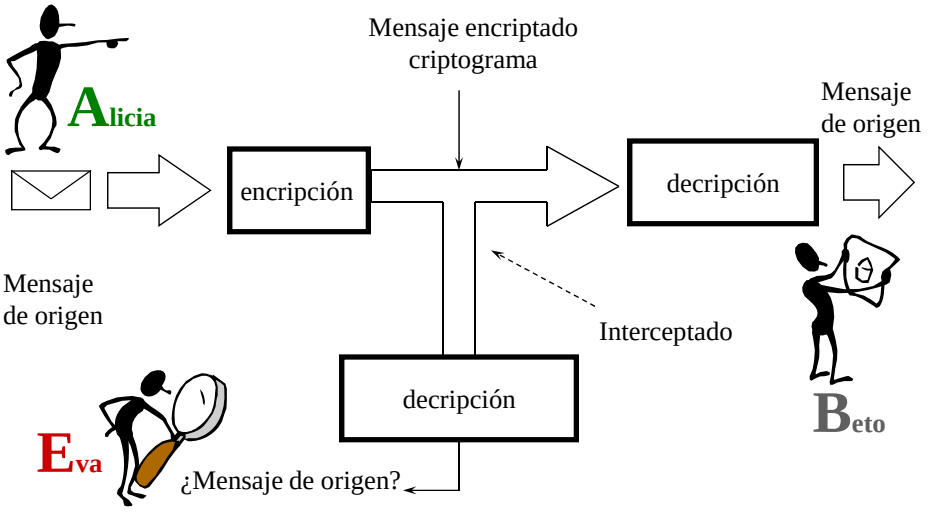



Lámina 9
Roberto Gómez C.

## Objetivos criptografía

- Mantener la confidencialidad del mensaje
  - la información contenida en el mensaje permanezca secreta
- Garantizar la autenticidad tanto del mensaje como del par remitente/destinatario
  - el mensaje recibido ha de ser realmente el enviado
  - el remitente y destinatario han de ser realmente quienes dicen ser y no remitentes y/o destinatarios fraudulentos

Lámina 10
Roberto Gómez C.

## Clasificación seguridad criptográfica

- Seguridad incondicional (teórica).
  - sistema seguro frente a un atacante con tiempo y recursos computacionales ilimitados.
- Seguridad computacional (práctica).
  - el sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados.
- Seguridad probable.
  - no se puede demostrar su integridad, pero el sistema no ha sido violado.

Lámina 11
Roberto Gómez C.

- Seguridad condicional.
  - todos los demás sistemas, seguros en tanto que el enemigo carece de medios para atacarlos.

Lámina 12
Roberto Gómez C.

## Criptografía y seguridad

- En la práctica la seguridad que ofrece un criptosistema consiste en mostrar que *"cualquier ataque que tiene una probabilidad de romper la llave requiere de una cantidad infinita de computación"*.
- Un sistema criptográfico se dice *inseguro* cuando los contenidos de encripción pueden ser descifrados en un tiempo polinomial.

Lámina 13
Roberto Gómez C.

## Obscuridad vs Seguridad

Si guardo en una caja fuerte una carta, **escondo** la caja en **algún** lugar de Nueva York, y luego les pido que lean la carta, eso **no es seguridad**: es **obscuridad**.

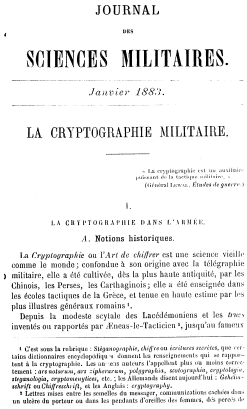
Si por otra parte, guardo en una caja fuerte una carta, **les doy las especificaciones** de la caja, y cientos de cajas fuertes con sus combinaciones para que ustedes y analistas **expertos revisen el mecanismo** de seguridad; y aún así **no pueden** abrir la caja fuerte y leer la carta, eso es **seguridad**."

*Principio de Kerchkhoffs*
*La criptografía militar*

Lámina 14
Roberto Gómez C.

# Principio de Kerckhoffs

Establece que la seguridad del encriptado ha de residir exclusivamente en el secreto de la llave, y no en el mecanismo de encripción.



JOURNAL
DES
SCIENCES MILITAIRES.
*Janvier 1883.*

LA CRYPTOGRAPHIE MILITAIRE.

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE.

*A.* Notions historiques.

La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains [1].

Depuis la modeste scytale des Lacédémoniens et les *tracés* inventés ou rapportés par Æneas-le-Tacticien [2], jusqu'au fameux

[1] C'est sous la rubrique : *Stéganographie, chiffres ou écritures secrètes*, que certains dictionnaires encyclopédiques donnent les renseignements qui se rapportent à la cryptographie. Les uns ont autrefois l'appellent plus ou moins correctement : *ars notaria, ars ziphercum, polygraphia, steelographia, cryptologia, steganologia, cryptomenytica*, etc. ; les Allemands disent aujourd'hui : *Geheimschrift* ou *Chiffrirkunst*, et les Anglais : *cryptography*.

[2] Lettres mises entre les semelles du messager, communications cachées dans un nœud de porteur ou dans les pendants d'oreilles des femmes, des perles de

Holandés nacido en 1835

http://www.petitcolas.net/fabien/kerckhoffs/

Lámina 15

Roberto Gómez C.

# Reglas de Kerckhoffs

- No debe existir ninguna forma de recuperar mediante el criptograma el texto inicial o la llave.
  - esta regla se considera cumplida siempre que la complejidad del proceso de recuperación del texto original sea suficiente para mantener la seguridad del sistema.
- Todo sistema criptográfico debe estar compuesto por dos tipos distintos de información.
  - pública, como es la familia de algoritmos que lo definen
    - en los sistemas de llave pública, parte de la llave es también información pública.
  - privada, como es la llave que se usa en cada encripción particular

Lámina 16

Roberto Gómez C.

## Reglas de Kerckhoffs

- La forma de escoger la llave debe ser fácil de recordar y modificar.
- Debe ser factible la comunicación del criptograma por los medios de transmisión habituales.
- La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido

Lámina 17
Roberto Gómez C.

## Requisitos de un criptosistema

- Algoritmo de cifrado/descifrado rápido y fiable.
- Posibilidad de transmitir archivos por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido a la encripción o decripción.
- La seguridad del sistema deberá residir solamente en el secreto de una llave y no de las funciones de encripción.
- La fortaleza del sistema se entenderá como la imposibilidad computacional (tiempo de cálculo en años que excede cualquier valor razonable) de romper el criptosistema o encontrar la llave secreta a partir de otros datos de carácter público.

Lámina 18
Roberto Gómez C.

## Clasificación criptográfia

- Criptografía clásica
  - transposición
  - substitución
- Criptografía moderna
  - simetrica (llave privada)
  - asimetrica (llave pública)

Lámina 19
Roberto Gómez C.

## Las funciones hash

- Transforman un conjunto de bits en un número de identificación único, generalmente expresado en hexadecimal.
- También conocidas como funciones de un solo sentido.
- Principales algoritmos
  - MD5
  - SHA-1

Lámina 20
Roberto Gómez C.

## Criptoanálisis

- Objetivo:
  - encontrar alguna debilidad o inseguridad en un esquema criptográfico
- ¿Quién lo lleva a cabo?
  - un atacante hostil que intenta destruir un sistema,
  - diseñador de un sistema que desea evaluar si un sistema es seguro
- Criptoanálista
  - persona que lleva a cabo criptoanálisis

Lámina 21
Roberto Gómez C.

## ¿Qúé significa romper un criptosistema?

- Breaking a cipher doesn't necessarily mean finding a practical way for an eavesdropper to recover the plaintext from just the ciphertext. In academic cryptography, the rules are relaxed considerably. Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity lessthan brute-force. Never mind that brute-force might require $2^{128}$ encryptions; an attack requiring $2^{110}$ encryptions would be considered a break. Breaks might also require unrealistic amounts of known or chosen plaintex -$2^{56}$ blocks - or unrealistic amounts of storage: $2^{80}$. Simply put, a break can just be a "certificational weakness": evidence that the cipher does not perform as advertised.

Bruce Schneier A Slef-Study Course in Block-Cipher Cryptanalysis

Lámina 22
Roberto Gómez C.