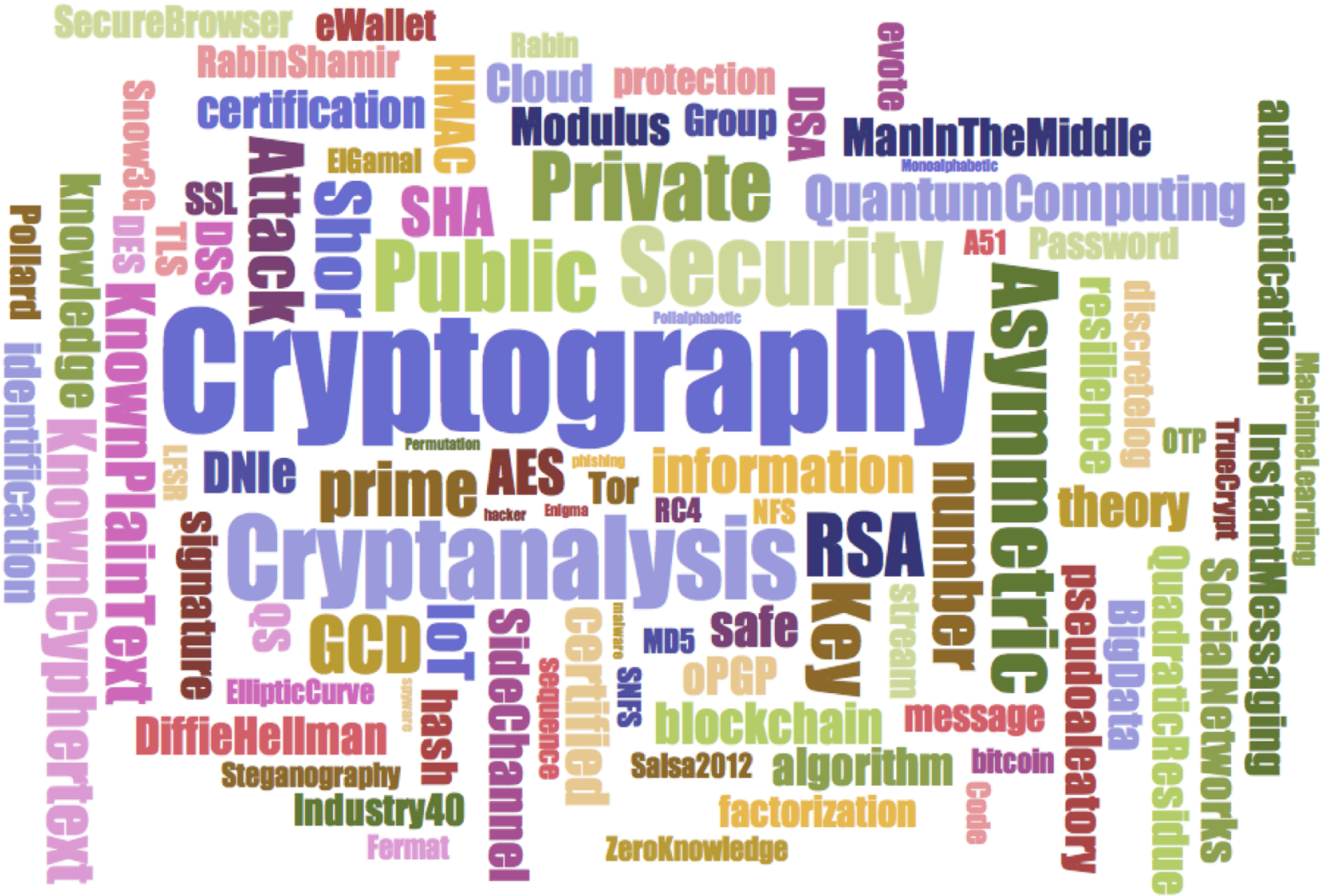
Introducción a la Criptografía

DSIC-UPV

Contenido

Bibliografía

- Handbook of applied crytography. *A. J. Menezes, P. C. van Oorshot and S. A. Vanstone*. CRC Press. 1996.


SecureBrowser
eWallet
RabinShamir
Rabin
HMAC
Cloud
protection
evote
certification
Modulus
Group
DSA
ManInTheMiddle
Monoalphabetic
Snow3G
DES
TLS
SSL
DSS
Attack
Shor
ElGamal
SHA
Private
QuantumComputing
authentication
Pollard
knowledge
KnownPlainText
Public
Security
A51
Password
Polialphabetic
Cryptography
Asymmetric
resilience
discretelog
identification
KnownCyphertext
Permutation
LFSR
DNIe
prime
AES
phishing
Tor
information
OTP
TrueCrypt
InstantMessaging
MachineLearning
hacker
Enigma
RC4
NFS
theory
Cryptanalysis
RSA
number
signature
QS
GCD
IoT
SideChannel
malware
certified
MD5
safe
Key
stream
pseudoaleatory
BigData
QuadraticResidue
SocialNetworks
EllipticCurve
sequence
SNFS
oPGP
blockchain
message
DiffieHellman
hash
Salsa2012
algorithm
bitcoin
Steganography
Code
Industry40
factorization
Fermat
ZeroKnowledge

Historia

Historia

- Nacimiento criptografía moderna
  - Segunda Guerra mundial. Proyecto ULTRA (Blentchley Park, A. Turing) con objeto de romper el sistema ENIGMA
  - Coincide con lo que podría considerarse el primer computador.
- Años 60 y 70 del s.XX
  - La expansión de la computadora y las redes de comunicación proporciona un gran impulso a la criptografía
  - Investigaciones (en su mayoría) a cargo de la NSA de los EEUU
  - Sólo recientemente se desarrolla una investigación univesitaria en criptografía, con resultados publicados en revistas y congresos.
    En este contexto nace la criptografía de clave pública (Diffie Hellman '76 y RSA '78)

Historia

- En paralelo con el desarrollo de la criptografía, los gobiernos (especialmente EEUU) intentan controlar los avances en criptografía
  - Debilitación *deliberada (?)* del algoritmo de los teléfonos GSM
  - Denuncias de la existencia de una *puerta trasera* en el codigo criptgráfico de S.S.O.O. (Windows 1999)
  - Las versiones que se exportan de los navegadores más extendidos incorporan seguridad débil (las conexiones seguras no lo son, no siendo consciente de ello el usuario)
- El software criptográfico en EEUU está sujeto a las mismas leyes que el armamento nuclear (misma tendencia en la UE)

Historia

- Intención gubernamental de almacenar las claves individuales de los ciudadanos, considerando ilegales las no registradas
- Echelon: red gestionada por la NSA (USA) junto con Gran Bretaña, Canadá, Australia y Nueva Zelanda para monitorizar las comunicaciones. Existencia hecha pública en 1976. Pretexto: guerra fría.

Historia

- Intención gubernamental de almacenar las claves individuales de los ciudadanos, considerando ilegales las no registradas
- Echelon: red gestionada por la NSA (USA) junto con Gran Bretaña, Canadá, Australia y Nueva Zelanda para monitorizar las comunicaciones. Existencia hecha pública en 1976. Pretexto: guerra fría.
- Enfopol: versión europea de Echelon (Existencia conocida desde 1997). Se inicia con la *Resolución sobre Interceptación Legal de las Comunicaciones (1995)*. Pretexto: lucha antiterrorista

Historia

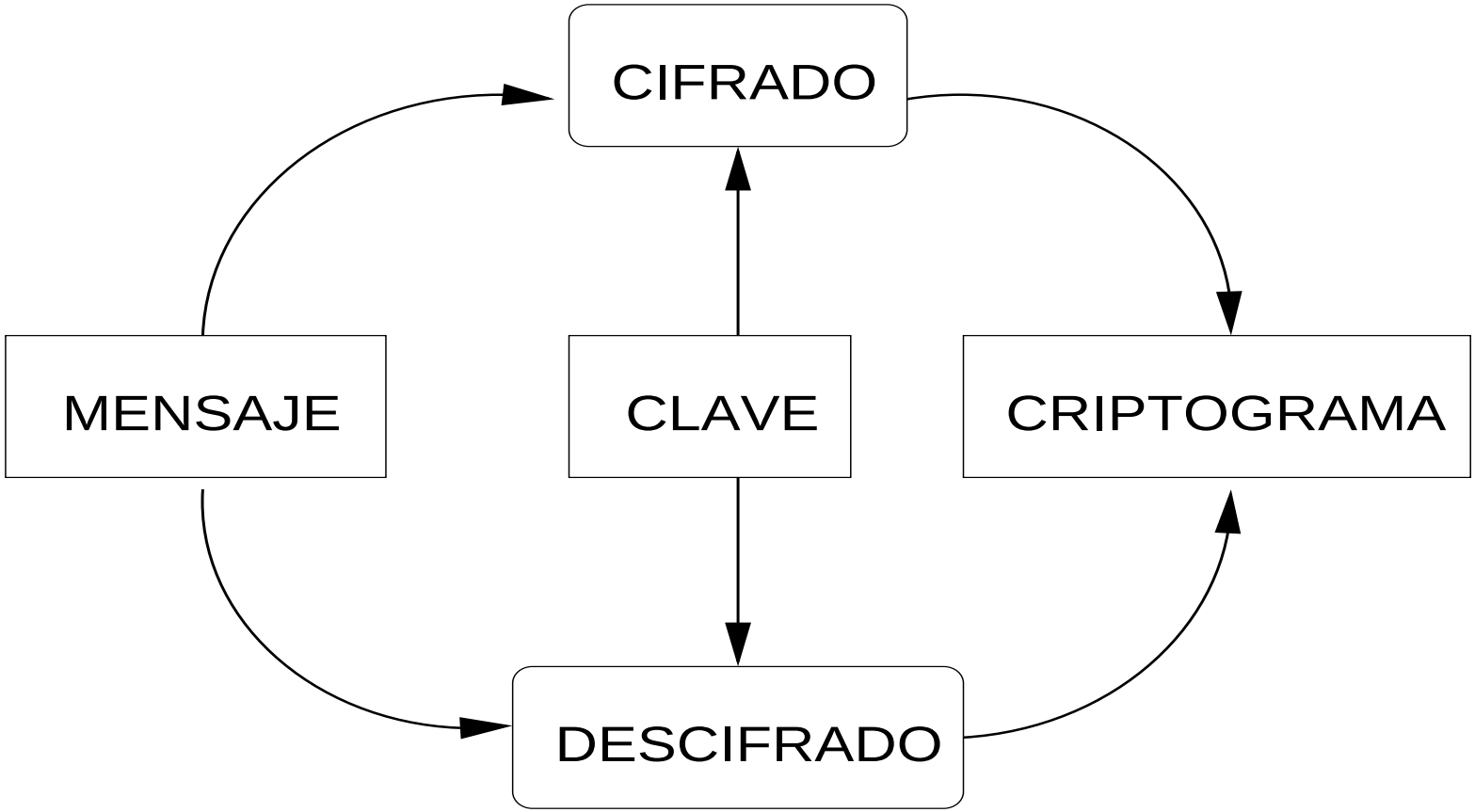
Recientemente:

- Control de la web por parte del gobierno de China (p.e. Weibo, versión twitter)
- Caso Snowden.
  - PRISM (2007). Programa de la NSA (parte de Echelon). Tiene como objetivo capturar los datos de compañías líderes en tecnológias de la información (Google, Apple, Microsoft o Facebook)
  - Escuchas por parte de USA de gobiernos de paises europeos
- OSEMINTI: proyecto de España, Francia e Italia. Se apoya en la ley de retención de datos europea, que regula la guarda de datos de las comunicaciones telefónicas y por Internet durante el plazo de dos años.

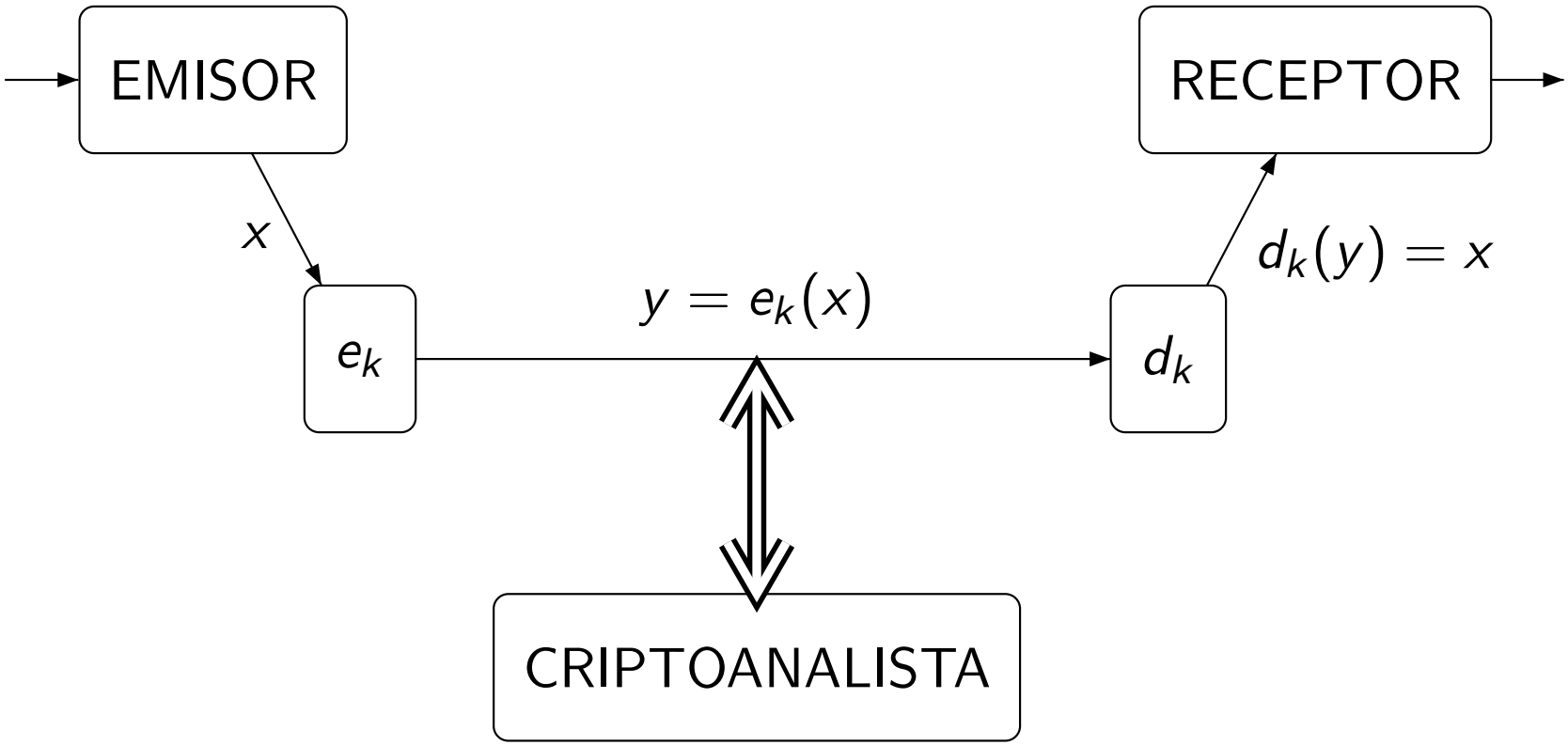
Conceptos básicos

Conceptos básicos: Sistema criptográfico
Procesos

Conceptos básicos: Sistema criptográfico
Procesos



Conceptos básicos: Sistema criptográfico
Participantes



- Consideraremos únicamente ataques lógicos

Confidencialidad : ocultar el contenido de la información salvo para aquellos autorizados. Fundamentalmente, aprovechando resultados de la teoría de números

Accesibilidad : asegurar quien, y en qué momento, puede acceder a una información

Autenticidad : el receptor de un mensaje debe poseer la certeza de su origen

Integridad : seguridad, para el receptor, de que el mensaje no ha sido modificado, así como posibilidad de detectar su posible manipulación

No repudio : Imposibilidad por parte del emisor de negar la autoría de un mensaje

Criptosistema
Características deseables

1. Cifrado y descifrado eficiente independientemente de la clave escogida:

   Dado un mensaje x y la función de cifrado e_k, la obtención de $y = e_k(x)$ ha de ser *fácil*

   Dado un criptograma y y la función de descifrado d_k, la obtención de $x = d_k(y)$ ha de ser *fácil*
2. El sistema ha de ser fácilmente utilizable
3. La seguridad del sistema debe depender únicamente del secreto de las claves utilizadas y no del secreto de los algoritmos de cifrado y descifrado.

   Debe asumirse que estos son conocidos por cualquier criptoanalista

Criptoanálisis
Tipos de ataque

Solo texto cifrado : Se dispone de varios criptogramas cifrados con el mismo algoritmo. El objetivo es determinar los mensajes que generaron dichos criptogramas, o mejor, las claves utilizadas en el cifrado

Criptoanálisis
Tipos de ataque

Solo texto cifrado : Se dispone de varios criptogramas cifrados con el mismo algoritmo. El objetivo es determinar los mensajes que generaron dichos criptogramas, o mejor, las claves utilizadas en el cifrado

Mensaje conocido : Además de disponer de varios criptogramas, se dispone de los mensajes que los originaron. Se busca obtener las claves de cifrado

Criptoanálisis
Tipos de ataque

Solo texto cifrado : Se dispone de varios criptogramas cifrados con el mismo algoritmo. El objetivo es determinar los mensajes que generaron dichos criptogramas, o mejor, las claves utilizadas en el cifrado

Mensaje conocido : Además de disponer de varios criptogramas, se dispone de los mensajes que los originaron. Se busca obtener las claves de cifrado

Mensaje escogido : Se dispone, para un conjunto de mensajes escogidos, de un conjunto de criptogramas. Se busca obtener las claves de cifrado

Criptoanálisis
Tipos de ataque

Solo texto cifrado : Se dispone de varios criptogramas cifrados con el mismo algoritmo. El objetivo es determinar los mensajes que generaron dichos criptogramas, o mejor, las claves utilizadas en el cifrado

Mensaje conocido : Además de disponer de varios criptogramas, se dispone de los mensajes que los originaron. Se busca obtener las claves de cifrado

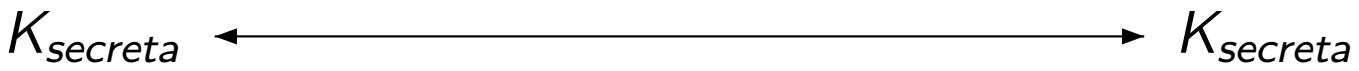
Mensaje escogido : Se dispone, para un conjunto de mensajes escogidos, de un conjunto de criptogramas. Se busca obtener las claves de cifrado

Criptograma escogido : A partir de varios criptogramas escogidos, se obtienen los mensajes que los generan. Esta información se utiliza para obtener la clave de cifrado. Útil para criptoanálisis de clave pública

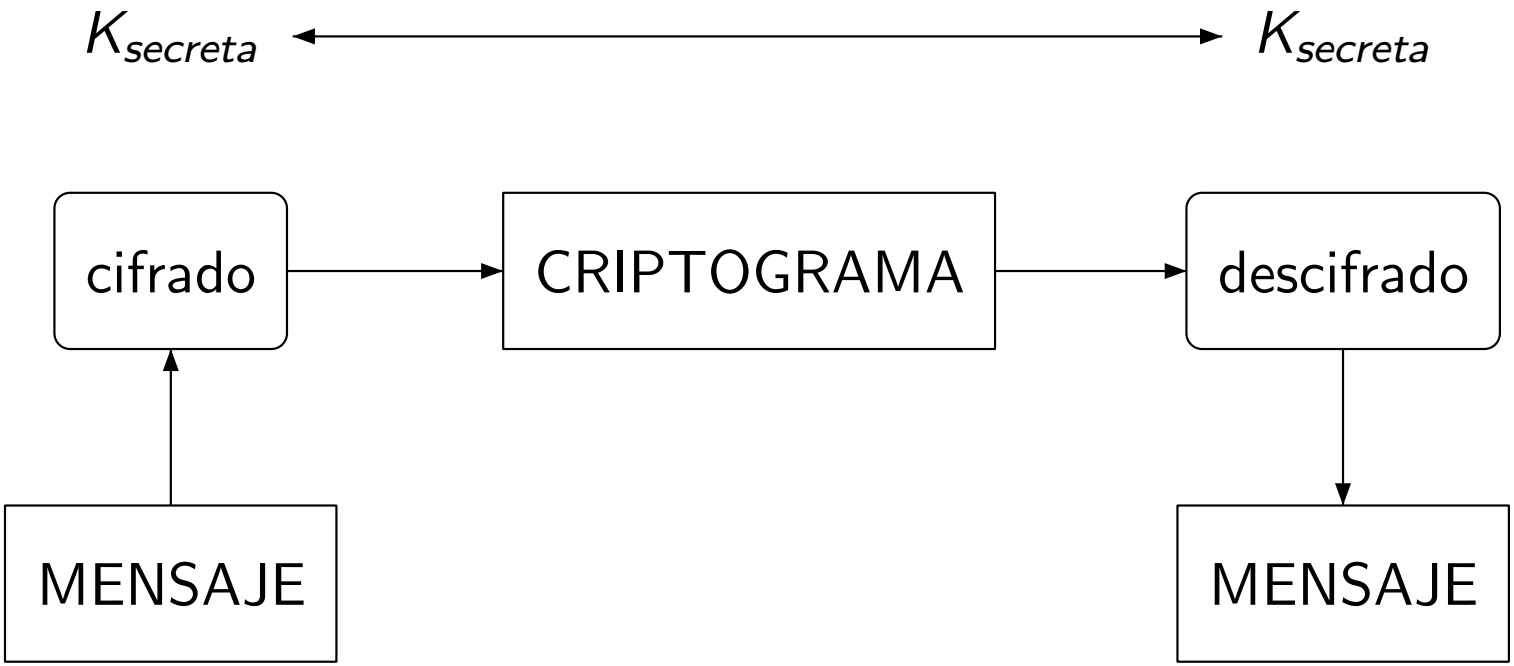
Principales aproximaciones

Criptografía de clave simétrica
Esquema

Criptografía de clave simétrica
Esquema



Criptografía de clave simétrica
Esquema



Criptografía de clave pública
Aproximaciones

- Uso de códigos
- Sistemas monoalfabéticos
- Sistemas polialfabéticos
- Sistemas poligráficos
- Cifrado por permutación
- Transformaciones variables en el tiempo
- Cifrado por bloques

Criptografía de clave pública
Esquema

Criptografía de clave pública
Esquema

$Extremo_A$
(K^A_{pb}, K^A_{pr})

$Extremo_B$
(K^B_{pb}, K^B_{pr})

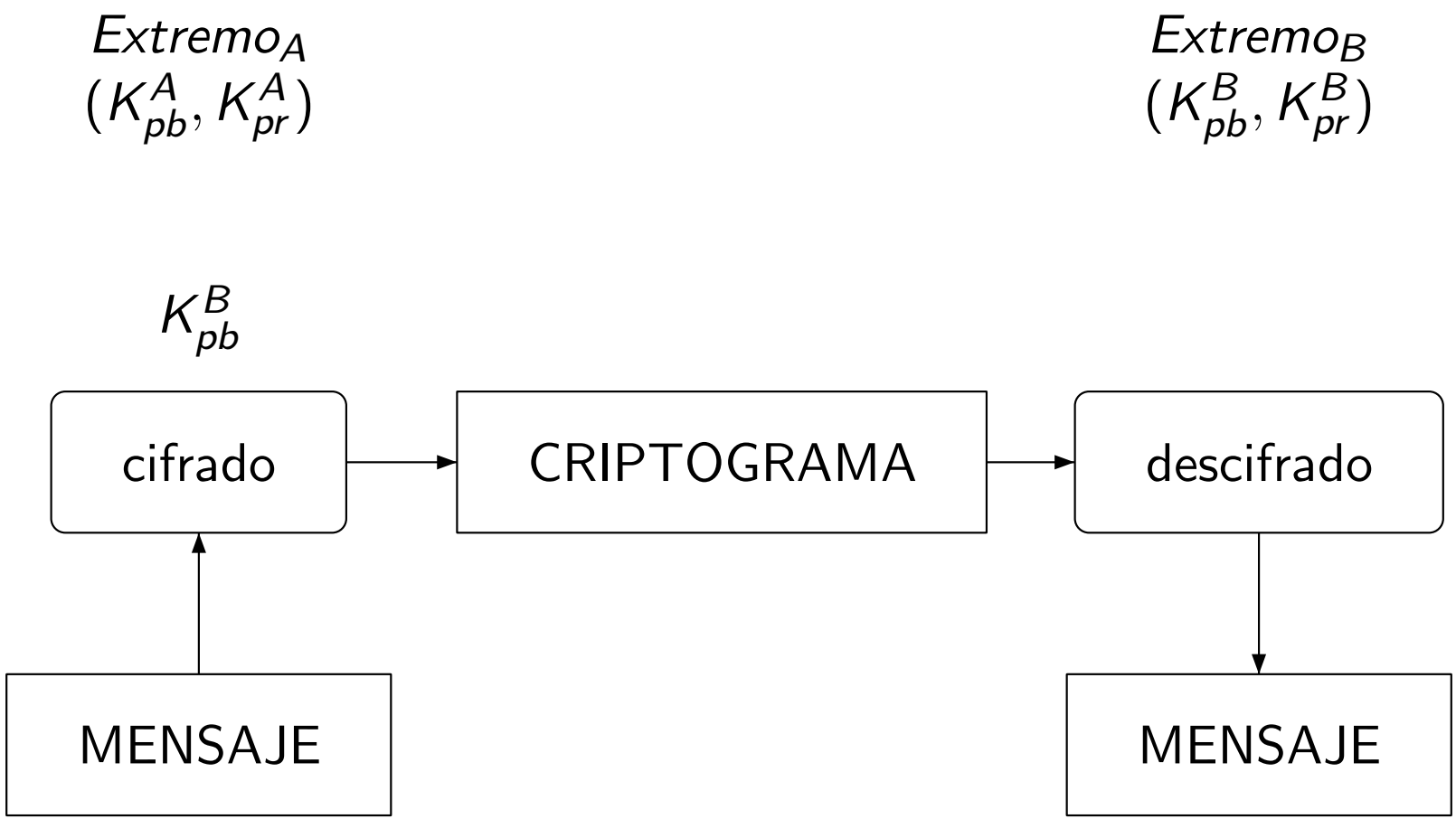
Criptografía de clave pública
Esquema

$Extremo_A$
(K^A_{pb}, K^A_{pr})

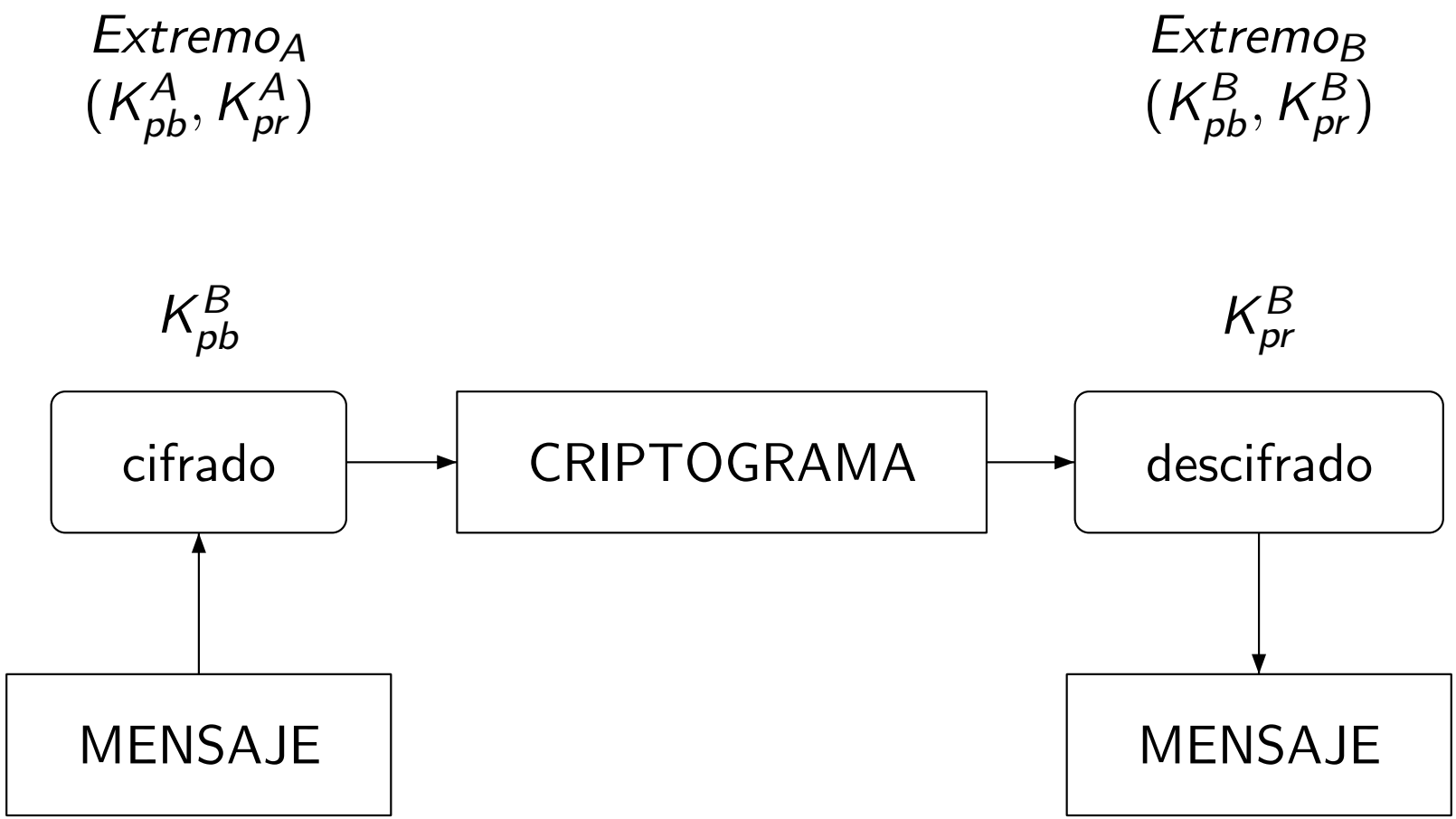
$Extremo_B$
(K^B_{pb}, K^B_{pr})

K^B_{pb}

Criptografía de clave pública
Esquema



Criptografía de clave pública
Esquema



Criptografía de clave pública
Función unidireccional

- Funciones unidireccionales: $f : X \to Y$ es unidireccional si y solo s para todo $x \in X$, $f(x)$ es fácil de computar, pero para *muchos* elementos $y \in Y$ es *computacionalmente intratable* encontrar $f^{-1}(y)$, por ejemplo, el *Logaritmo Discreto*

  p.e: $X = \{0, 1, \ldots, 16\}$, $f(x) = 3^x$ mód 17

x:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f(x):	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Criptografía de clave pública
Función unidireccional

- Funciones unidireccionales: $f : X \to Y$ es unidireccional si y solo s para todo $x \in X$, $f(x)$ es fácil de computar, pero para *muchos* elementos $y \in Y$ es *computacionalmente intratable* encontrar $f^{-1}(y)$, por ejemplo, el *Logaritmo Discreto*

  p.e: $X = \{0, 1, \ldots, 16\}$, $f(x) = 3^x$ mód 17

x:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f(x):	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

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

Criptografía de clave pública
Función unidireccional

- Funciones unidireccionales: $f : X \to Y$ es unidireccional si y solo s para todo $x \in X$, $f(x)$ es fácil de computar, pero para *muchos* elementos $y \in Y$ es *computacionalmente intratable* encontrar $f^{-1}(y)$, por ejemplo, el *Logaritmo Discreto*

  p.e: $X = \{0, 1, \ldots, 16\}$, $f(x) = 3^x$ mód 17

x:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f(x):	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

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

  p.e: Cálculo de $f(x) = 3^x$ mód n donde $n = pq$ con p, q primos. Si se conocen p y q entonces es fácil de calcular la inversa

Seguridad

Seguridad

Seguridad incondicional :

Seguridad computacional :

- El coste de obtener el mensaje supera el valor de este
- El tiempo necesario para obtener el mensaje supera la vida útil de la información contenida en él.

Se estima la vida del Universo en 14 mil millones de años...

Se estima la vida del Universo en 14 mil millones de años... (aprox. 2^{34} años).

Se estima la vida del Universo en 14 mil millones de años... (aprox. 2^{34} años).

número de segundos en un año: aprox. 2^{25}.

Se estima la vida del Universo en 14 mil millones de años... (aprox. 2^{34} años).

número de segundos en un año: aprox. 2^{25}.

número de segundos que han pasado desde el BigBang: 2^{60}.

Protocolos

Protocolo
Definición

- Protocolo: secuencia de pasos, que implican a dos o mas partes, encaminados a cumplir determinado objetivo
  - Todo implicado en el protocolo debe conocerlo a priori, así como su papel en él
  - Todos los implicados en el protocolo deben estar de acuerdo en seguirlo
  - El protocolo debe ser no ambiguo. Cada paso ha de estar bien definido
  - El protocolo debe ser completo. Debe especificar una acción para toda posible situación

Protocolo envío de mensajes cifrados
Criptografía de clave simétrica

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 acordados
4. EMISOR envía el mensaje a RECEPTOR
5. RECEPTOR descifra el mensaje utilizando el mismo algoritmo y la misma clave

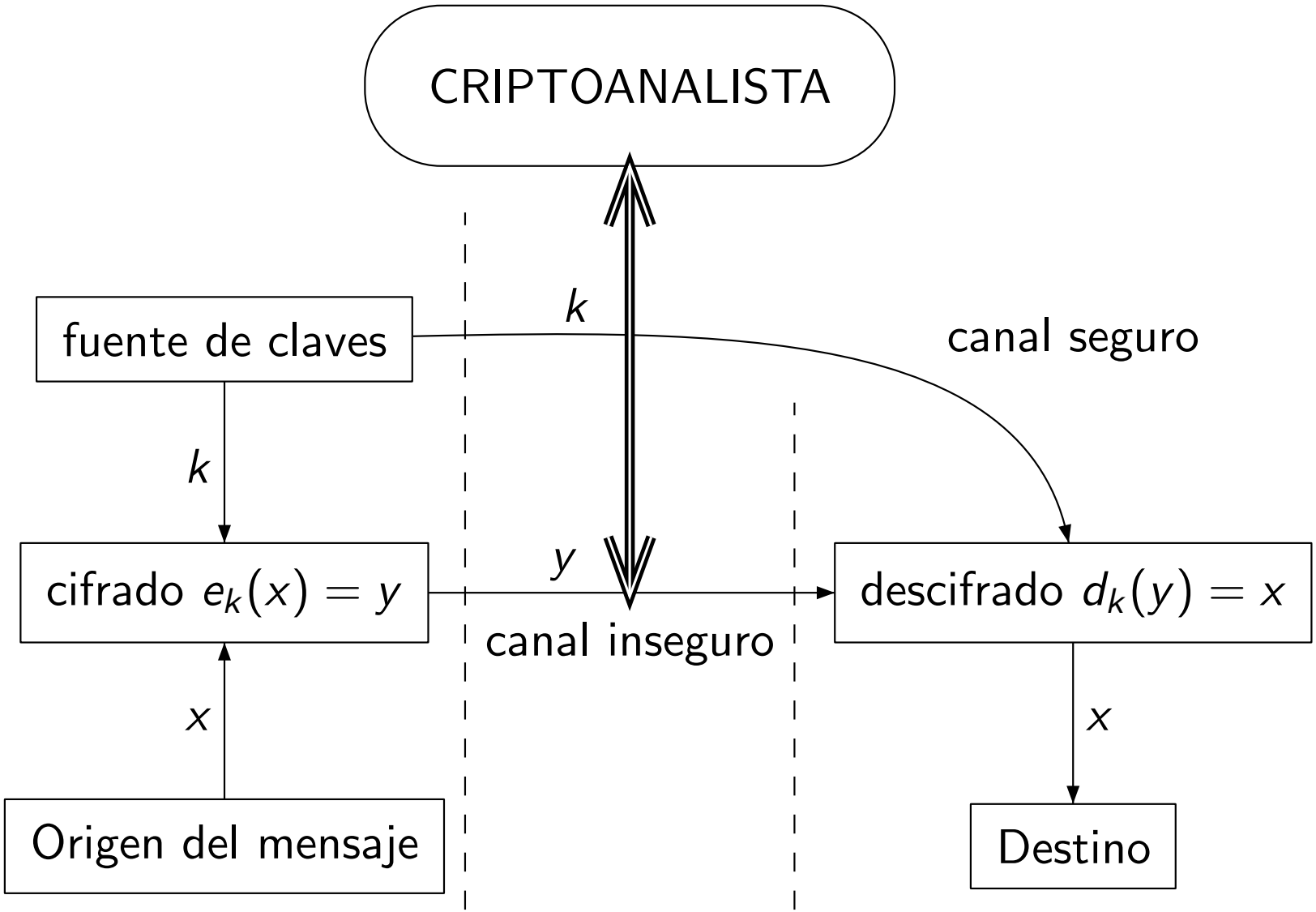
Protocolo envío de mensajes cifrados
Criptografía de clave simétrica

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 acordados
4. EMISOR envía el mensaje a RECEPTOR
5. RECEPTOR descifra el mensaje utilizando el mismo algoritmo y la misma clave

- ¿Número de claves para un colectivo de n usuarios?

Protocolo envío de mensajes cifrados

Clave simétrica: esquema



Protocolo envío de mensajes cifrados
Criptografía de clave asimétrica (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 y la clave pública recibida
4. EMISOR envía el mensaje a RECEPTOR
5. RECEPTOR descifra el mensaje utilizando el mismo algoritmo y la clave privada

Protocolo envío de mensajes cifrados
Criptografía de clave asimétrica (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 y la clave pública recibida
4. EMISOR envía el mensaje a RECEPTOR
5. RECEPTOR descifra el mensaje utilizando el mismo algoritmo y la clave privada

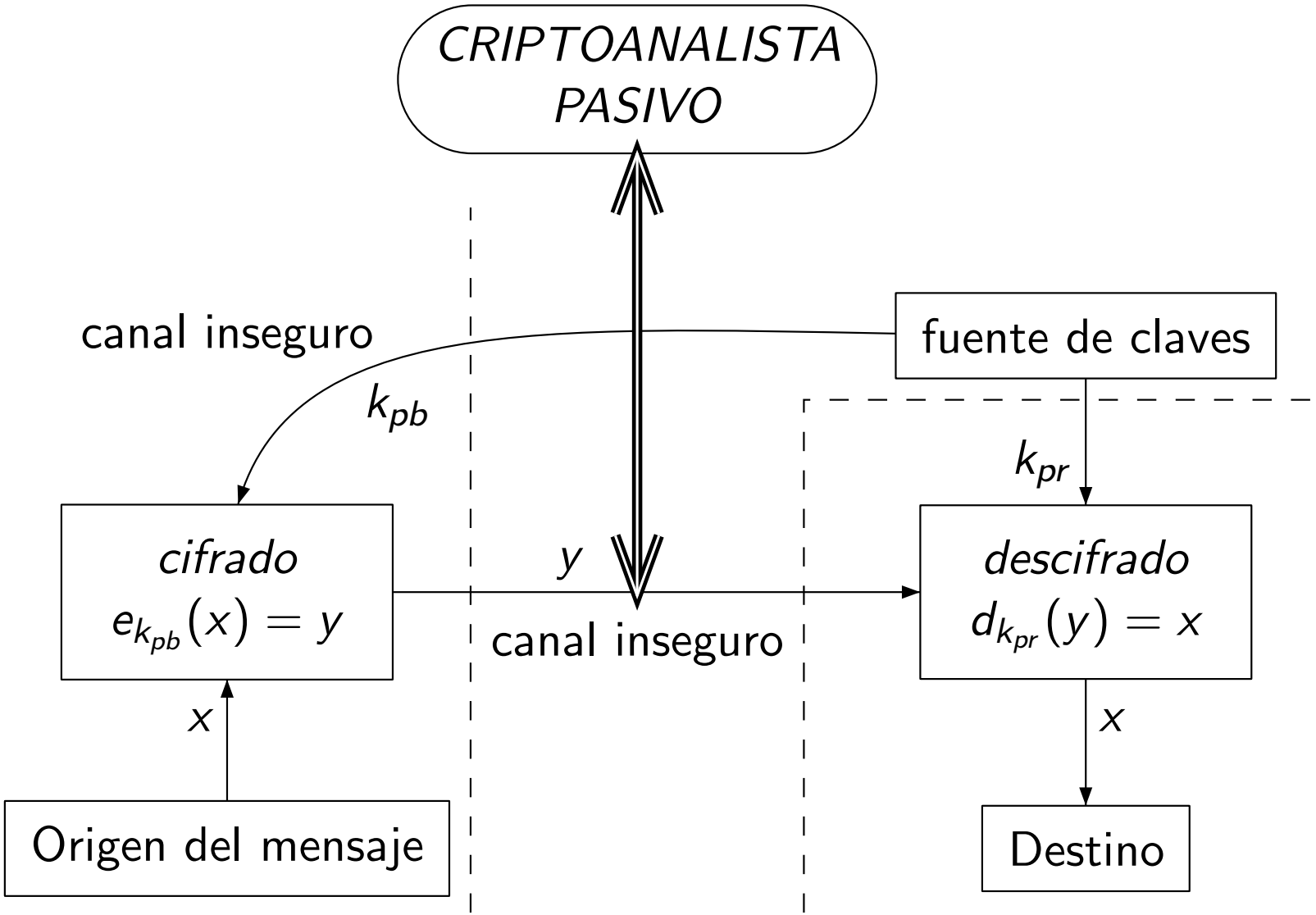
- ¿Número de claves para un colectivo de n usuarios?

Protocolo envío de mensajes cifrados
Criptografía de clave asimétrica (II)

1. Un conjunto 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 y la clave pública seleccionada
4. EMISOR envía el mensaje a RECEPTOR
5. RECEPTOR descifra el mensaje utilizando el mismo algoritmo y la clave privada

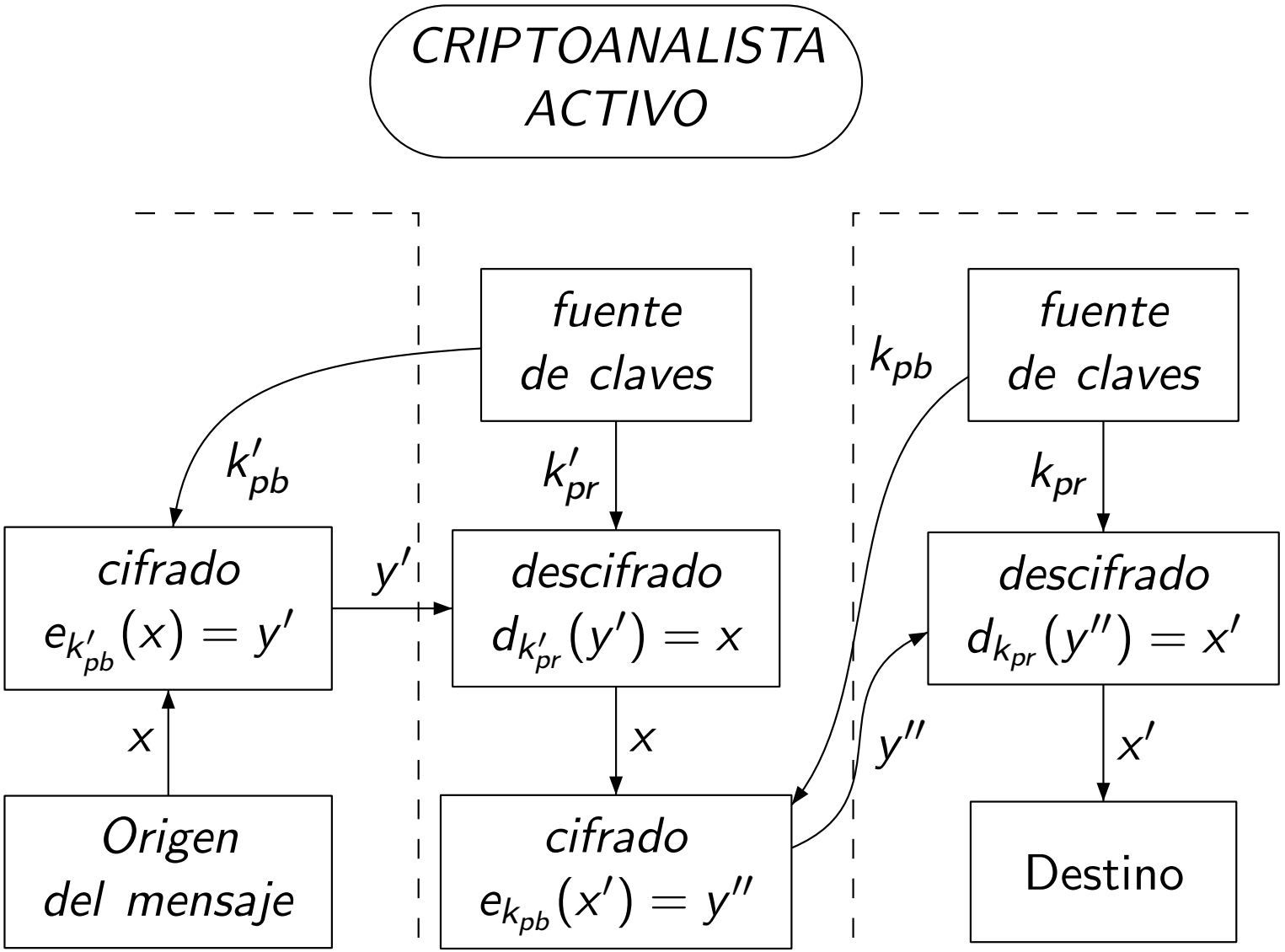
Protocolo envío de mensajes cifrados

Clave asimétrica: esquema



Protocolo envío de mensajes cifrados

Clave asimétrica: esquema



Protocolo envío de mensajes cifrados
Sistema híbrido

- Los sistemas de clave privada necesitan un canal seguro para comunicar la clave
- Los sistemas de cifrado de clave pública no son tan eficientes en tiempo como los sistemas de clave privada
- Una combinación de ambos permite conseguir las ventajas de las dos aproximaciones

Protocolo envío de mensajes cifrados
Sistema 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 (K_{pb}, K_{pr}) y comunica a EMISOR la parte pública
3. EMISOR genera una clave de sesión (criptografía de clave secreta)
4. EMISOR cifra el mensaje utilizando el algoritmo y la clave pública seleccionada
5. EMISOR envía el mensaje a RECEPTOR
6. RECEPTOR descifra el mensaje utilizando el mismo algoritmo y la clave privada

Firma digital
Propiedades

1. La firma ha de convencer al receptor que el emisor ha firmado el documento deliberadamente
2. La firma es infalsificable
3. La firma no debe ser reutilizable, debe formar parte del documento y no poderse trasladar a ningún otro
4. El documento no debe poder alterarse una vez firmado
5. El firmante no puede repudiar su firma

Protocolo firma digital
Clave simétrica

TESTIGO comparte con A y B sendas claves secretas k_A y k_B

1. A cifra el mensaje con k_A y lo envia a TESTIGO
2. TESTIGO lo descifra (utilizando k_A)
3. TESTIGO añade al texto una confirmación de su recepción proveniente de A
4. TESTIGO cifra el mensaje resultante con k_B y lo envia a B
5. B descifra el mensaje. Puede leer tanto el mensaje como la certificación

Protocolo firma digital
Clave simétrica

TESTIGO comparte con A y B sendas claves secretas k_A y k_B

1. A cifra el mensaje con k_A y lo envia a TESTIGO
2. TESTIGO lo descifra (utilizando k_A)
3. TESTIGO añade al texto una confirmación de su recepción proveniente de A
4. TESTIGO cifra el mensaje resultante con k_B y lo envia a B
5. B descifra el mensaje. Puede leer tanto el mensaje como la certificación

- TESTIGO necesita mantener una gran base de datos
- TESTIGO necesita ser infalible

Protocolo firma digital
Clave pública

Algunos sistemas de cifrado mediante clave pública pueden utilizarse como sistemas de firma

1. A firma el documento a enviar cifrandolo con su clave privada
2. A envia el criptograma a B
3. B descifra el documento con la clave pública de A verificando, al tiempo, la firma

Protocolo firma digital
Clave pública

Algunos sistemas de cifrado mediante clave pública pueden utilizarse como sistemas de firma

1. A firma el documento a enviar cifrandolo con su clave privada
2. A envia el criptograma a B
3. B descifra el documento con la clave pública de A verificando, al tiempo, la firma

Es innecesaria la existencia de un testigo para verificar la firma

Protocolo firma digital
Clave pública

Cada entidad dispone de dos pares de claves

- Claves pública/privada de firma: (F_A, V_A), (F_B, V_B)
- Claves pública/privada de cifrado: (C_A, D_A), (C_B, D_B)

1. A firma el mensaje x con su clave privada de firma: $F_A(x)$
2. A cifra el resultado con la clave pública de B: $C_B(F_A(x))$
3. A envia el resultado a B
4. B descifra el criptograma utilizando su clave privada (D_B): $D_B(C_B(F_A(x))) = F_A(x)$
5. B verifica el mensaje utilizando la clave pública de firma (V_A): $V_A(F_A(x)) = x$

Protocolo firma digital
Clave pública

Cada entidad dispone de dos pares de claves

- Claves pública/privada de firma: (F_A, V_A), (F_B, V_B)
- Claves pública/privada de cifrado: (C_A, D_A), (C_B, D_B)

1. A firma el mensaje x con su clave privada de firma: $F_A(x)$
2. A cifra el resultado con la clave pública de B: $C_B(F_A(x))$
3. A envia el resultado a B
4. B descifra el criptograma utilizando su clave privada (D_B): $D_B(C_B(F_A(x))) = F_A(x)$
5. B verifica el mensaje utilizando la clave pública de firma (V_A): $V_A(F_A(x)) = x$

IMPORTANTE: firmar antes de cifrar

Protocolo firma digital
Clave pública y funciones resumen

- Los algoritmos de clave pública no permiten firmar eficientemente documentos largos.
- Las funciones resumen (unidireccionales) permiten reducir el documento, ganando en eficiencia.
- La función resumen y el algoritmo de firma son acordados de antemano

Protocolo firma digital
Clave pública y funciones resumen

1. A produce un resumen de su documento
2. A firma (cifra) el resumen con su clave privada
3. A envía el documento y el resumen firmado a B
4. B calcula el resumen del documento, verifica la firma (descifra el resumen con la clave pública de A) y compara ambos resumenes, verificando si son iguales

Voto electrónico
Propiedades

Democracia : Únicamente los votantes incluídos en el **censo** pueden participar en el proceso y únicamente una vez.

Privacidad : No puede relacionarse voto y elector.

Seguridad : Nadie puede suplantar a un elector que decide no participar en el proceso.

Justicia : Nadie puede conocer el resultado de la votación antes de que esta finalice.

Resistencia Coercitiva : Ningún elector puede mostrar a un tercero el sentido de su voto.

Voto electrónico
Propiedades

Completitud: El resultado de la votación ha de ser preciso.

Precisión: Un voto emitido no puede ser alterado.
Un voto nulo no es contabilizado de otro modo.
Cada elector tiene la certeza de que su voto ha sido considerado.

Verficabilidad: (individual/universal) Los electores pueden verificar que (su/todo) voto ha sido considerado en el sentido en que se emitió.

Voto electrónico
Descripción del contexto

- Se propone un sistema basado en doble autoridad: Mesa de Identificación (MI) y Mesa Electoral (ME).
- Estas se reparten la responsabilidad del registro, validación, depósito y escrutinio.
- Se asume que ambas autoridades son independientes, no teniendo relación excepto para la comunicación de claves.
- En todo momento se asumen canales de comunicación seguros. En cualquier caso puede considerarse un protocolo de clave pública para implementar dichos canales.

Voto electrónico
Descripción de un protocolo

- La MI configura una clave pública (F_{MI}, V_{MI}) para ser utilizada como certificado, comunicando a la ME la parte pública (de verificación).
- Sea v la versión binaria del voto del elector. El elector genera un valor aleatorio h de la misma longitud de v. Sea $v' = v \oplus h$. El elector mantiene el valor de h secreto.
- El elector comunica a la MI el par $\langle v', id \rangle$
- La MI comprueba si el id del elector pertenece al censo. En este caso firma el voto del elector $RSA_{F_{MI}}(v')$ comunicando el resultado al elector.
- El elector puede comprobar en este momento la corrección del proceso, comunicando posteriormente a la urna el par $\langle RSA_{F_{MI}}(v'), h \rangle$.
- La urna verifica la firma del voto obteniendo v'. El voto se obtiene despues de computar $v = v' \oplus h$.