Criptografía

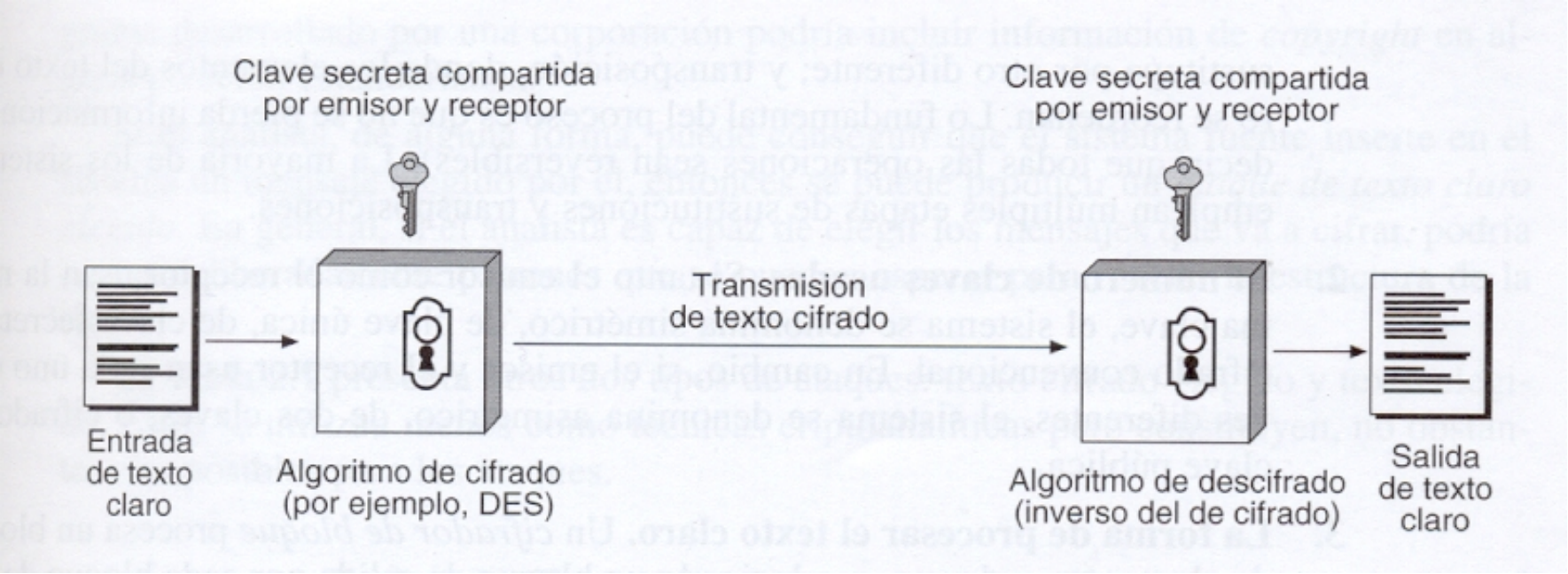
Temario

- Criptografía de llave secreta (simétrica)
  - Algoritmos de cifrado
  - Definir el problema con este tipo de cifrado
- Criptografía de llave pública (asimétrica)
  - Algoritmos de cifrado
  - Definir el problema con este tipo de cifrado
  - Firmas digitales
  - Sobres digitales
  - Certificado digital
    - Autoridad certificadoras

Definición de Criptografía

- La criptografía proviene del griego kryptos: "ocultar", y grafos: "escribir". Es decir, significa "escritura oculta". Como concepto son las técnicas utilizadas para cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Esquema de cifrado simétrico



Los sistemas criptográficos se clasifican en:

a) El número de claves usadas
b) El tipo de operación utilizado para transformar el texto claro en texto cifrado
c) La forma de procesar el texto claro

El número de claves usadas

- Si tanto el emisor como el receptor usan la misma clave, el sistema se denomina simétrico, de clave única, de clave secreta o cifrado convencional. En cambio, si el emisor y el receptor usan cada uno claves diferentes, el sistema se denomina asimétrico, de dos claves o cifrado de clave pública.

El tipo de operación utilizado para transformar el texto claro en texto cifrado

- Todos los algoritmos de cifrado se basan en dos principios: sustitución* y transposición*. Lo fundamental es que todas las operaciones sean inversas (descifrar).

La forma de procesar el texto claro

- Un cifrador de bloques procesa un bloque de elementos cada vez, produciendo un bloque de salida por cada bloque de entrada. Un cifrador de flujo procesa los elementos de entrada continuamente, produciendo la salida de un elemento cada vez.

Criptoanálisis

- Es el proceso por el que se intenta descubrir un texto claro o una clave de cifrado. La estrategia usada por el criptoanalista depende de la naturaleza del esquema de cifrado y de la información disponible.

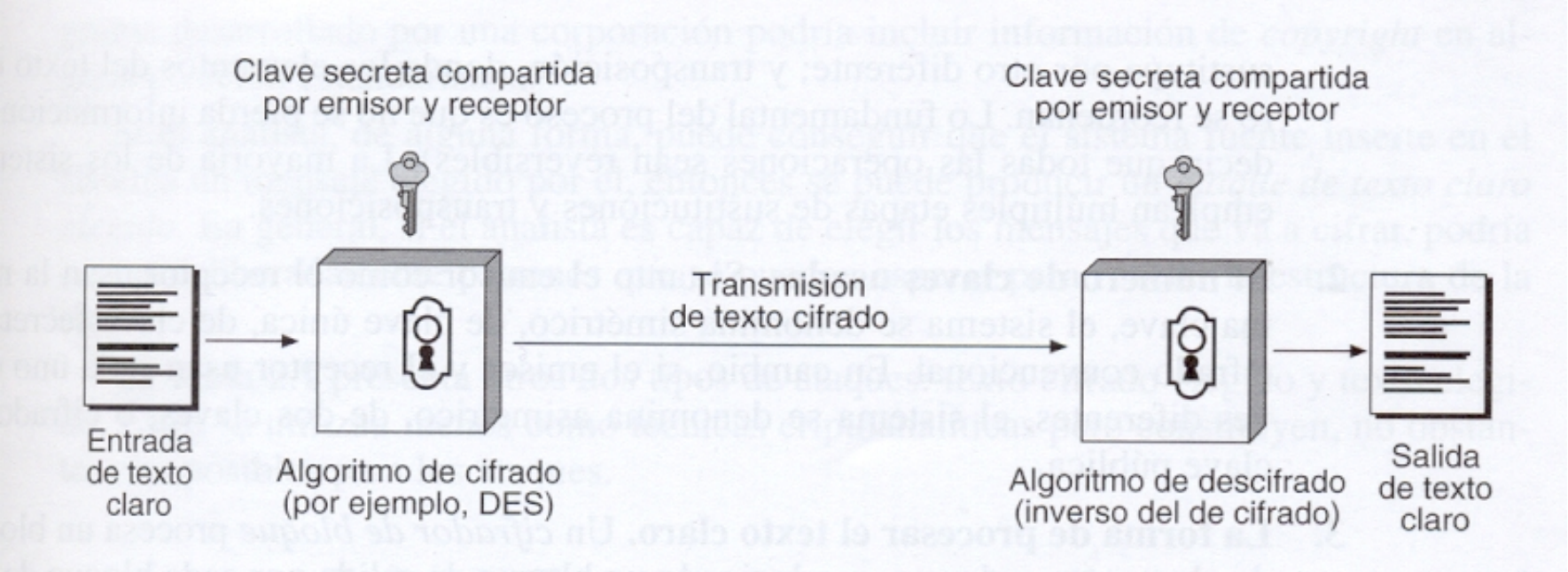
Ataque de fuerza bruta

- Implica intentar cada clave posible hasta que se obtenga la traducción legible del texto cifrado al texto claro
- Como promedio, se debe intentar la mitad de todas las claves posibles para conseguir descubrirla

Tiempo medio para la búsqueda exhaustiva de claves

Tamaño de clave (bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/μs	Tiempo necesario a 10^6 cifrado/μs
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1.142 años	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	21^{27} μs = 5,4 x 10^{24} años	5,4 x 10^{18} años
168	$2^{168} = 3{,}7 \times 10^{50}$	21^{67} μs = 5,9 x 10^{36} años	5,9 x 10^{30} años

Esquema de cifrado simétrico

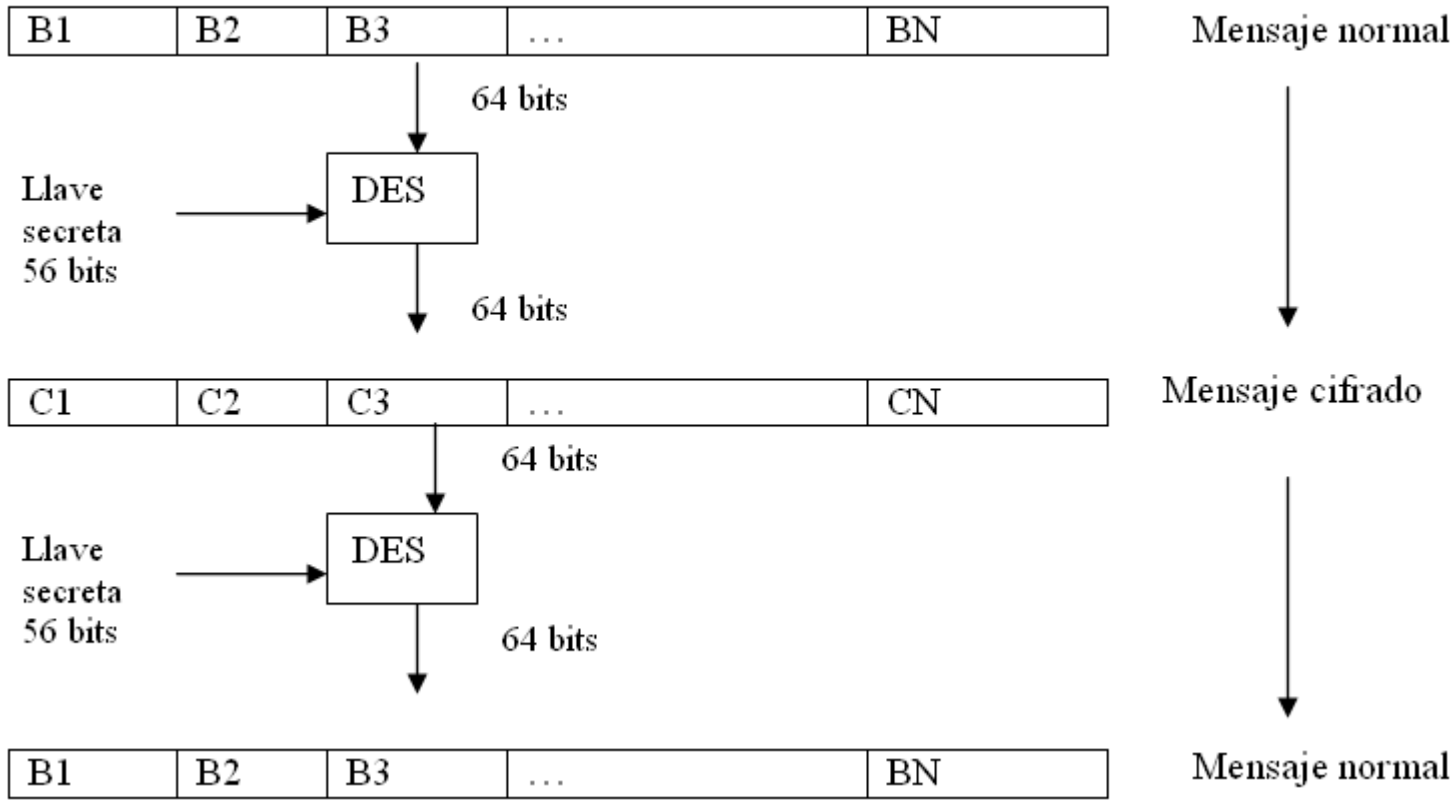


DES (Data Encryption Standard)

- El texto en claro tiene una longitud de 64 bits y la clave de 56; si el texto es más largo se procesa en bloques de 64 bits.
- El cifrado y descifrado de cada bloque de 64 bits es realizado mediante:
  - Permutaciones de bits
  - Sumas binarias tipo XOR entre los datos y la llave secreta
  - Funciones de sustitución que mediante tablas fijas mapean un grupo de bits a un grupo de bits diferente.

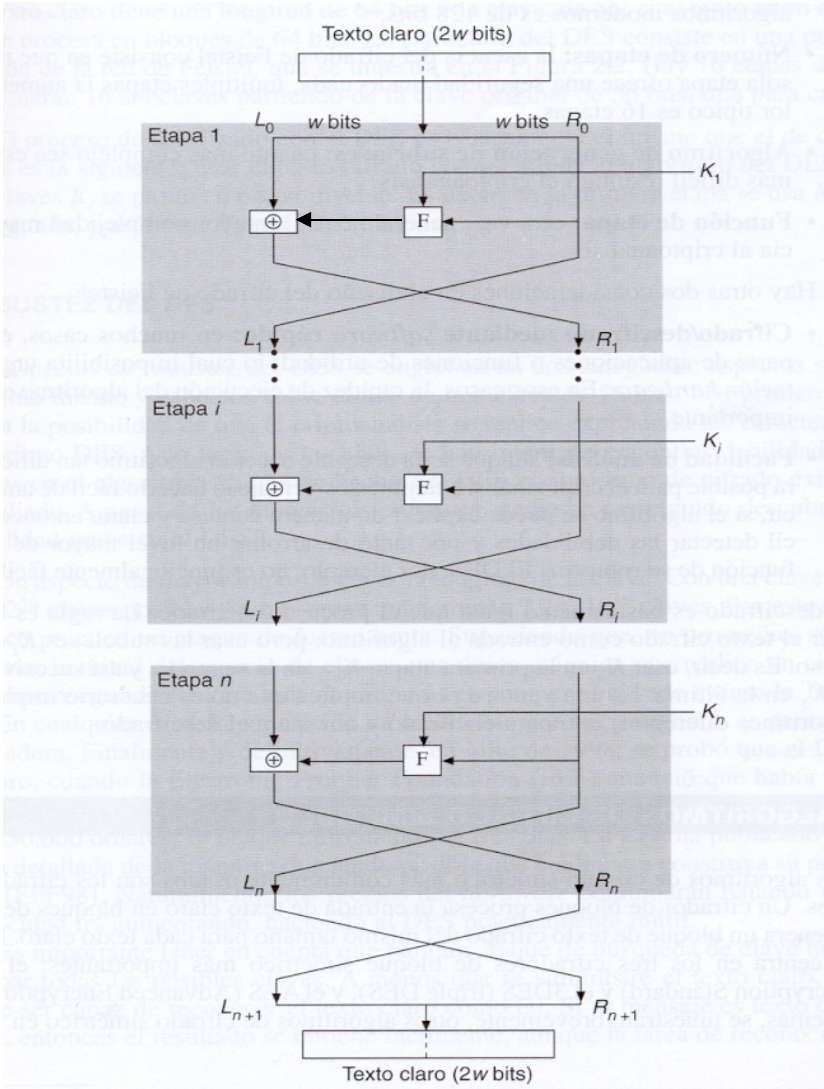
DES (Data Encryption Standard)

Modo en que trabaja:



Estructura de los algoritmos de C.S. incluido el DES

- 16 etapas de proceso.
- Se generan 16 subclaves partiendo de la clave original de 56 bits, una para cada etapa



Descifrado

- El proceso de descifrado del DES es básicamente el mismo que el de cifrado. Simplemente se utiliza el texto cifrado como entrada al algoritmo del DES, pero las subclaves K_i se pasan en orden inverso. Es decir, en la primera etapa se usa K_{16}, K_{15} en la segunda y así hasta K_1 en la 16ª y última etapa.

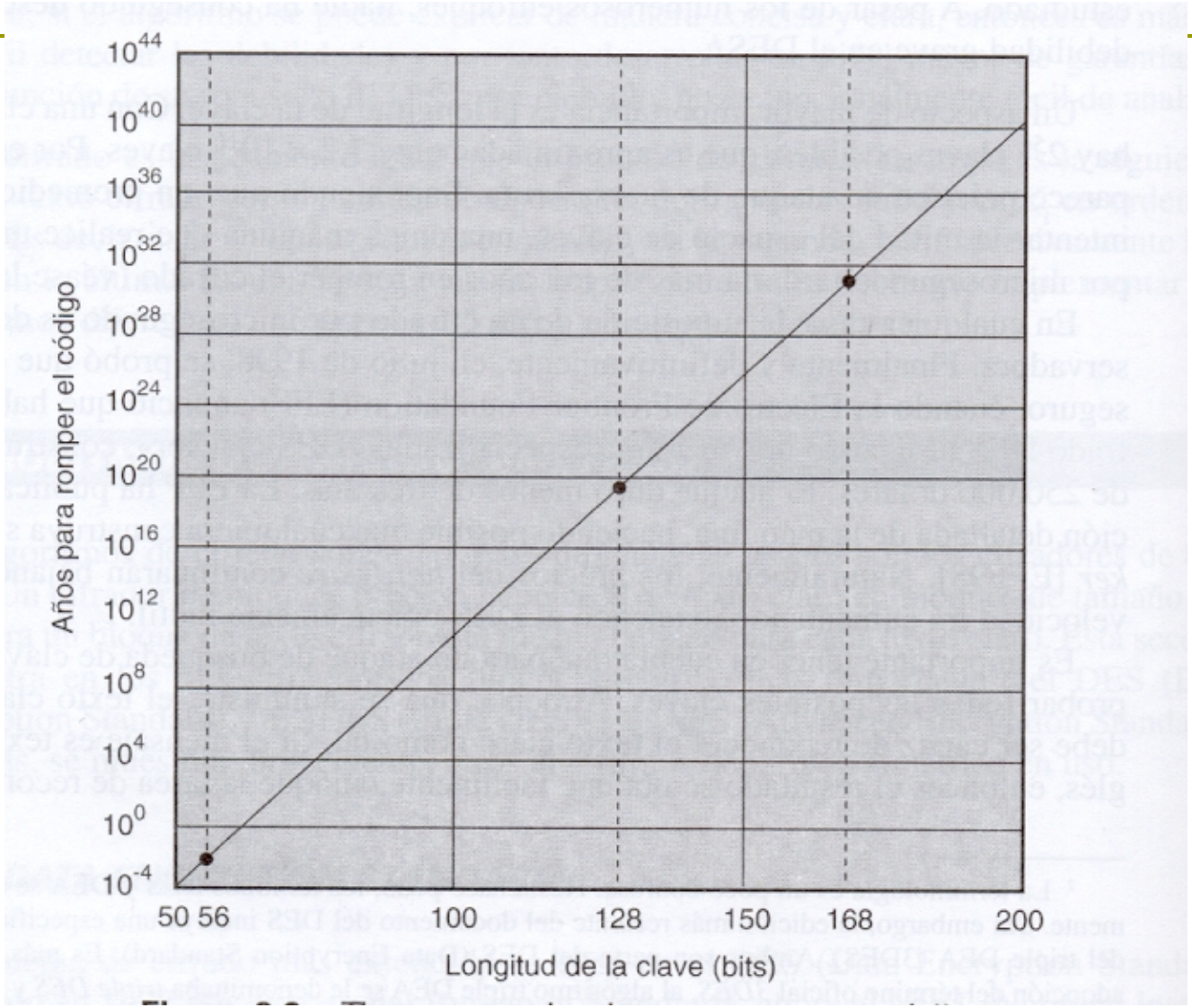
Robustez del DES

- Se engloba en dos aspectos:
  - Aspectos sobre el algoritmo mismo (nadie ha conseguido descubrir ninguna debilidad grave en el DES)
  - Aspectos sobre el uso de una clave de 56 bits (con dicha clave, existen 2^{56} claves posibles, no parece práctico un ataque por fuerza bruta, ya que en promedio se intenta la mitad del espacio de claves, una única máquina que realice un cifrado por microseg. Tardaría más de mil años en romper el cifrado)

DES -- no seguro

- En 1998 la Electronic Frontier Foundation (EFF) anunció que había roto un cifrado DES utilizando una máquina especializada <<DES cracker>>. La EFF ha publicado la descripción detallada de la máquina, haciendo posible que cualquiera construya su propio cracker.
- Si la única forma de ataque a un algoritmo de cifrado es la fuerza bruta, entonces se necesitan usar claves más largas.

Cracker de la EFF suponiendo 1 millón de descifrados por µs



Triple DES

- El 3DES usa tres claves y tres ejecuciones del algoritmo DES. La función sigue la secuencia cifrar-descifrar-cifrar.

$$C = E_{K3} [D_{K2} [E_{K1}[P]]]$$

Donde:

C = texto cifrado

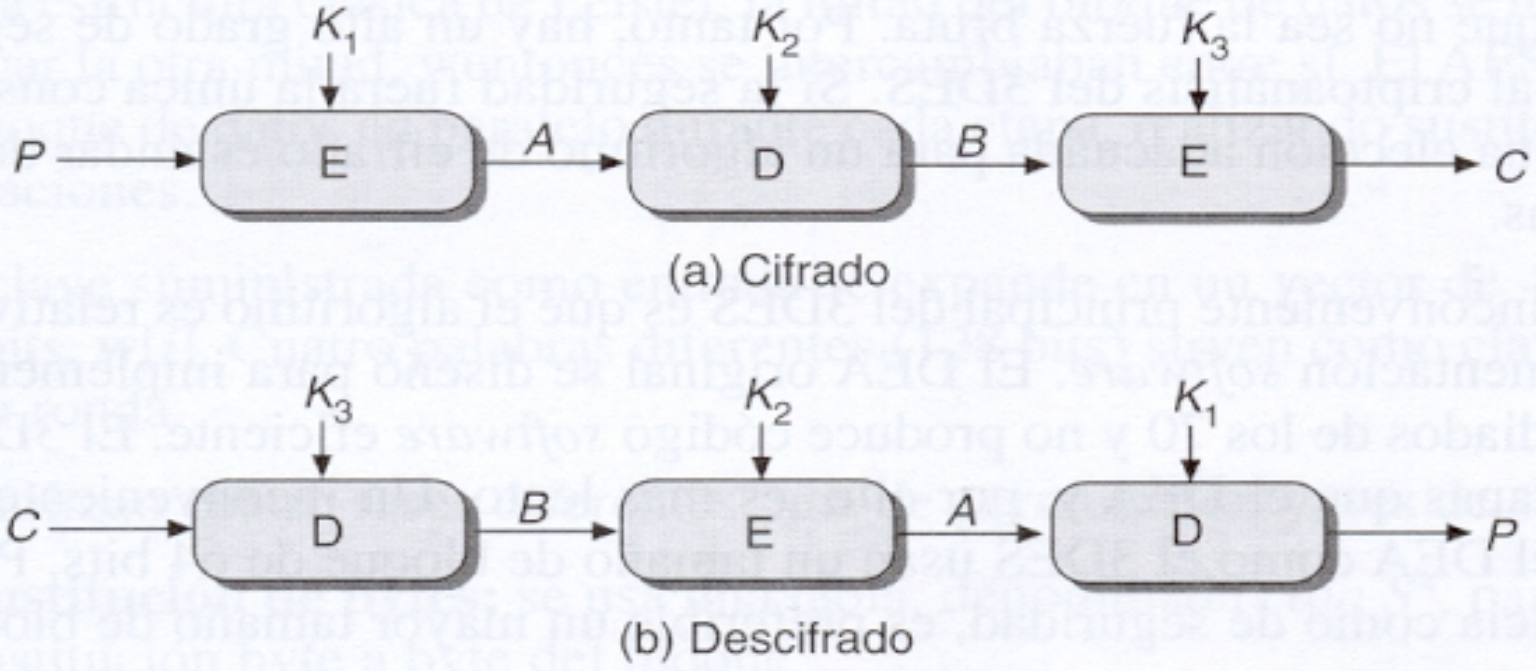
P = texto claro

$E_K[X]$ = cifrado de X usando la clave K

$D_K[Y]$ = descifrado de Y usando la clave K

Descifrado.- misma operación con las claves en orden inverso

$$P = D_{K1}[\,E_{K2}[\,D_{K3}[C]]]$$



Robustez del 3DES

- Con tres claves diferentes, el 3DES tiene una longitud efectiva de clave de 168 bits. También se permite el uso de dos claves, con $K_1 = K_3$, lo que proporciona una longitud de clave de 112 bits.
- Con una clave de 168 bits de longitud, los ataques de fuerza bruta son efectivamente imposibles
- Único inconveniente es que tiene 3 veces más etapas que el DES y por ello 3 veces más lento.

Algoritmos de cifrado convencional

Algoritmo	Tamaño de clave (bits)	Tamaño de bloque (bits)	Número de etapas	Aplicaciones
DES	56	64	16	SET, Kerberos
Triple DES	112 o 168	64	48	Financial Key management, PGP, S/MIME
AES	128, 192 o 256	128	10, 12 o 14	Destinados a sustituir DES y 3DES
IDEA	128	64	8	PGP
Blowfish	Variable hasta 448	64	16	Varios paquetes de software
RC5	Variable hasta 2048	64	Variable hasta 255	Varios paquetes de software

Problemas con los sistemas de clave simétrica

- El problema principal de seguridad consiste en mantener la privacidad de la clave
- Así como la distribución de la misma.

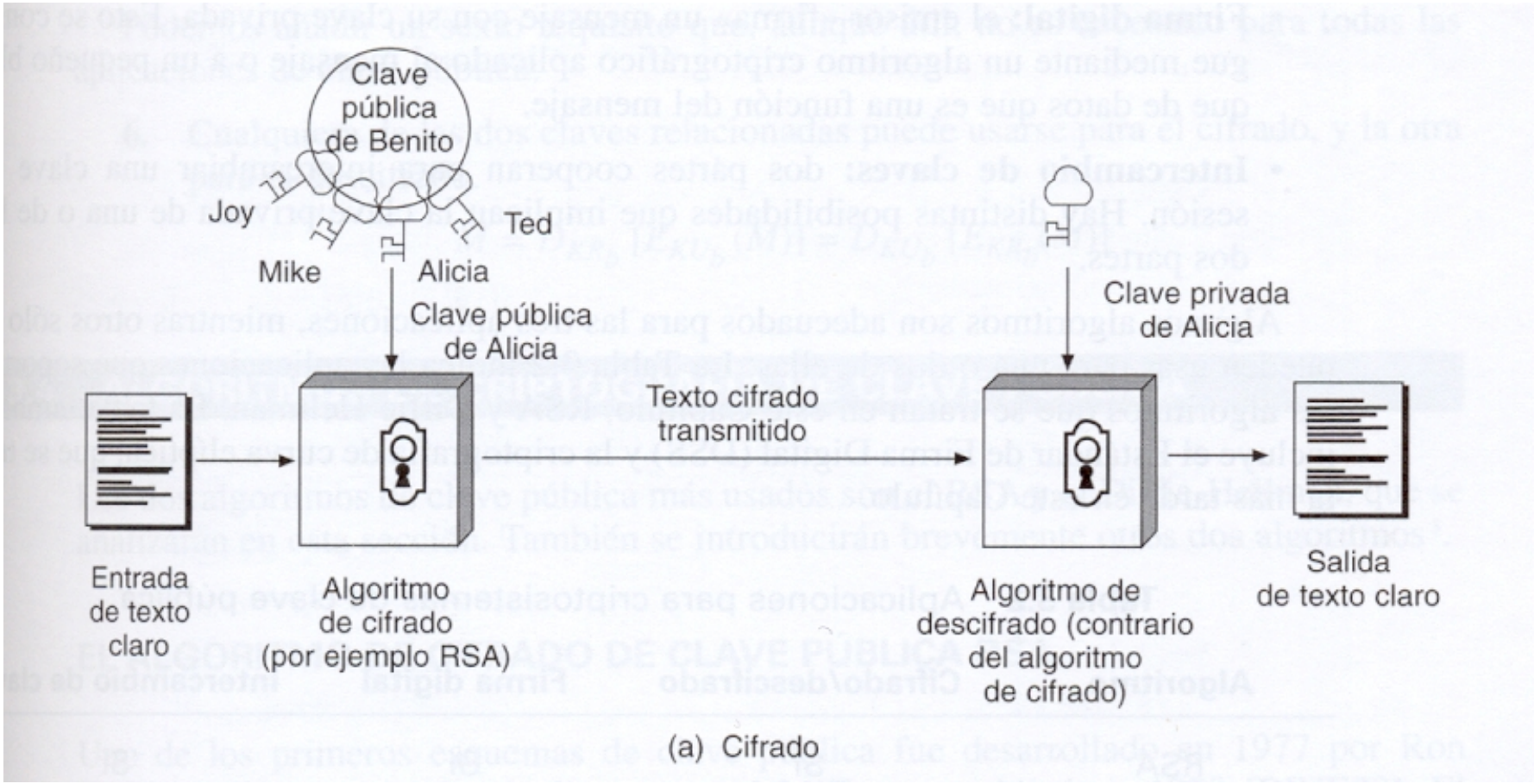
Criptografía de llave pública

- Los algoritmos de clave pública están basados en funciones matemáticas y no en simples operaciones sobre los patrones de bits.
- Esta criptografía es asimétrica, lo que implica el uso de dos claves separadas (una clave pública y otra privada) y no solo de una como en la criptografía simétrica

Claves

- Como los nombres lo sugieren, la clave pública de dicha pareja de claves se hace pública para que los otros la usen, mientras que la clave privada sólo es conocida por su propietario. Un algoritmo criptográfico de clave pública con propósito general se basa en una clave para el cifrado y otra diferente, aunque relacionada para el descifrado

Criptografía de llave pública



Confusiones comunes

- El cifrado de clave pública es más seguro ante el criptoanálisis que el cifrado convencional (falso)
  - La seguridad de cualquier esquema de cifrado depende de la longitud de la llave. No hay nada sobre el cifrado simétrico ni de clave pública que haga a uno superior al otro en lo que respecta a la resistencia al criptoanálisis.

- La idea que el cifrado de clave pública ha dejado desfasado el cifrado convencional (falso)
  - Por el contrario, debido al coste computacional de los esquemas actuales de cifrado de clave pública, no parece que el cifrado simétrico vaya a abandonarse.
- Se piensa que es más sencillo la distribución de llaves
  - Se necesita de alguna autoridad certificadora para validar las claves públicas

Los pasos fundamentales son los siguientes:

- Cada usuario genera un par de llaves
- Localiza una de las dos claves en un registro público u otro archivo accesible. Esta es la clave pública.
- Si Benito quiere enviar un mensaje privado a Alicia, cifra el mensaje usando la clave pública de Alicia.
- Cuando Alicia recibe el mensaje, lo descifra usando su clave privada. Ningún otro receptor puede descifrar el mensaje porque sólo Alicia conoce su clave privada.

Requisitos para la criptografía de clave pública

- Desde el punto de vista computacional, para una parte B es fácil generar una pareja de claves (pública KU_b, privada KR_b)
- En términos computacionales, para un emisor A que conozca la clave pública y el mensaje que ha de cifrarse, M, es fácil generar el texto cifrado:

$$C = E_{KUb}(M)$$

- Desde el punto de vista computacional, es imposible que un oponente, conociendo la clave pública KU_b, determine la clave privada KR_b.
- Desde el punto de vista computacional, es imposible que un oponente, conociendo la clave pública, KU_b, y un texto cifrado, C, recupere el mensaje original, M.
- Cualquiera de las claves relacionadas puede usarse para el cifrado, y la otra para el descifrado

$$M = D_{KRb}\,[E_{KUb}(M)] = D_{KUb}\,[E_{KRb}(M)]$$

Generación de claves

Generación clave

Seleccionar p, q	p y q primos, $p \neq q$
Calcular $n = p \times q$	
Calcular $\phi(n) = (p - 1)(q - 1)$	
Seleccionar entero e	$gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calcular d	$de \bmod \phi(n) = 1$
Clave pública	$KU = \{e, n\}$
Clave privada	$KR = \{d, n\}$

d Inverso multiplicativo de e

Ejemplo del RSA

1.- Seleccionar dos números primos, p = 17 y q = 11.

2.- Calcular n = pq = 17 x 11 = 187

3.- Calcular $\Phi(n)=(p-1)(q-1)=16x10 = 160$

4.- Seleccionar e tal que sea primo relativo de $\Phi(n)=160$ y menor a $\Phi(n)$; e = 7.

5.- Determinar d tal que ***de*** mod 160 = 1 y $d<160$. El valor es d=23, porque 23x7 = 161 = 10x160+1

   * Por lo que KU = {7,187} y KR={23,187}

Algoritmo de clave pública RSA

Tanto el emisor como el receptor deben conocer los valores de n y e, y sólo el receptor conoce el valor de d. Por tanto:

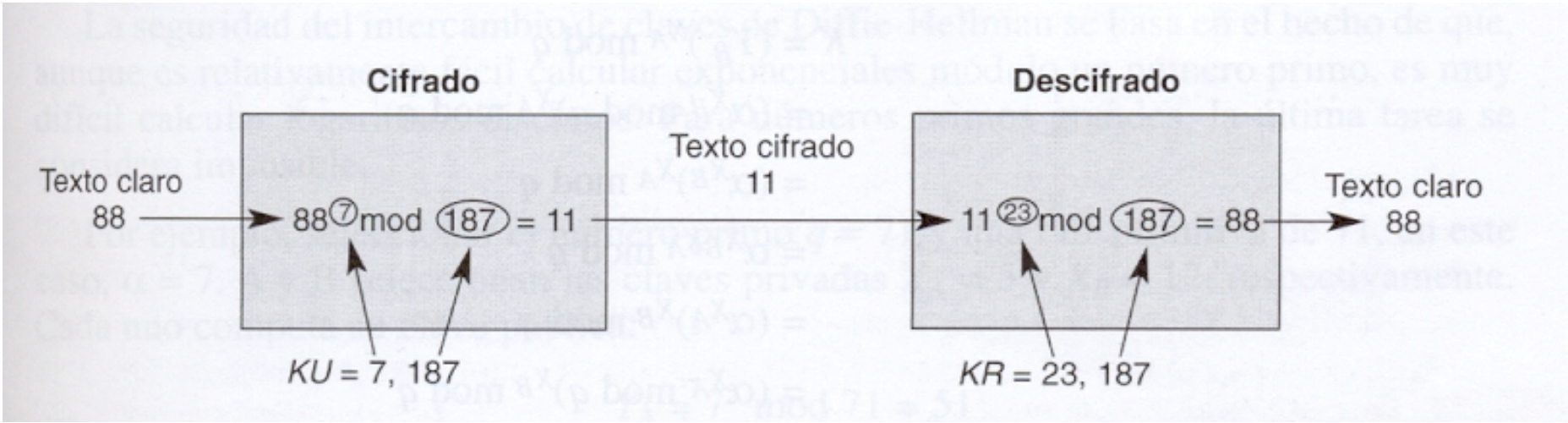
KU = {e, n} y KR = {d, n}

- Para un bloque de texto claro M y un bloque de texto cifrado C, el cifrado y descifrado son de la siguiente forma:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Ejemplo



KU = {e, n}

KR = {d, n}

Por las propiedades de la aritmética modular se tiene que:

$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$

$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$

$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 11$

Y para calcular $M = 11^{23} \bmod 187$

$11^{23} \bmod 187 = [(11^{1} \bmod 187) \times (11^{2} \bmod 187) \times (11^{4} \bmod 187) \times (11^{8} \bmod 187) \times (11^{8} \bmod 187)] \bmod 187$

$11^{1} \bmod 187 = 11$

$11^{2} \bmod 187 = 121$

$11^{4} \bmod 187 = 14{,}641 \bmod 187 = 55$

$11^{8} \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$

$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$

Robustez del RSA

- Cuanto mayor sean los números e y d, más seguro será el algoritmo. Sin embargo debido a los cálculos que tienen lugar tanto en la generación de claves como en el cifrado/descifrado son complejos, cuanto mayor sea el tamaño de la clave, más lento irá el sistema.
- Es complejo factorizar n en sus dos factores primos
- Debe usarse un tamaño de clave pública mayor a 428 bits, actualmente se utiliza una clave de 1024 bits

Intercambio de clave Diffie - Hellman

- La finalidad del algoritmo es que los usuarios intercambien de forma segura una clave secreta que pueda ser usada para el cifrado posterior de mensajes.
- Dicho algoritmo depende para su efectividad de la dificultad de computar logaritmos discretos.

- Podemos definir el logaritmo discreto de la siguiente forma: primero, definimos una raíz primitiva de un número primo ***q*** cuyas potencias generan todos los enteros desde 1 a ***q–1***:

$$a \bmod q,\ a^2 \bmod q \ldots,\ a^{q-1} \bmod q$$

Son distintos y consisten en los enteros desde 1 hasta ***q–1.***

Para cualquier entero ***b*** menor que ***q*** y una raíz primitiva ***a*** del número primo se puede encontrar un único exponente ***i*** tal que:

$$b = a^i \bmod q \quad \text{donde } 0 \leq i \leq (q-1)$$

Al exponente ***i*** se le conoce como el logaritmo discreto

Algoritmo

- Existen dos números conocidos públicamente: un número primo q y un entero α que es la raíz primitiva de q.
- A y B quieren intercambiar una clave.
- El usuario A selecciona un entero $X_A < q$ y computa $Y_A = \alpha^{XA} \bmod q$. Igual, el usuario B selecciona un entero $X_B < q$ y calcula $Y_B = \alpha^{XB} \bmod q$. Cada parte mantiene privado el valor de X y público el valor de Y.

Algoritmo

Elementos públicos globales

q	número primo
α	$\alpha < q$ y α una raíz prima de q

Generación de la clave del usuario *A*

Seleccionar X_A privada	$X_A < q$
Calcular Y_A pública	$Y_A = \alpha^{X_A} \bmod q$

Generación de la clave del usuario *B*

Seleccionar X_B privada	$X_B < q$
Calcular Y_B pública	$Y_B = \alpha^{X_B} \bmod q$

Generación de la clave secreta por el usuario *A*

$K = (Y_B)^{X_A} \bmod q$

Generación de la clave secreta por el usuario *B*

$K = (Y_A)^{X_B} \bmod q$

- El usuario A computa la clave como $K = (Y_B)^{XA} \bmod q$ y el usuario B computa la clave como $K = (Y_A)^{XB} \bmod q$

$$
\begin{aligned}
K &= (Y_B)^{XA} \bmod q \\
&= (\alpha^{XB} \bmod q)^{XA} \bmod q \\
&= (\alpha^{XB})^{XA} \bmod q \\
&= \alpha^{XBXA} \bmod q \\
&= (\alpha^{XA})^{XB} \bmod q \\
&= (\alpha^{XA} \bmod q)^{XB} \bmod q \\
&= (Y_A)^{XB} \bmod q
\end{aligned}
$$

Ejemplo

- Se selecciona el número primo q = 71 y una raíz primitiva de 71, es α = 7. A y B seleccionan las claves privadas $X_A = 5$ y $X_B = 12$, respectivamente. Cada uno computa su clave pública:

$$Y_A = 7^5 \bmod 71 = 51$$

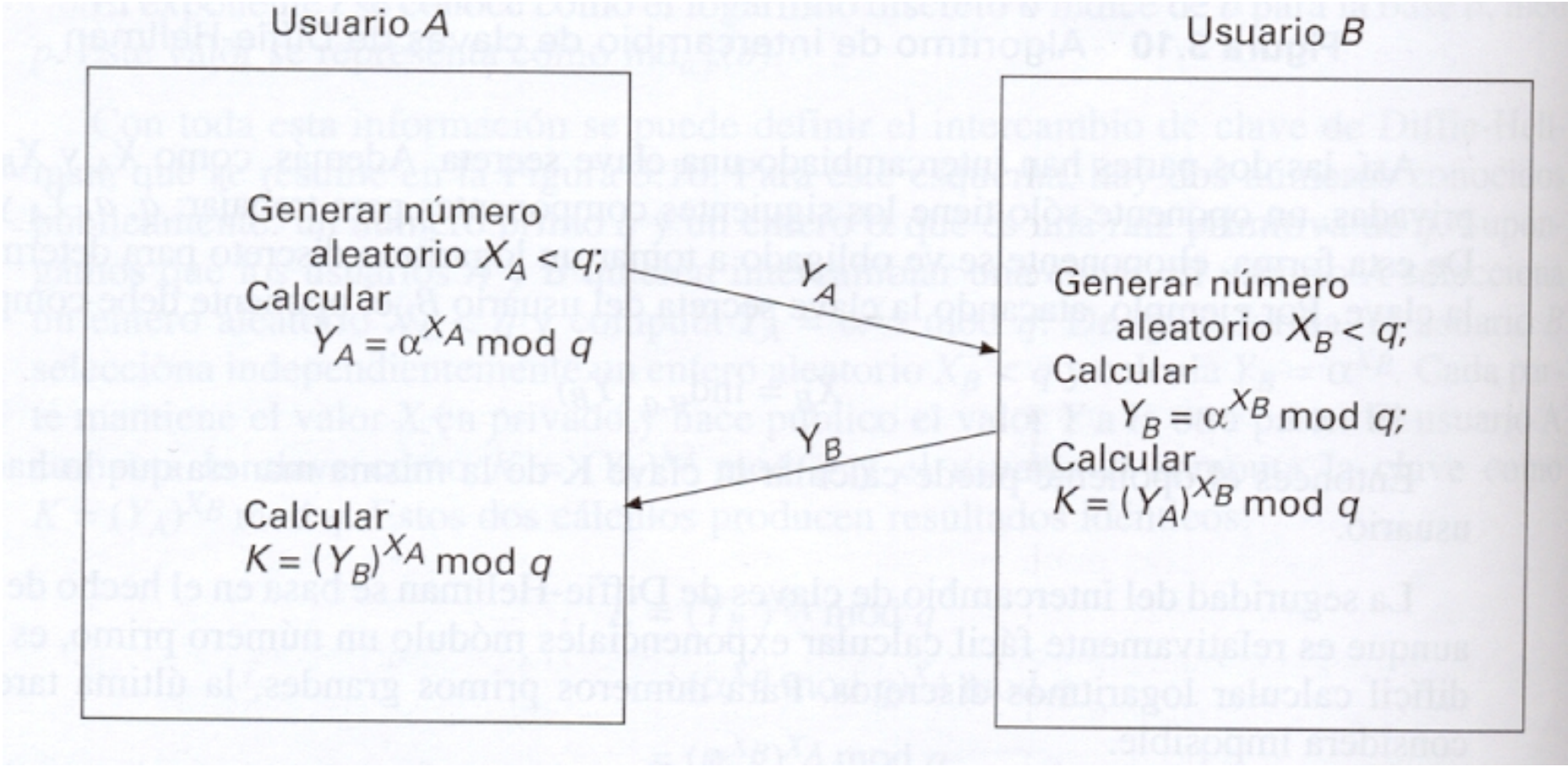
$$Y_B = 7^{12} \bmod 71 = 4$$

Después de intercambiar sus claves públicas, cada uno calcula la clave secreta

$$K = (Y_B)^{XA} \bmod 71 = 4^5 \bmod 71 = 30$$

$$K = (Y_A)^{XB} \bmod 71 = 51^{12} \bmod 71 = 30$$

Protocolo que hace uso del algoritmo



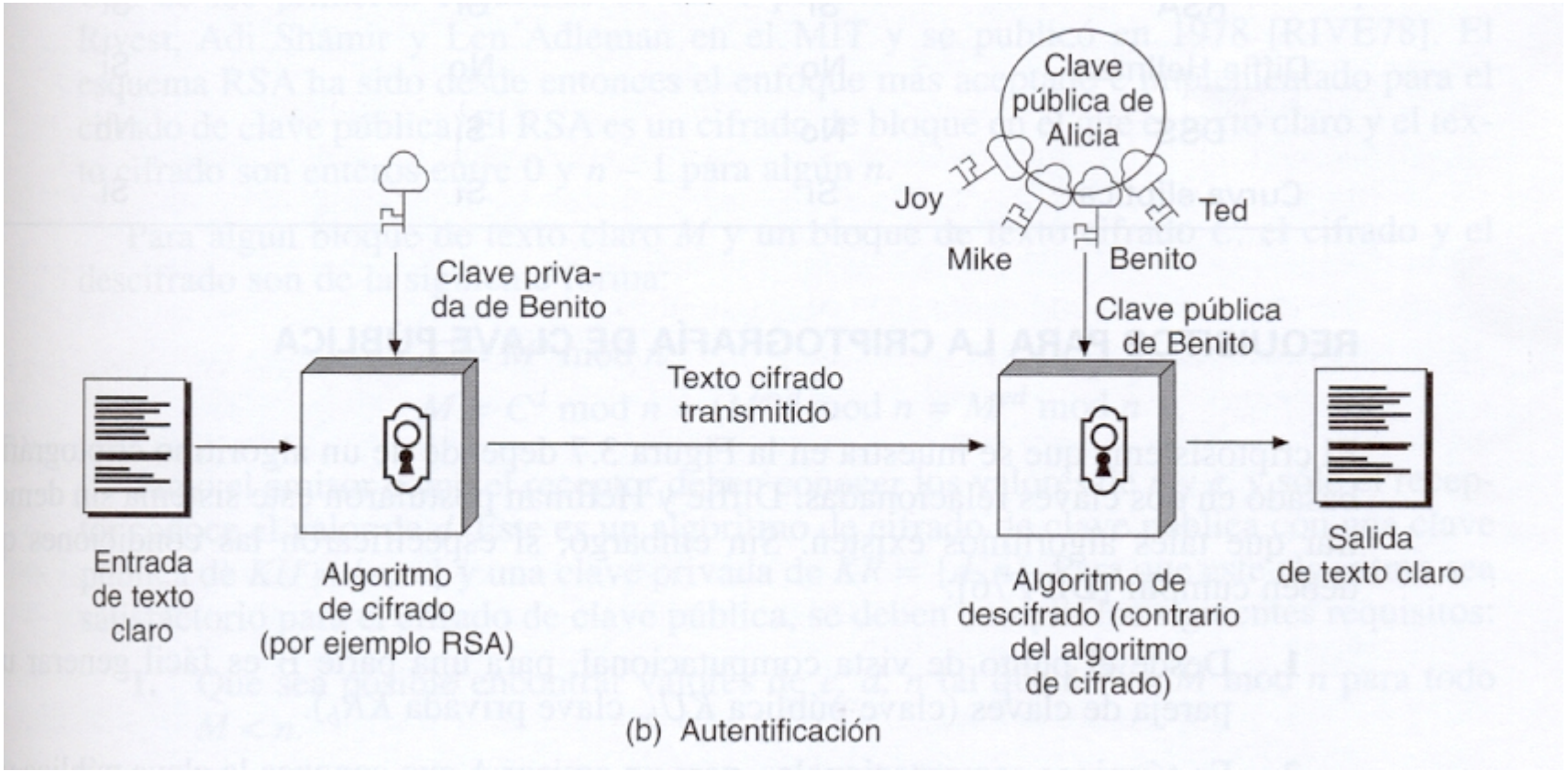
Aplicaciones para criptosistemas de clave pública

Algoritmo	Cifrado/descifrado	Firma digital	Intercambio de clave
RSA	Sí	Sí	Sí
Diffie-Hellman	No	No	Sí
DSS	No	Sí	No
Curva elíptica	Sí	Sí	Sí

Firmas Digitales

- Su finalidad no es que el mensaje se mantenga en secreto (confidencialidad), sino que el receptor se asegure que el mensaje provino de algún emisor (autenticación).
- El emisor usa su clave privada para cifrar el mensaje, cuando el receptor recibe el texto cifrado, se encuentra con que puede descifrarlo con la clave pública del emisor, demostrando así que el mensaje ha debido ser cifrado por él.

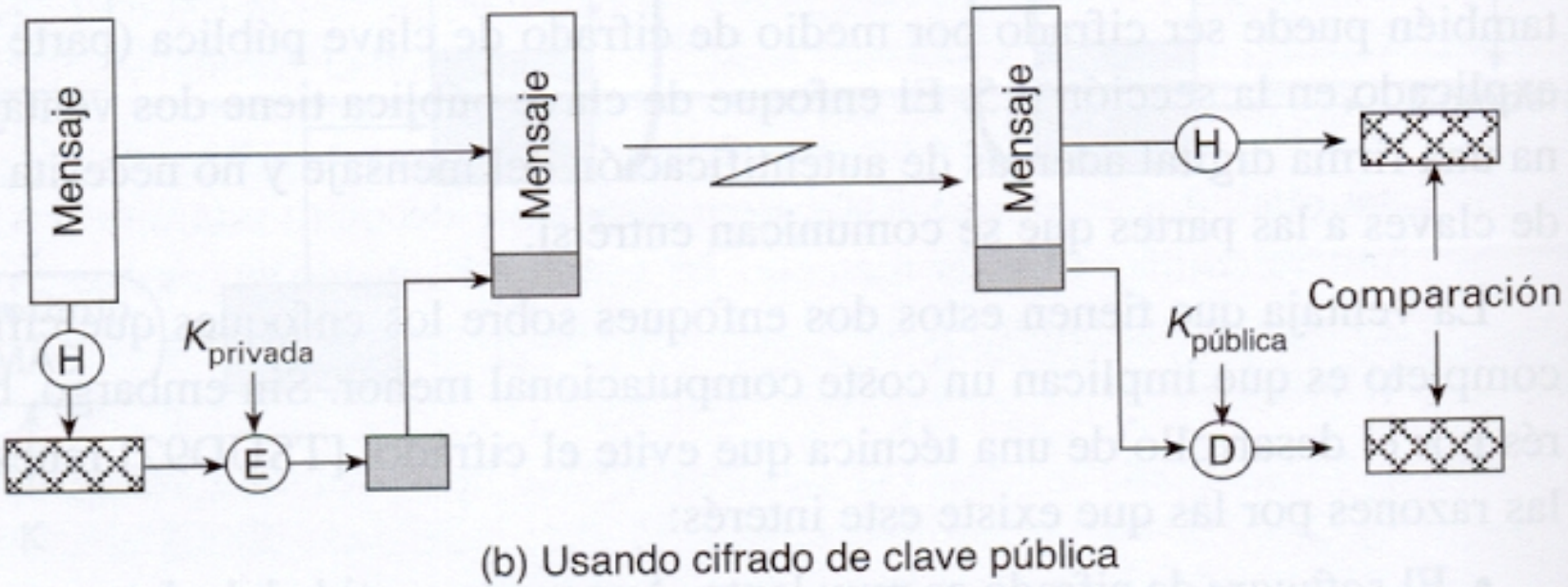
- Además, es imposible alterar el mensaje sin acceso a la clave privada del emisor, teniendo aquí integridad en los datos.



Inconvenientes

- Alto coste computacional cifrar todo el mensaje si en realidad cualquiera lo puede leer (clave pública).
- Una forma más efectiva es obtener una función del documento, función hash (obtener una huella del documento) y después la salida de dicha función cifrarla con la clave privada del emisor.

Función hash



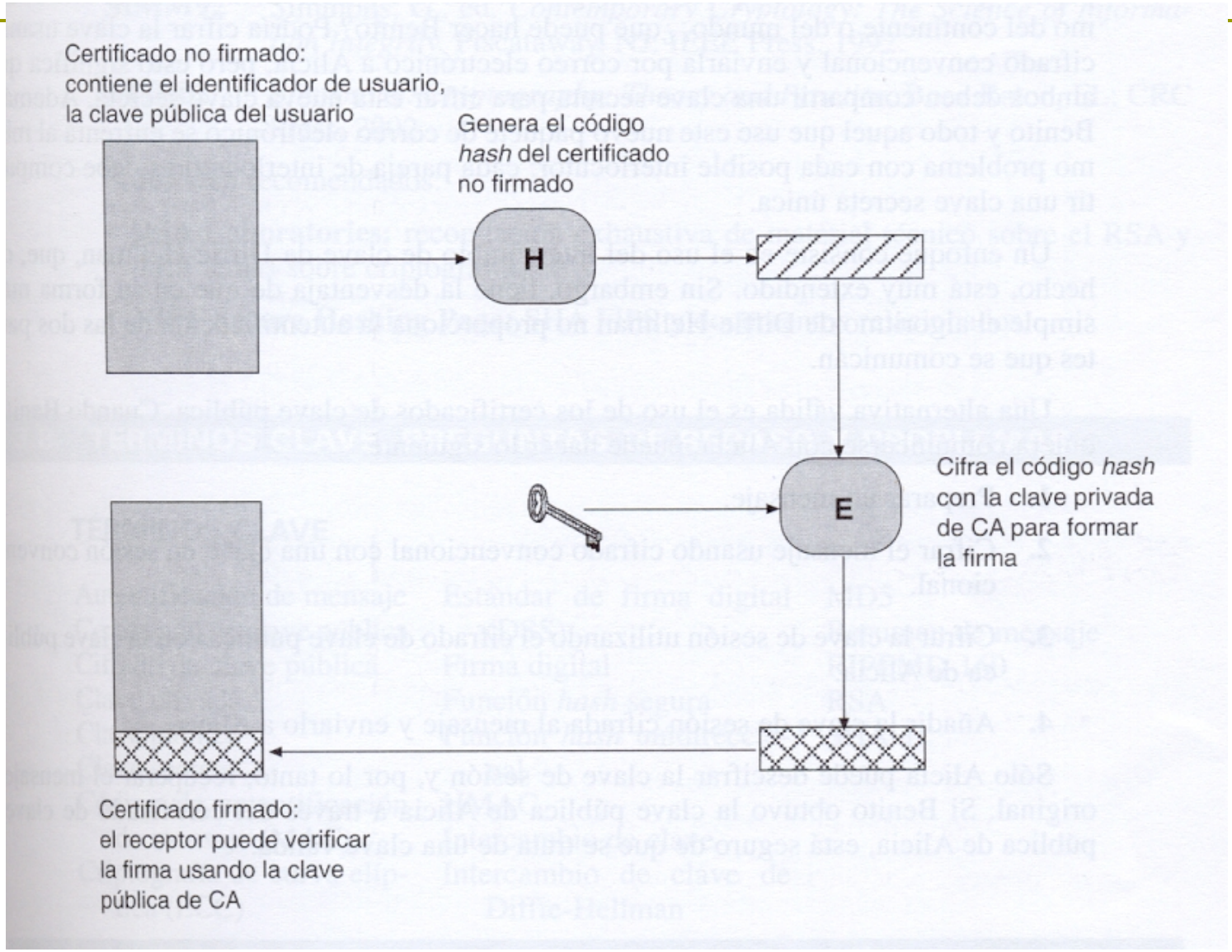
(b) Usando cifrado de clave pública

Certificados digitales

- Ya que la base del cifrado de clave pública se encuentra en el hecho de que la clave pública es pública. Este enfoque tiene el inconveniente que cualquiera puede falsificar ese dato.
- Un usuario se podría hacer pasar por el usuario A y enviar una clave pública a otro participante o difundirla. Hasta el momento en que A descubre la falsificación y alerta a los demás, el falsificador puede leer todos los mensajes cifrados enviados a A así como firmar documentos.

- La solución a dicho problema es la certificación de clave pública
- Un certificado consiste en una clave pública y un identificador o nombre de usuario del dueño de la clave, con todo el bloque firmado por una tercera parte confiable (autoridad certificadora) en la que confía la comunidad de usuarios.
- Un usuario presenta su clave pública a la autoridad, obtiene un certificado y luego lo publica. Cualquier usuario puede obtener el certificado y verificar que es válida por medio de la firma fiable adjunta.

Uso de la autoridad certificadora

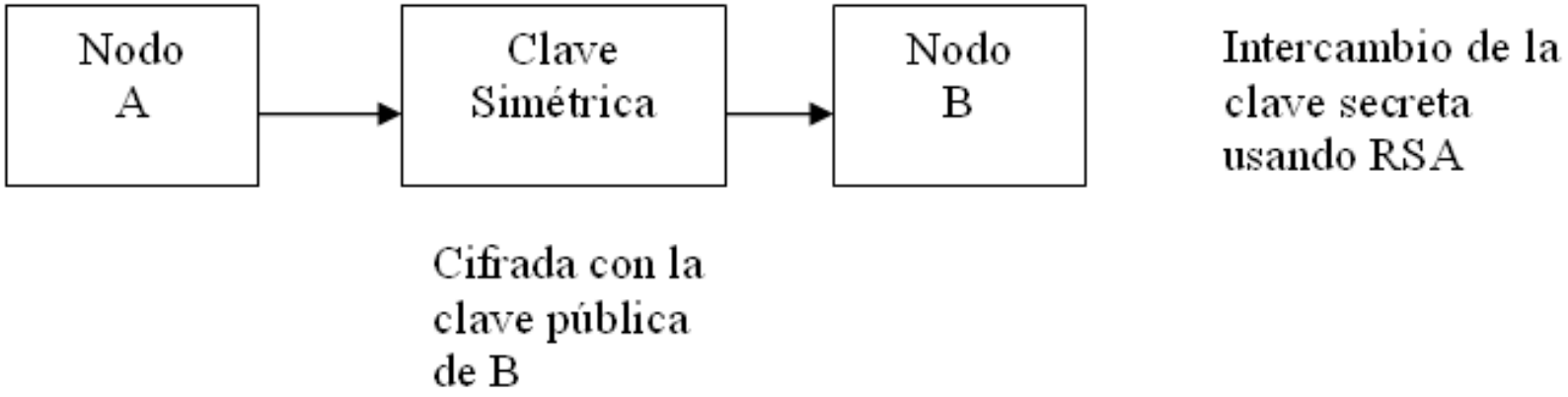


Sobres digitales

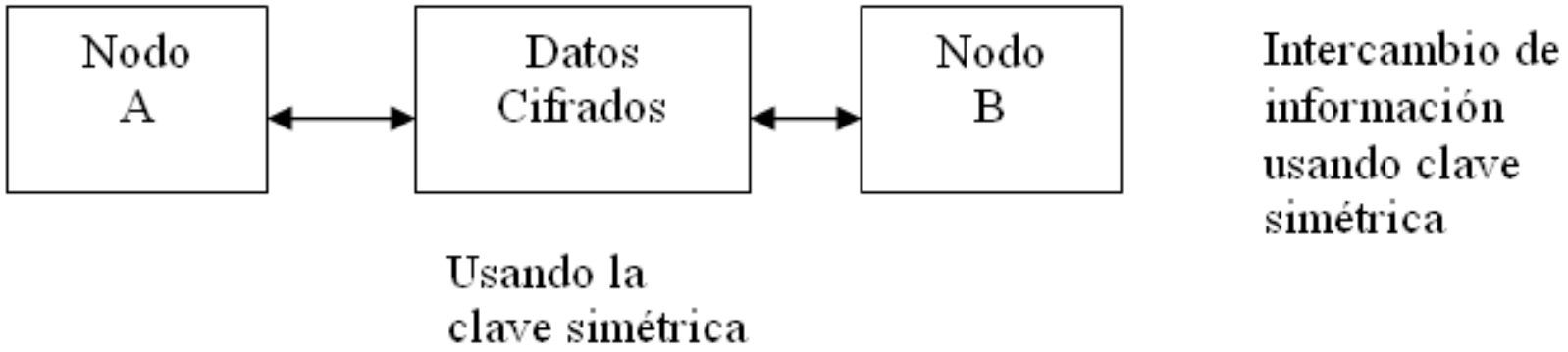
Aplicaciones para criptosistemas de clave pública

- Cifrado/descifrado: el emisor cifra un mensaje con la clave pública del receptor.
- Firma digital: el emisor firma un mensaje con su clave privada.
- Intercambio de claves: dos partes cooperan para intercambiar una clave de sesión

- El nodo tx A elige una clave simétrica, la cual es cifrada usando la clave pública del nodo receptor B. Posteriormente esta clave simétrica cifrada es transmitida por A hacia B



- El nodo B descifra la clave simétrica y se inicia el intercambio de información cifrada con la clave simétrica



Las mejores implementaciones del RSA son miles de veces más lentas que las que se logran con el DES