Seguridad Informática

Introducción a la Criptografía

Ramón Hermoso y Matteo Vasirani

Universidad Rey Juan Carlos

Índice

1 Terminología e historia

2 Primitivas criptográficas

3 Nociones de criptoanálisis

Índice

1 Terminología e historia

2 Primitivas criptográficas

3 Nociones de criptoanálisis

Terminología básica

Criptografía

Ciencia que se ocupa de la búsqueda y mejora de técnicas para la transmisión segura de la información

Criptoanálisis

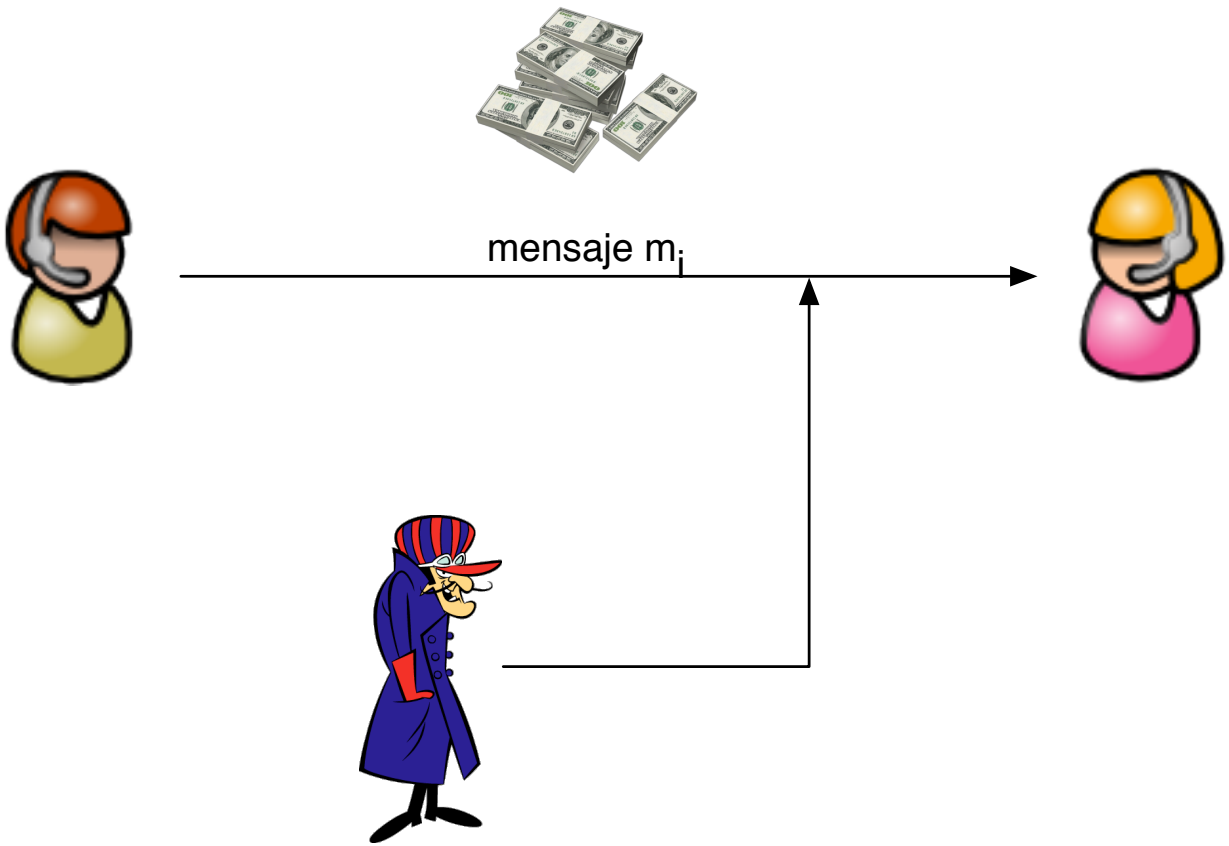
Estudio crítico de los sistemas criptográficos

Criptología

Criptografía + Criptoanálisis

Caso base I

Caso base II



Esteganografía

- Criptografía $\neq$ Esteganografía $\Rightarrow$ técnicas para la ocultación de un mensaje dentro de otro mensaje.

Ejemplo

Los asirios tenían amarrados los caballos a anclajes mientras los olmecas sólo ajustaban largos amarres sobre octogonales calesas que se hacían ocultar.

- Si tomamos la primera letra de cada palabra (mayor de una sílaba) del texto original:

Ataquemos a la ocho

Esteganografía

- Criptografía $\neq$ Esteganografía $\Rightarrow$ técnicas para la ocultación de un mensaje dentro de otro mensaje.

Ejemplo

Los asirios tenían amarrados los caballos a anclajes mientras los olmecas sólo ajustaban largos amarres sobre octogonales calesas que se hacían ocultar.

- Si tomamos la primera letra de cada palabra (mayor de una sílaba) del texto original:

Mensaje oculto

Atacamos a la ocho

Esteganografía

- Criptografía $\neq$ Esteganografía $\Rightarrow$ técnicas para la ocultación de un mensaje dentro de otro mensaje.

Ejemplo

Los asirios tenían amarrados los caballos a anclajes mientras los olmecas sólo ajustaban largos amarres sobre octogonales calesas que se hacían ocultar.

- Si tomamos la primera letra de cada palabra (mayor de una sílaba) del texto original:

Mensaje oculto

Atacamos a la ocho

Tipos de Criptología I

Criptología clásica o de clave secreta (o simétrica)

- Rapidez
- Máximo nivel de seguridad
- Intercambio previo de información entre usuarios

Tipos de Criptología II

Criptología moderna o de clave pública (o asimétrica)

- Más reciente (> 1976)
- La seguridad es en gran medida heurística
- No hay intercambio previo de información

Un poco de historia I

- 2000 a.C. los egipcios comienzan a usar símbolos no convencionales
- 50 a.C. Algoritmo de Julio César para cifrar mensajes
- 500-1400 Criptografía es considerada como magia negra (gran declive de estudios)
- 855 Aparece el primer libro sobre criptografía, en Arabia (Al-Kindi)
- s. XV Auge de la criptografía en Italia (relaciones diplomáticas)
- 1466 Disco de Alberti (primer sistema polialfabético que se conoce). ”Padre de la criptografía”

Un poco de historia II

- 1585 Blaise de Vigenère → primer sistema polialfabético con autoclave, conocido como ”Le chiffre indéchiffrable”→ cifrado de Vigenère
- 1917 Vernam desarrolla la cinta aleatoria de un sólo uso, el único sistema criptográfico seguro
- 1944 Máquinas de cifrado → Enigma, Colossus.
- 1949 Teorema de Shannon. Algoritmo de cifrado teóricamente irrompible
- 1976 Whitfield Diffie y Martin Hellman publican ”New Directions in Cryptography”. Padres de la criptografía de clave pública (Intercambio de claves).

Objetivos de la Criptografía

1. **Privacidad**: asegurar que nadie es capaz de observar la información que se envía de un extremo a otro
2. **Integridad de datos**: asegurar que el mensaje que se envía no es alterado
3. **Autenticación**: asegurar que tanto el que envía el mensaje como el que lo recibe son quienes dicen ser
4. **No repudio**: imposibilidad de negar la autoría de un mensaje por parte del emisor

Objetivos de la Criptografía

1. **Privacidad**: asegurar que nadie es capaz de observar la información que se envía de un extremo a otro
2. **Integridad de datos**: asegurar que el mensaje que se envía no es alterado
3. **Autenticación**: asegurar que tanto el que envía el mensaje como el que lo recibe son quienes dicen ser
4. **No repudio**: imposibilidad de negar la autoría de un mensaje por parte del emisor

Objetivos de la Criptografía

1. **Privacidad**: asegurar que nadie es capaz de observar la información que se envía de un extremo a otro
2. **Integridad de datos**: asegurar que el mensaje que se envía no es alterado
3. **Autenticación**: asegurar que tanto el que envía el mensaje como el que lo recibe son quienes dicen ser
4. **No repudio**: imposibilidad de negar la autoría de un mensaje por parte del emisor

Objetivos de la Criptografía

1. **Privacidad**: asegurar que nadie es capaz de observar la información que se envía de un extremo a otro
2. **Integridad de datos**: asegurar que el mensaje que se envía no es alterado
3. **Autenticación**: asegurar que tanto el que envía el mensaje como el que lo recibe son quienes dicen ser
4. **No repudio**: imposibilidad de negar la autoría de un mensaje por parte del emisor

Índice

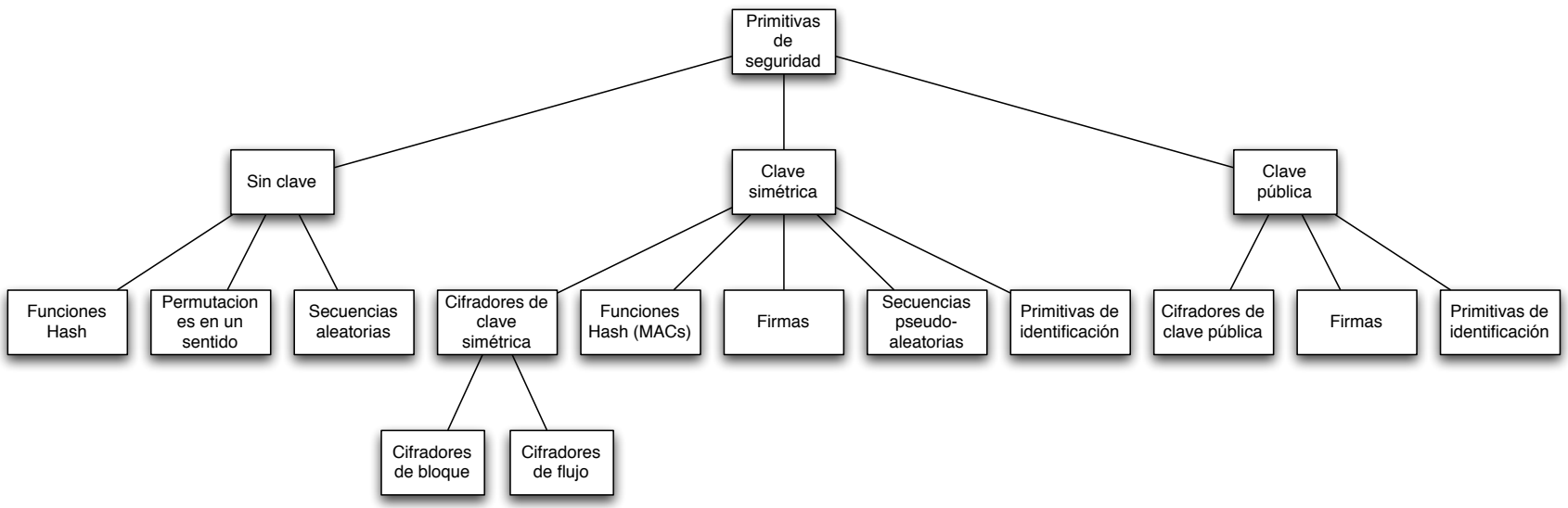
1 Terminología e historia

2 Primitivas criptográficas

3 Nociones de criptoanálisis

Primitivas criptográficas I

- Las primitivas se usan como bloques básicos para construir cualquier sistema criptográfico.



Primitivas criptográficas II

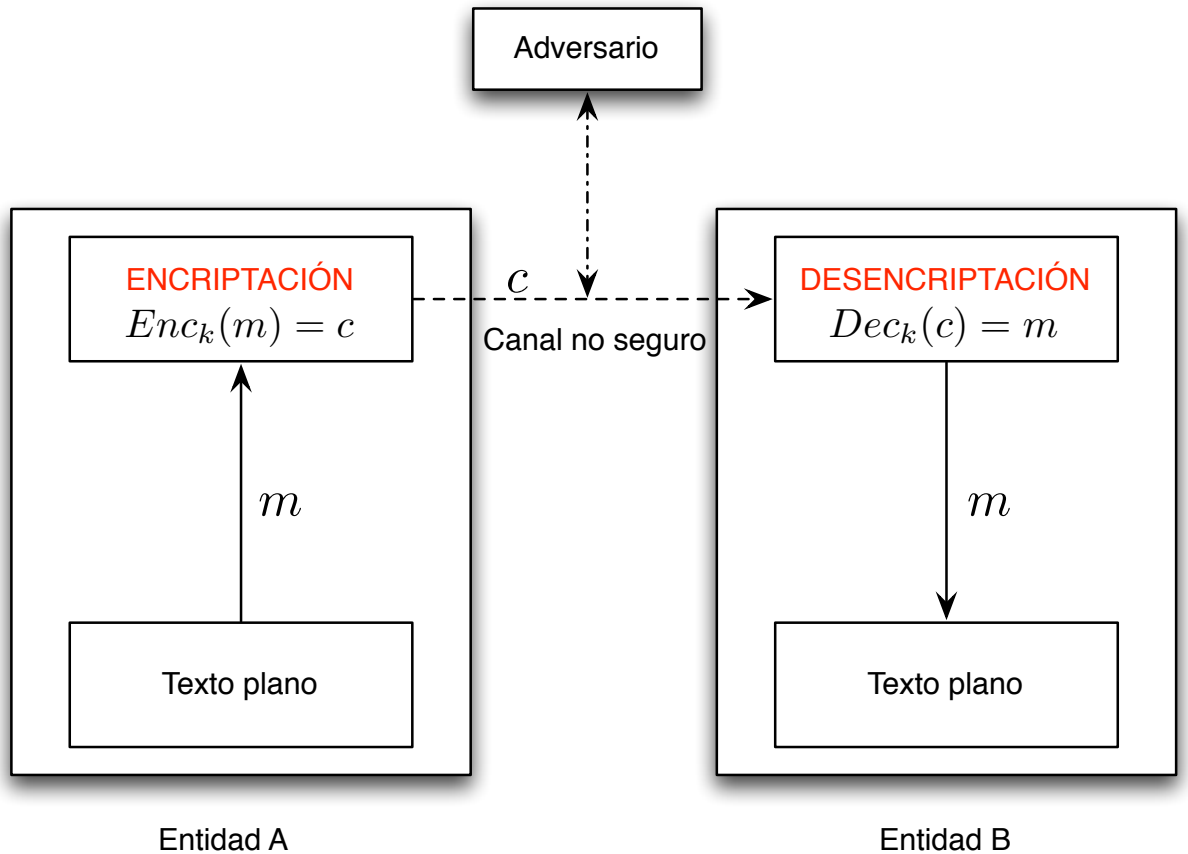
Ejemplo:

Esquema de cifrado de clave secreta

- Consta de 3 algoritmos: Gen, Enc y Dec
- $k \leftarrow Gen$ Genera la clave secreta
- $c \leftarrow Enc_k(m)$ Cifra el texto en claro
- $m \leftarrow Dec_k(c)$ Descifra el texto previamente cifrado
- Comprobación: $m \leftarrow Dec_k(Enc_k(m))$

Primitivas criptográficas III

Ejemplo: esquema de comunicación entre dos entidades usando encriptación:



Adaptado de Menzes et al. Handbook of Applied Cryptography (Ch. I)

Índice

1 Terminología e historia

2 Primitivas criptográficas

3 Nociones de criptoanálisis

Nociones de criptoanálisis I

Principio de Kerckhoff (s. XIX)

El adversario potencial conoce toda la información el esquema de encriptación que pretende atacar, con excepción de las claves secretas.

Nociones de criptoanálisis II

¿Quién obtiene más ventaja?

- Es difícil mantener el algoritmo de encriptación oculto
- Si el algoritmo fuese descubierto y hubiera que reemplazarlo sería muy costoso
- Permite comunicación bilateral en un grupo sólo utilizando claves distintas

De hecho, actualmente se prefiere hacer el esquema público:

- Otorga confianza a la seguridad del esquema
- La comunidad puede mejorarlo progresivamente: los fallos y las correcciones se detectan públicamente
- Permite establecer estándares.

Características de un buen Criptosistema

- Tanto en cifrado como el descifrado deben ser eficientes para todas las claves. Es decir, dados un mensaje m y la función de cifrado Enc_k, la obtención de $Enc_k(m)$ ha de ser fácil
- El sistema debe ser fácil de utilizar
- La seguridad del sistema debe depender únicamente de la privacidad de las claves y no del secreto de los algoritmos de cifrado y descifrado

Ataques a un sistema de cifrado
PASIVOS

- Ciphertext-only (**eav**): el adversario sólo tiene acceso a (1..n) textos cifrados
- Known-plaintext (**kpa**): el adversario tiene acceso a (1..n) pares del tipo:

$$\langle \underline{\text{texto en claro}}, \underline{\text{texto cifrado}} \rangle$$

Ataques a un sistema de cifrado
ACTIVOS

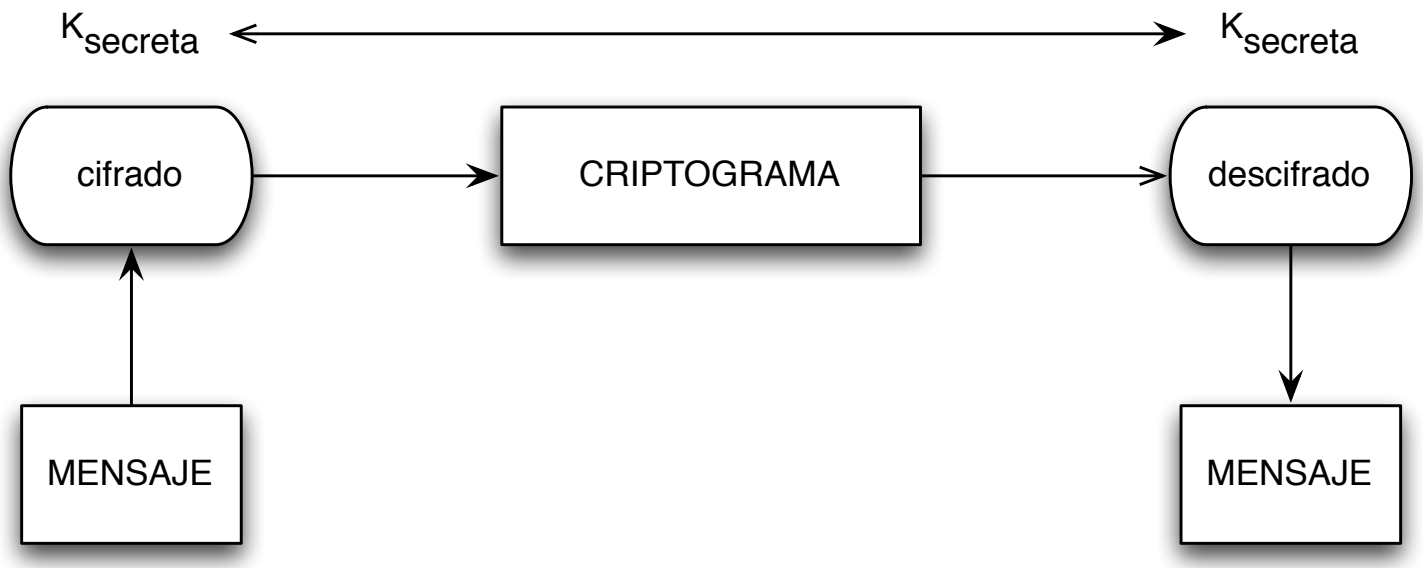
- Chosen-plaintext (**cpa**): el adversario puede ver el cifrado correspondiente a textos en claro de su elección (ENIGMA)
- Chosen-ciphertext (**cca**): el adversario puede elegir textos cifrados para observar cuál es el texto plano resultante

Otros:

- birthday, brute force, dictionary, differential, meet-in-the middle, middleperson, precomputation

Criptografía de clave simétrica I

Esquema:



Criptografía de clave simétrica II

Ejemplo: Algoritmo de César (Sustitución mono-alfabética) - $K = 3$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Codificar: ”**Atacar ahora**”
Mensaje encriptado:

”**xqxzxo xdlox**”

Criptografía de clave simétrica III

Ejemplo: Algoritmo de César (Sustitución poli-alfabética).
Período = 3, Clave $K = \{3, 17, 8\}$

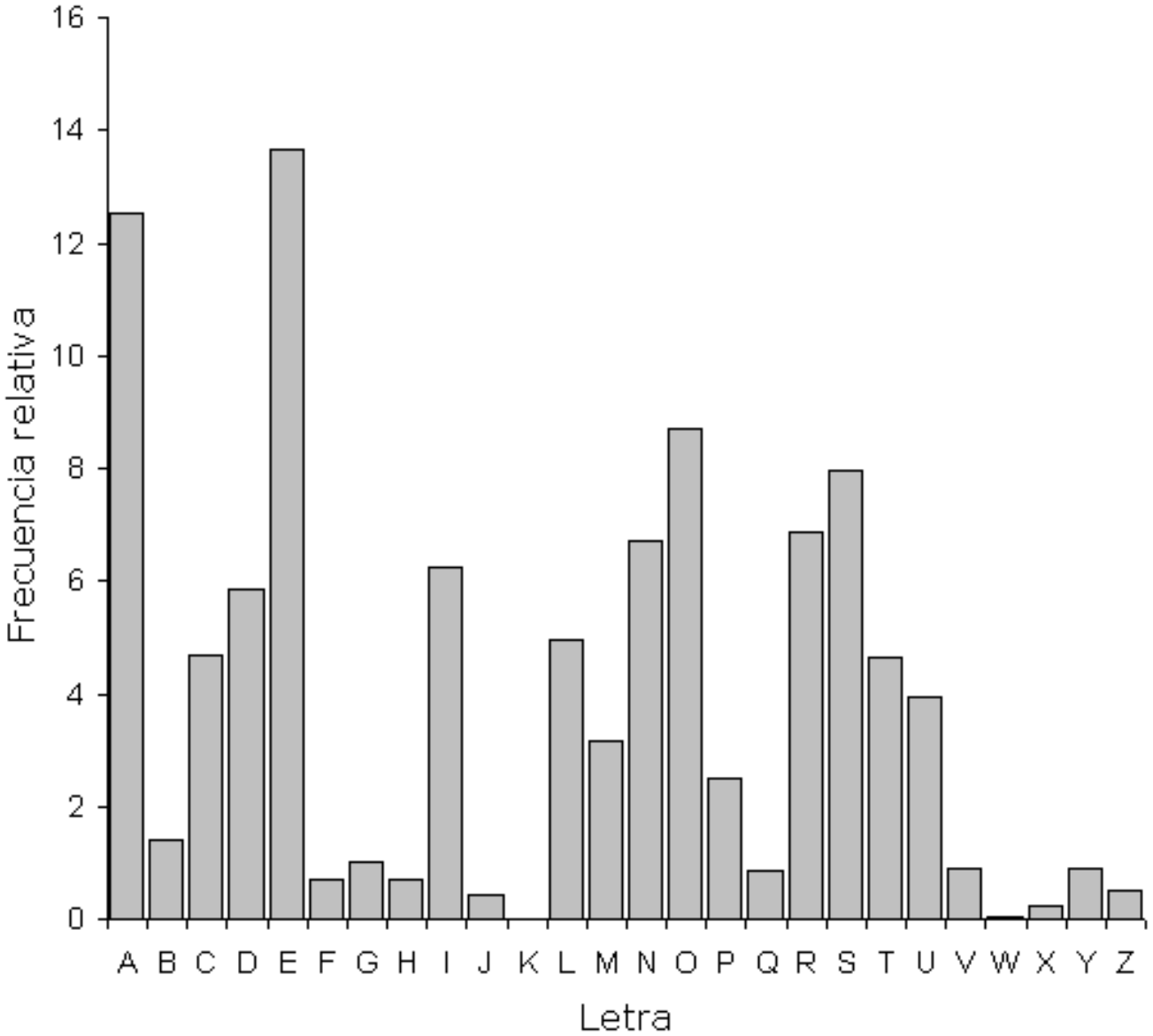
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Codificar: ”Invadir a medianoche”
Mensaje cifrado:

”**fwnxmao j ebmaxwgzqw**”

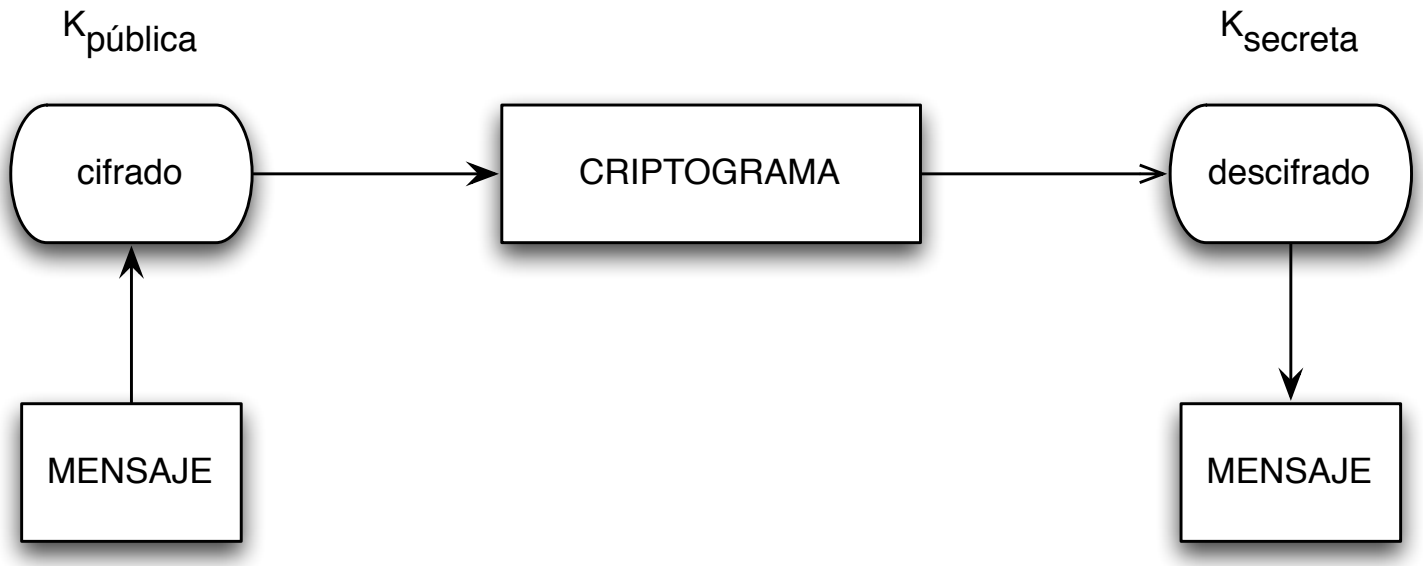
- ¿Problemas?

Criptografía de clave simétrica IV



Criptografía de clave pública I

Esquema:



Criptografía de clave pública II

- Funciones unidireccionales: $f : X \rightarrow Y$ es unidireccional si y solo si para todo $x \in X, f(x)$ es fácil de computar, pero para muchos elementos $y \in Y$, es *computacionalmente intratable* encontrar un $x \in X$ tal que $f(x) = y$

  Ejemplo: cálculo del logaritmo discreto

$$X = \{0, 1, 2, ..., 16\}, f(x) = 3^x \ mod \ 17$$

x	1	2	3	4	5	6	7	8	9	10
$f(x)$	3	9	10	13	5	15	11	16	14	8

Criptografía de clave pública III

- Función unidireccional con *trampa*: función unidireccional tal que cierta información adicional permite el cálculo rápido de la inversa

  Ejemplo: cálculo de $f(x) = x^3 mod\ n$ donde $n = p \cdot q$, con p y q, números primos. Si se conocen p y q es fácil calcular la inversa

Protocolos criptográficos I

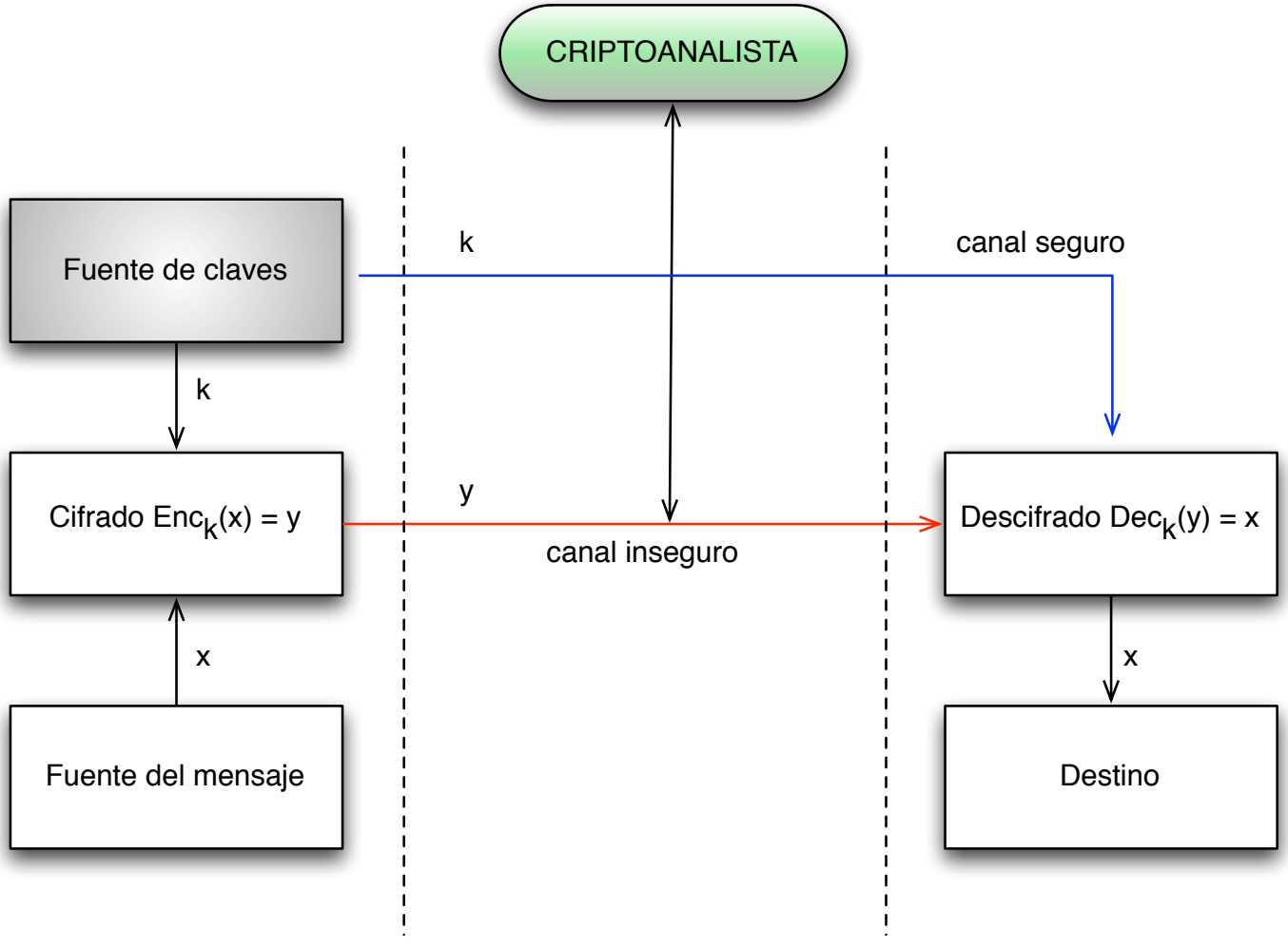
- **Protocolo**: secuencia de pasos que implican a dos o más partes y que están encaminados a cumplir un determinado objetivo
  - Todo implicado en el protocolo debe conocerlo de antemano, así como su papel en él
  - Los implicados deben estar de acuerdo en seguirlo
  - El protocolo no puede ser ambiguo (AFD)
  - El protocolo debe ser completo (una acción para cada posible situación)

Protocolos criptográficos II

- **Envío de mensajes**. Esquema simétrico (clave secreta):
  1. EMISOR y RECEPTOR acuerdan un algoritmo de cifrado
  2. EMISOR y RECEPTOR acuerdan una clave
  3. EMISOR cifra el mensaje utilizando el algoritmo y la clave acordadas
  4. EMISOR envía el criptograma a RECEPTOR
  5. RECEPTOR descifra el texto cifrado usando el mismo algoritmo y la misma clave
- ¿Número de claves para n usuarios?

Protocolos criptográficos III

Clave secreta:



Protocolos criptográficos IV

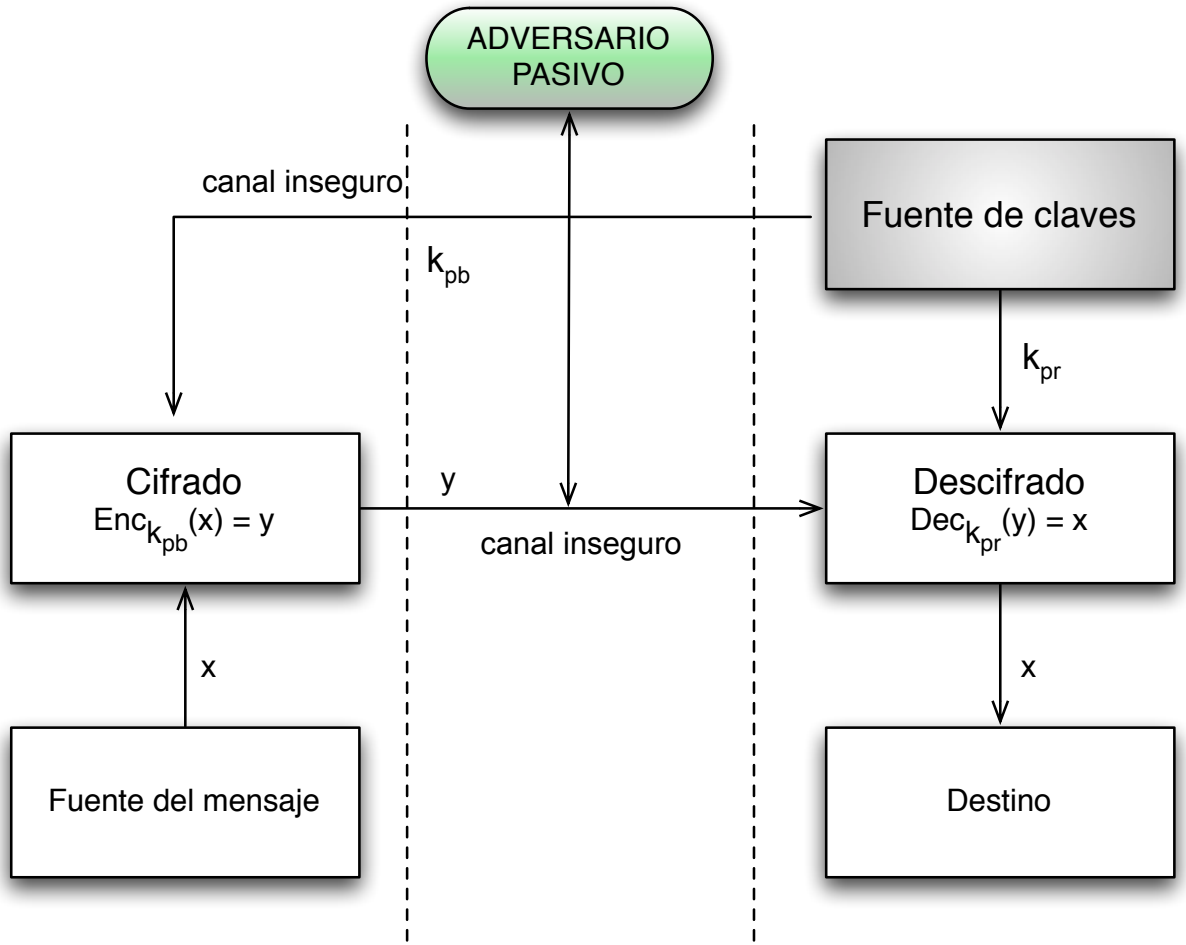
- **Envío de mensajes**. Esquema público (clave pública) (I):
  1. EMISOR y RECEPTOR acuerdan un algoritmo de cifrado
  2. RECEPTOR envía a EMISOR su clave pública
  3. EMISOR cifra el mensaje utilizando el algoritmo acordado y la clave pública del RECEPTOR
  4. EMISOR envía el criptograma a RECEPTOR
  5. RECEPTOR descifra el texto mensaje cifrado utilizando el mismo algoritmo y su clave secreta
- ¿Número de claves para n usuarios?

Protocolos criptográficos V

- **Envío de mensajes**. Esquema público (clave pública) (II):
  1. Un conjunto de de usuarios acuerdan un algoritmo de cifrado y publican sus claves públicas en una base de datos accesible a todos
  2. EMISOR toma de la base de datos la clave pública del RECEPTOR del mensaje
  3. EMISOR cifra el mensaje utilizando el algoritmo acordado y la clave pública de RECEPTOR
  4. EMISOR envía el criptograma a RECEPTOR
  5. RECEPTOR descifra el mensaje cifrado usando el mismo algoritmo y su clave secreta

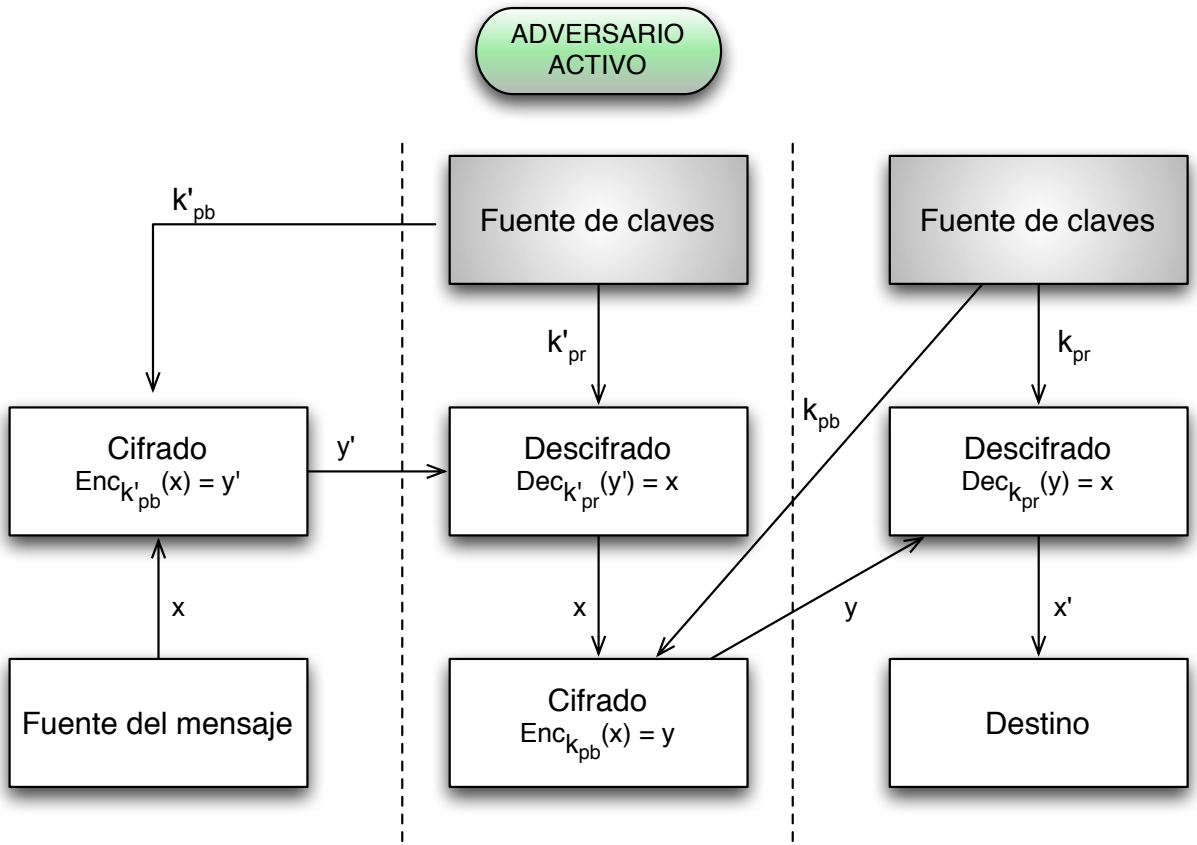
Protocolos criptográficos VI

Clave pública (i):



Protocolos criptográficos VII

Clave pública (ii):



Protocolos criptográficos VIII

- **Envío de mensajes**. Esquema híbrido
  1. EMISOR y RECEPTOR acuerdan dos algoritmos de cifrado: uno de clave pública y otro de clave secreta
  2. RECEPTOR genera un par de claves y comunica a EMISOR su clave pública
  3. EMISOR genera una clave de sesión K
  4. EMISOR cifra la clave de sesión utilizando la clave pública de RECEPTOR y se la envía a éste
  5. RECEPTOR descifra la clave de sesión de EMISOR descifrándola con su clave secreta
  6. EMISOR y RECEPTOR pueden establecer una comunicación segura utilizando el algoritmo de clave secreta