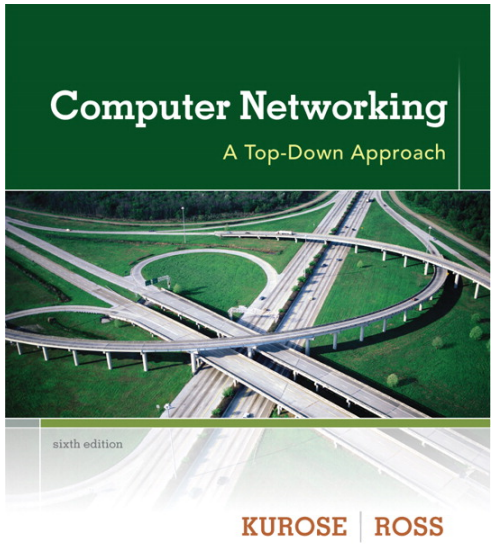


Capítulo 8
Seguridad en redes

Estas clases son de Kurose y Ross

Gracias a Kurose y Ross que pusieron este material libre

La traducción y adaptación es de Alejandra Stolk para la materia Redes de Computadoras

Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

All material copyright 1996-2012
© J.F Kurose and K.W. Ross, All Rights Reserved

¿Qué es la seguridad en la red?

Confidencialidad: sólo el emisor y el receptor deseado pueden entender los contenidos de los mensajes

- Emisor cifra el mensaje
- Receptor descifra el mensaje

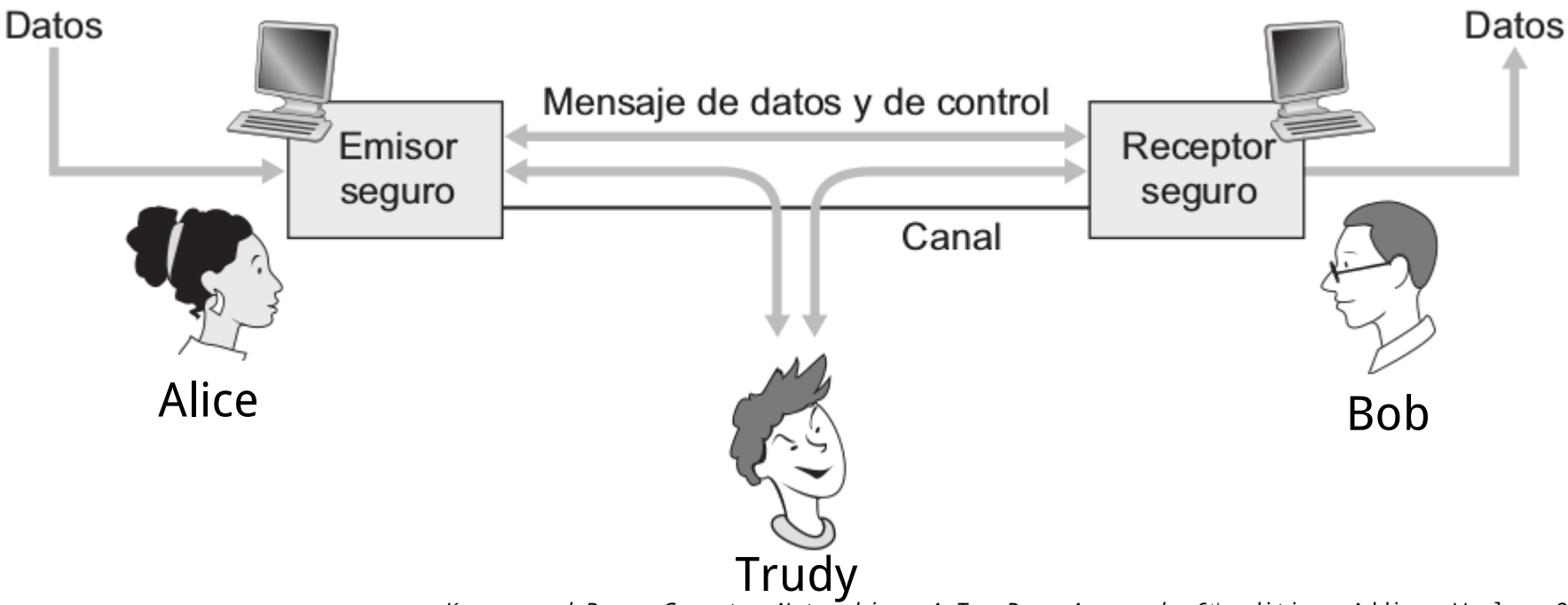
Autenticación: el emisor y el receptor quieren confirmar la identidad del otro

Integridad de los mensajes: el emisor y el receptor quieren asegurar que el mensaje no es alterado (en tránsito ni después) sin detección

Acceso y disponibilidad: services servicios tienen que ser accesibles y disponibles a los usuarios

Amigos y enemigos: Alice, Bob, Trudy

- Muy conocidos en el mundo de la seguridad
- Bob, Alice (amigos!) quieren comunicarse en forma “segura”
- Trudy (intrusa) puede interceptar, borrar, e insertar mensajes



¿Quienes pueden ser Bob y Alice?

- ...bueno...Gente real como Bob y Alice!
- Browser/servidor web usados para transacciones electrónicas (e.g. compras en línea)
- Aplicaciones cliente/servidor cómo un banco en línea (e.g. Redbank)
- Servidores DNS
- Enrutadores intercambiando actualizaciones de tablas
- Otros ejemplos?

Hay gente mala en el mundo!

P: Que puede hacer una persona mala?
R: Mucho!

escuchar: interceptar mensajes activamente insertar mensajes en una conexión

impersonar: puede cambiar (spoof) dirección de origen de un paquete (o cualquier campo en un paquete)

secuestrar: "apoderarse" de conexion activa al remover transmisor o receptor, insertandose a cambio

negación de servicio: prevenir que el servicio sea usado por otros (e.g., al sobrecargar recursos, mandando información errónea que haga que un servidor muera)

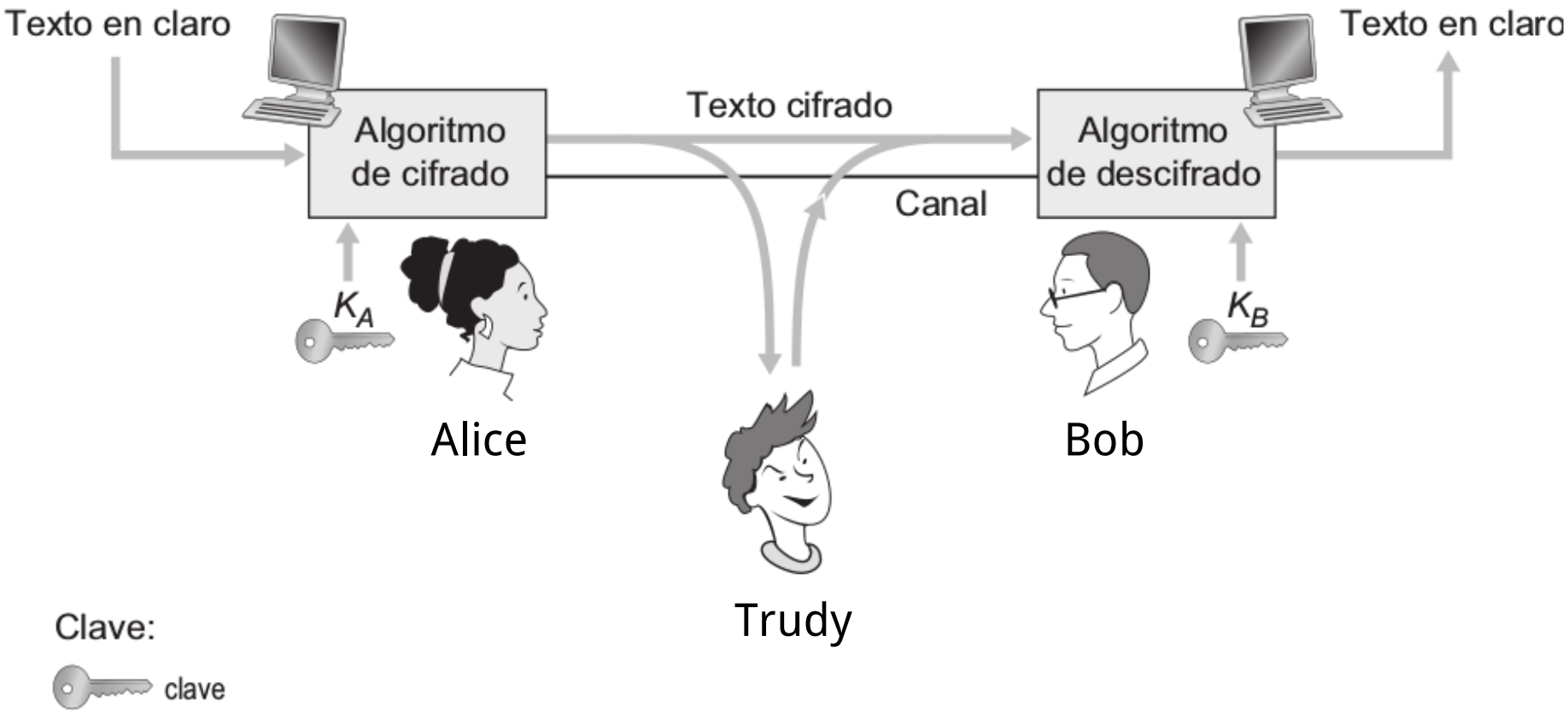
¿Qué es criptografía?

- Del griego:
  - Kryptos: ocultar
  - Graphos: escrito
- Escritura oculta
- Estudio y diseño de sistemas de comunicaciones secretas.

¿Qué es el criptoanálisis?

- Del griego:
  - Kryptos: ocultar
  - Analýein: desatar
- Estudio y diseño de sistemas para descubrir la información ocultada en sistemas criptográficos

El lenguaje de la criptografía



criptografía de claves simétricas: emisor, receptor tienen llaves idénticas
criptografía de claves publicas (public-keys): llave para cifrar es pública, llave para descifrar es secreta (privada)

Rompiendo el esquema de cifrado

- Ataque de sólo texto cifrado: En algunos casos, el intruso puede tener acceso únicamente al texto cifrado interceptado, sin disponer de información segura acerca del contenido del mensaje en claro. En cómo el análisis estadístico puede ayudarnos a realizar un ataque de sólo texto cifrado al esquema de cifrado.
- 2 enfoques:
  - ataque de fuerza bruta: realiza todas las combinaciones posibles hasta romper la llave
  - análisis estadístico

Rompiendo el esquema de cifrado

- Ataque de texto en claro conocido: Anteriormente hemos visto que si Trudy estuviera seguro, de alguna manera, de que las palabras “Bob” y “Alice” aparecen en el mensaje de texto cifrado, entonces podría haber determinado las parejas (texto en claro, texto cifrado) para las letras a, l, i, c, e, b y o.

Rompiendo el esquema de cifrado

- Ataque de texto en claro conocido: Trudy también podría haber sido lo suficientemente afortunado como para haber grabado todas las transmisiones de texto cifrado y luego encontrar en una hoja de papel la propia versión descifrada por Alicia de una de las transmisiones cifradas.

Rompiendo el esquema de cifrado

- Ataque de texto en claro conocido: Cuando un intruso conoce alguna de las parejas (texto en claro, texto cifrado), decimos que se trata de un *ataque de texto en claro* conocido al esquema de cifrado.

Cifrado polialfabético

Usando n cifrados mono-alfabéticos: $M_1, M_2, \ldots, M_n$

Más patrón cíclico:

e.g., n=4, M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2;

Para cada símbolo en texto plano nuevo, usar el patrón mono-alfabético subsecuente en el ciclo.

utfsm: u desde M_1, t de M_3, f de M_4, s de M_3, ..

Clave: los n cifrados y el patrón cíclico.

Tipos de criptografía moderna

La criptografía normalmente usa un algoritmo conocido por todos y sólo las claves son secretas.

Criptografía de clavesimétrica usa una clave. También llamado cifrado simétrico

Criptografía de clave pública usa dos claves. También llamado cifrado asimétrico

Esquema de cifrado simétrico

Cifrado de sustitución: sustituyendo una cosa por la otra

- Cifrado monoalfabético: sustituye una letra otra

Texto plano: abcdefghijklmnopqrstuvwxyz

Texto crifrado: mnbvcxzasdfghjklpoiuytrewq

ejemplo: **Texto plano: bob. Te amo. alice**

Texto cifrado: nkn. s gktc wky. mgsbc

Clave de cifrado: mapeando de un conjunto de 26 letras a un conjunto de 26 letras

Tipos de cifrado simétrico

Cifrado de bloques

Se divide el mensaje legible en bloques de igual tamaño.

Cifra cada bloque como una unidad.

Cifrado de flujo de símbolos básicos

Cifrado de un bit a la vez.

Cifradores de bloque

El mensaje es procesado en bloques de k bits (e.g., bloques de 64 bit).

Se usa mapeo 1-a-1 para mapear k bit del texto a k bits cifrados.

Ejemplo con k=3:

input	output
000	110
001	111
010	101
011	100

input	output
100	011
101	010
110	000
111	001

¿Cuál es el texto cifrado para 010110001111 ?

Cifrado de bloque

¿Cuántos mapeos existen para K=3?

- ¿Cuántos bloques de 3 bits?
- ¿Cuántos mapeos podemos hacer? (son las permutaciones posibles)
- Respuesta: 40.320 ; No muchas

En general, $2^k!$ mapeos; muchos para k=64

Problema:

- Si lo hacemos por tablas, se requiere tablas de 2^{64} entradas, cada entrada con 64 bits

Tabla muy grande, en su lugar conviene usar una función que simule una tabla de permutación aleatoria.

Cifrado simétrico: DES

DES: Data Encryption Standard

- Standard de cifrado en USA [NIST 1993]
- Llave simétrica de 56-bit, plaintext de 64-bits
- ¿Cuan seguro es DES?
- El desafío de DES: una frase cifrada con llave de 56-bit fue descifrado usando (fuerza bruta) en 4 meses
- No hay método “de atajo” (“backdoor”) conocido de descifrado
- Haciendo DES más seguro:
  - usar tres llaves secuencialmente (3-DES) sobre cada dato
  - encadenamiento de cifradores

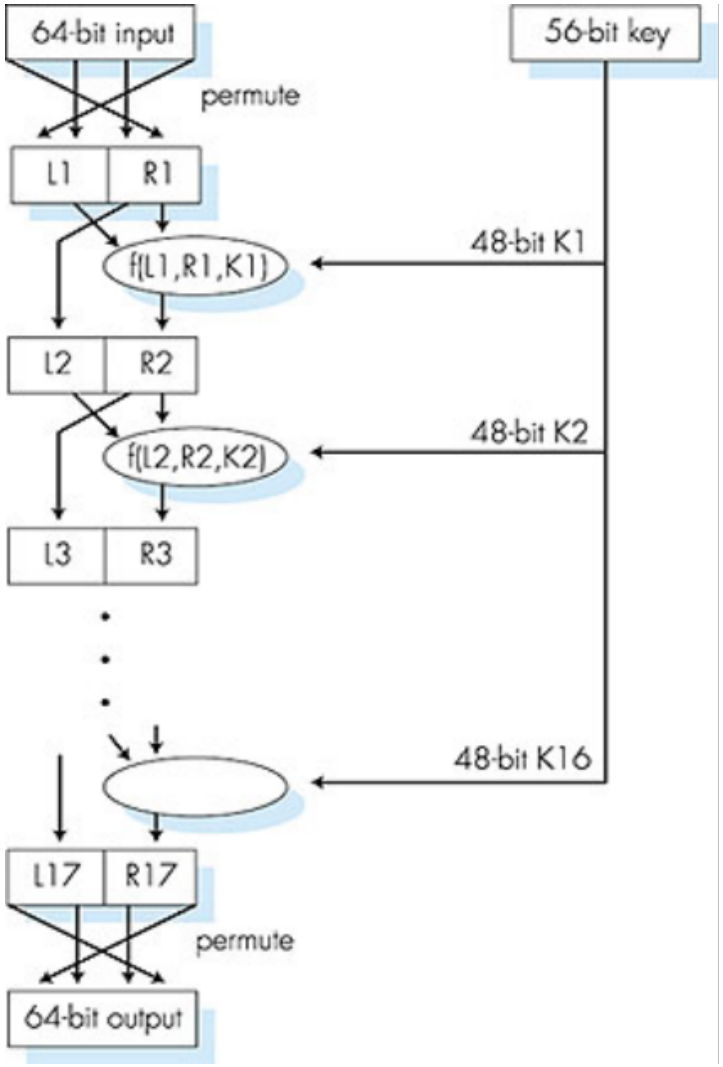
Criptografía de claves simétricas: DES

Operación de DES

Permutación inicial

16 ciclos idénticos pero usando una clave de 48 bits diferente

Permutación final



Criptografía de claves simétricas: AES

AES: Advanced Encryption Standard

- Es el estándar para cifrado de llaves simétricas utilizado por NIST

  (Nov. 2001), reemplaza DES
  - Procesa datos en bloques de 128 bits
  - Llaves de 128, 192, o 256 bits
  - Descrifado por fuerza bruta (tratando cada llave) que durara 1 segundo en DES, tomaría 149 trillones de años para AES

OJO una vulnerabilidad fue encontrada en el 2011 esto obligo a utilizar sólo llaves robustas

Criptografía de llaves públicas

Criptografía de llave simétrica

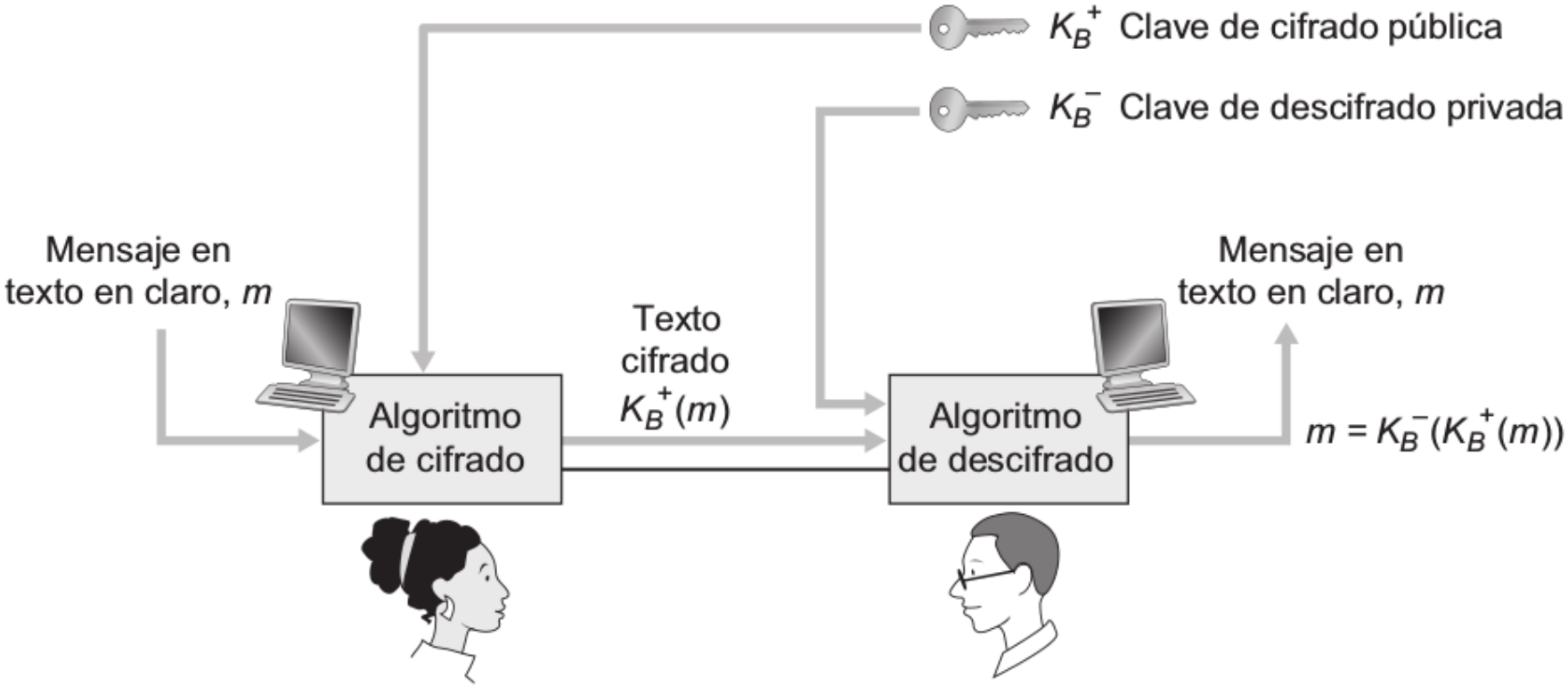
- Requiere que el emisor y el receptor compartan la llave secreta
- P: como estar de acuerdo en la llave (especialmente si

  nunca se han "encontrado")?

Criptografía de llave pública

- Estrategia radicalmente diferente
- Desarrollado por Diffie y Hellman, RSA78
- Emisor y receptor NO comparten la llave secreta
- la llave *pública* para cifrar es conocida por *todos*
- la llave *private* para descifrar es sólo conocida por el receptor

Criptografía de llaves públicas



Criptografía de llaves públicas

RSA: entiendo de qué trata

- mensaje: es un patrón de bits
- un patrón de bits que sólo puede ser representando por un número entero
- por lo tanto, cifrar un mensaje es equivalente a cifrar un número

ejemplo:

- m= 10010001 . Este mensaje sólo puede ser representado por el número 145.
- Para cifrar m, nosotros ciframos el número correspondiente, lo que da cómo resultado un nuevo número (el texto cifrado ó ciphertext).

Criptografía de llaves públicas

RSA

Requerimientos:

1. necesitamos $K_B^+(\cdot)$ y $K_B^-(\cdot)$ tales que

$$K_B^-(K_B^+(m)) = m$$

2. usando la llave publica K_B^+, debe ser imposible calcular llave privada K_B^-

Algoritmo Rivest, Shamir, Adelson (RSA)

Criptografía de llaves públicas

RSA: eligiendo las llaves

1. Elegir dos números primos grandes *p, q.* (e.g., de 1024 bits)
2. Calcular $n = pq$, $z = (p-1)(q-1)$
3. Elegir e ($e \ll n$) que no tengan factores en común con z. (e, z son "relativamente primos").
4. Elegir d de forma que $ed - 1$ sea exactamente divisible por z (de forma que: $ed \bmod z = 1$).
5. La llave publica es $\underbrace{(n,e)}_{K_B^+}$. La llave privada es $\underbrace{(n,d)}_{K_B^-}$.

Criptografía de llaves públicas

RSA: cifrado, descifrado

0. Dado (n,e) y (n,d) como calculados anteriormente

1. Para cifrar el patrón de bits, m, calcular
   $c = m^e \bmod n$ (i.e., resto cuando m^e es dividido por n)

2. Para descifrar patrón recibido, c, calcular
   $m = c^d \bmod n$ (i.e., resto cuando c^d es dividido por n)

Magia ocurre!

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

Criptografía de llaves públicas

RSA: ejemplo

Bob elige $p = 5$, $q = 7$. Entonces $n = 35$, $z = 24$.
$e = 5$ (e, z relativamente primos).
$d = 29$ ($ed-1$ exactamente divisible por z).

	letter	m	m^e	$c = m^e \bmod n$
encrypt:	L	12	248832	17

	c	c^d	$m = c^d \bmod n$	letter
decrypt:	17	48196857210675091509141182522307169 7	12	L

Criptografía de llaves públicas

RSA: otra propiedad...

La siguiente propiedad es util:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{usar llave publica seguida por privada}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{usar llave privada seguida por publica}}$$

Mismo resultado!

Criptografía de llaves públicas

RSA: porque es seguro

- Supongamos que sabes la llave pública de BOB (n,e). Qué tan dificil es determinar d?
- Esencialmente para encontrar los factores de n sin saber los dos factores p y q
  - hecho: factorizar un número grande es muy dificil