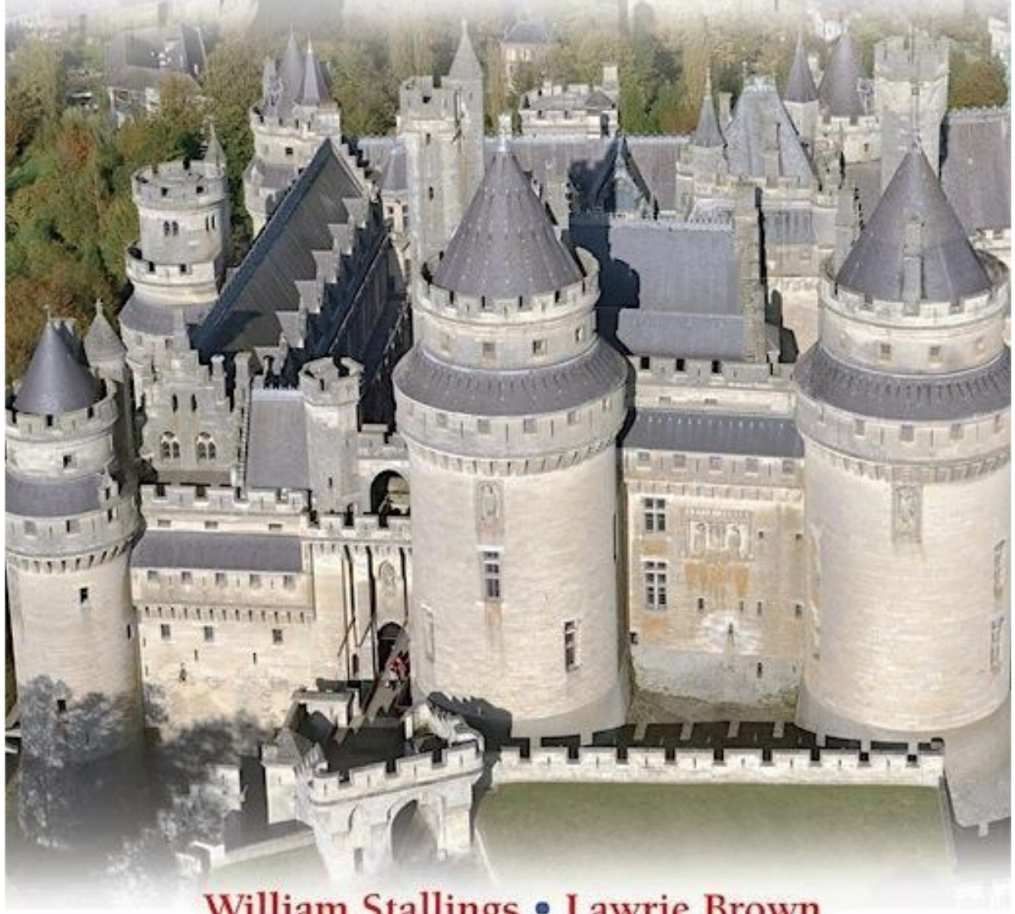
COMPUTER SECURITY

PRINCIPLES AND PRACTICE

Third Edition



William Stallings • Lawrie Brown

Capítulo 2

Herramientas criptográficas

Cifrado simétrico

- La técnica universal para proporcionar confidencialidad para datos transmitidos o almacenados
- También conocido como cifrado convencional o cifrado de clave única.
- Dos requisitos para un uso seguro:
  - Necesita un algoritmo de cifrado fuerte
  - El remitente y el receptor deben haber obtenido copias de la clave secreta de manera segura y deben mantener la clave segura.

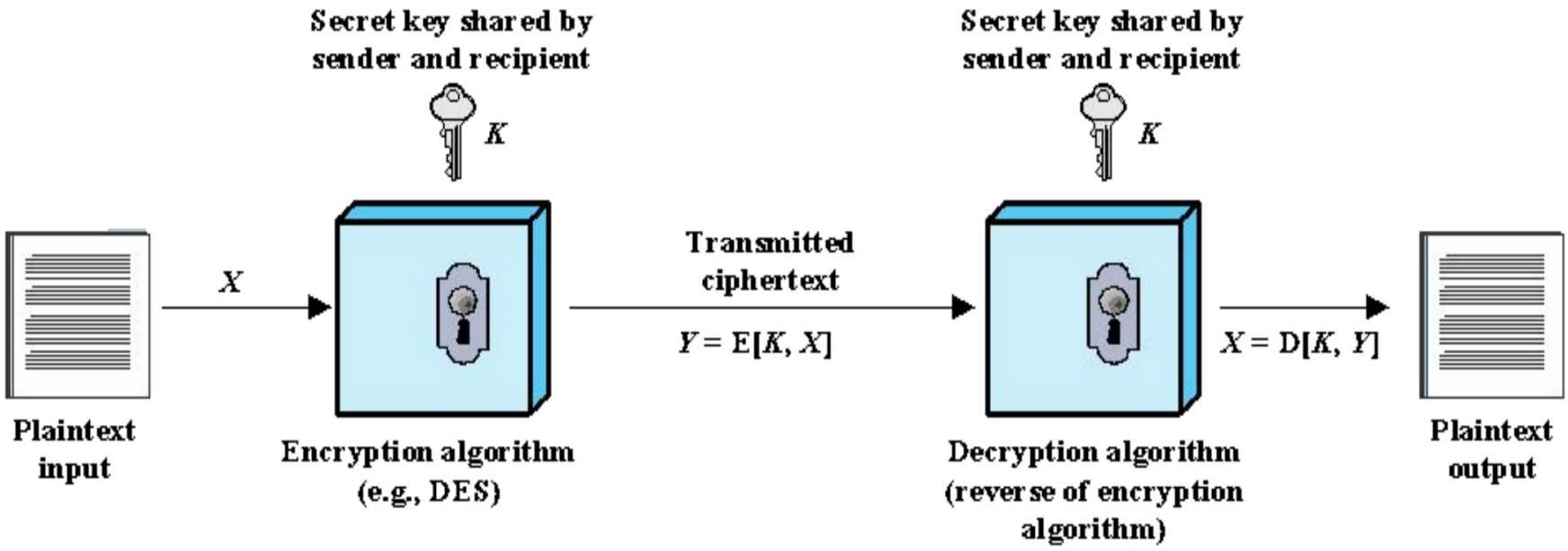


Figure 2.1 Simplified Model of Symmetric Encryption

tacng ymmetrc Encriptación

Ataques criptoanalíticos

- Confíe en:
  - Naturaleza del algoritmo
  - Algunos conocimientos de la Características generales del texto plano
  - Algunos ejemplos de pares de texto simple y texto cifrado
- Explota las características del algoritmo para intentar deducir un texto claro específico o la clave que se está utilizando.
  - Si tiene éxito, todos los mensajes futuros y pasados cifrados con esa clave se verán comprometidos.

Ataque de fuerza bruta

- Probar todas las claves posibles en algún texto cifrado hasta obtener una traducción inteligible en texto simple
  - En promedio, se deben probar la mitad de todas las claves posibles para lograrlo. éxito

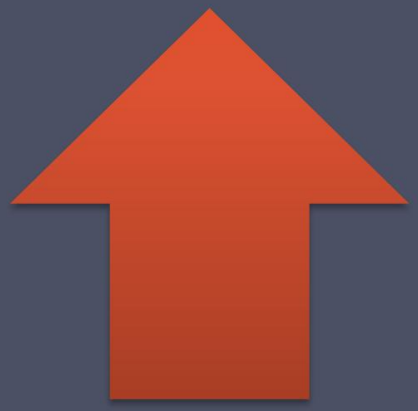
Tabla 2.1

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Comparación de tres modelos simétricos populares
Algoritmos de cifrado

Estándar de cifrado de datos (DEL)



- El esquema de cifrado más utilizado
  - FIPS PUB 46
  - Conocido como el cifrado de datos Algoritmo (DEA)
  - Utiliza un bloque de texto simple de 64 bits y una clave de 56 bits para producir un bloque de texto cifrado de 64 bits

- Preocupaciones sobre la fuerza:
  - Preocupaciones sobre el algoritmo
    - DES es el algoritmo de cifrado más estudiado que existe.
  - Uso de clave de 56 bits
    - La Electronic Frontier Foundation (EFF) anunció en julio de 1998 que había descifrado un código DES.

Tabla 2.2

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Tiempo promedio necesario para una búsqueda exhaustiva de claves

Triple DES (3DES)

- Repite el algoritmo básico DES tres veces utilizando dos o tres claves únicas
- Primero estandarizado para su uso en aplicaciones financieras en Norma ANSI X9.17 en 1985
- Atracciones:
  - La longitud de clave de 168 bits supera la vulnerabilidad a los ataques de fuerza bruta de DES
  - El algoritmo de cifrado subyacente es el mismo que en DES
- Desventajas:
  - El algoritmo es lento en el software.
  - Utiliza un tamaño de bloque de 64 bits

Cifrado avanzado Estándar (AES)

Necesitaba un reemplazo para 3DES

3DES no era razonable para un uso a largo plazo

El NIST solicitó propuestas para un nuevo AES en 1997

- Debe tener un nivel de seguridad igual o mejor que 3DES
- Eficiencia significativamente mejorada
- Cifrado de bloques simétricos
- Datos de 128 bits y claves de 128/192/256 bits

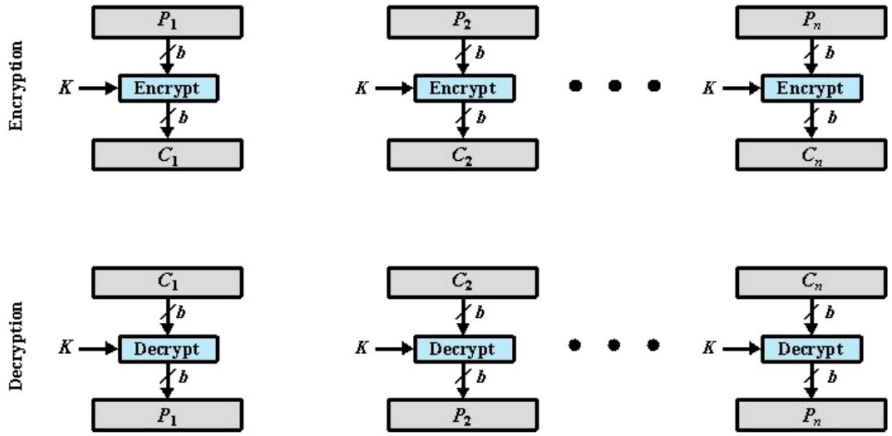
Seleccionado en Rijndael Noviembre de 2001

Publicado como

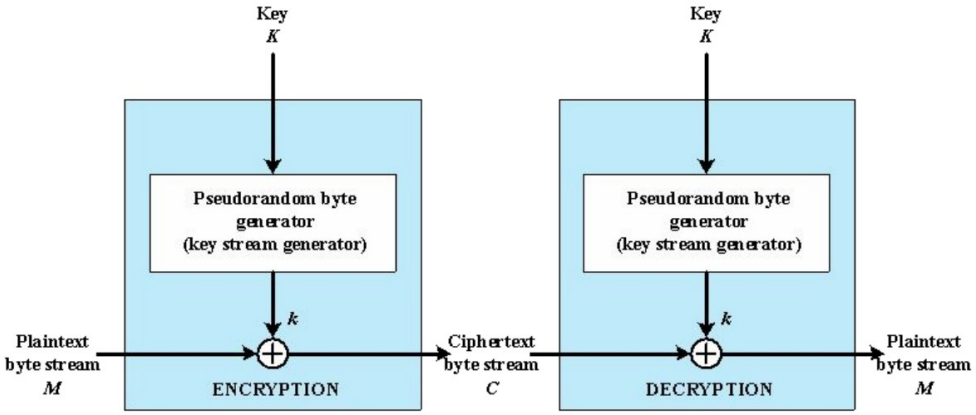
Norma FIPS 197

Cuestiones prácticas de seguridad

- Normalmente, el cifrado simétrico se aplica a una unidad de datos más grande que un solo bloque de 64 o 128 bits.
- El modo de libro de códigos electrónico (ECB) es el enfoque más simple para el cifrado de múltiples bloques.
  - Cada bloque de texto sin formato se cifra utilizando la misma clave
  - Los criptoanalistas pueden ser capaces de explotar regularidades en el texto sin formato
- Modos de funcionamiento
  - Se desarrollaron técnicas alternativas para aumentar la seguridad del cifrado de bloques simétricos para secuencias grandes
  - Supera las debilidades del BCE



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Figure 2.2 Types of Symmetric Encryption

Cifrados de bloque y de flujo

Cifrado de bloque

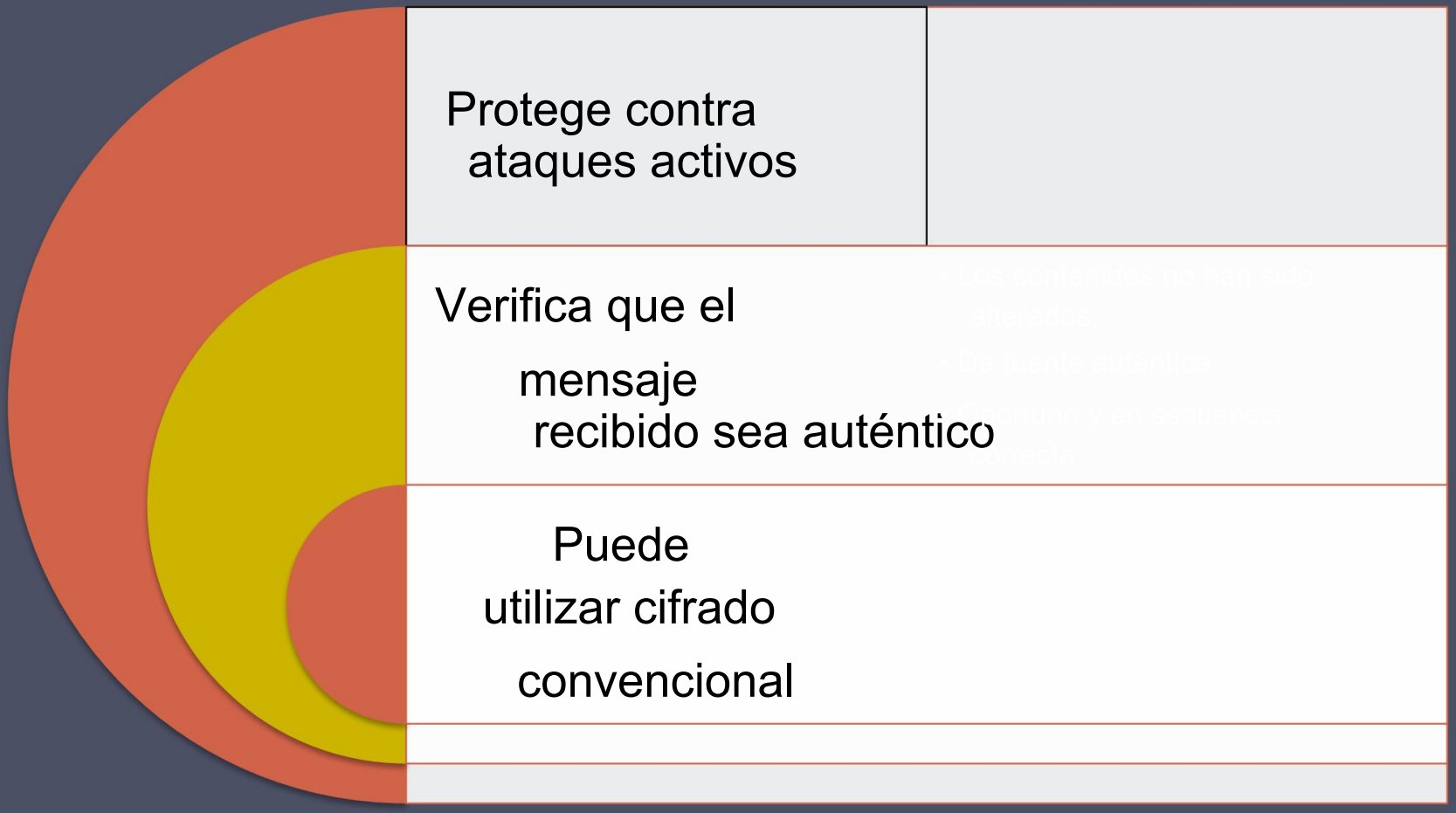
• Procesa la entrada de un bloque de elementos a la vez • Produce un bloque de salida para cada bloque de entrada • Puede reutilizar claves • Más común

Cifrado de flujo

• Procesa los elementos de entrada de forma continua • Produce un elemento de salida a la vez • La ventaja principal es que casi siempre son más rápidos y utilizar mucho menos código

• Cifra el texto sin formato un byte a la vez • El flujo pseudoaleatorio es aquel que es impredecible sin el conocimiento de la clave de entrada

Autenticación de mensajes



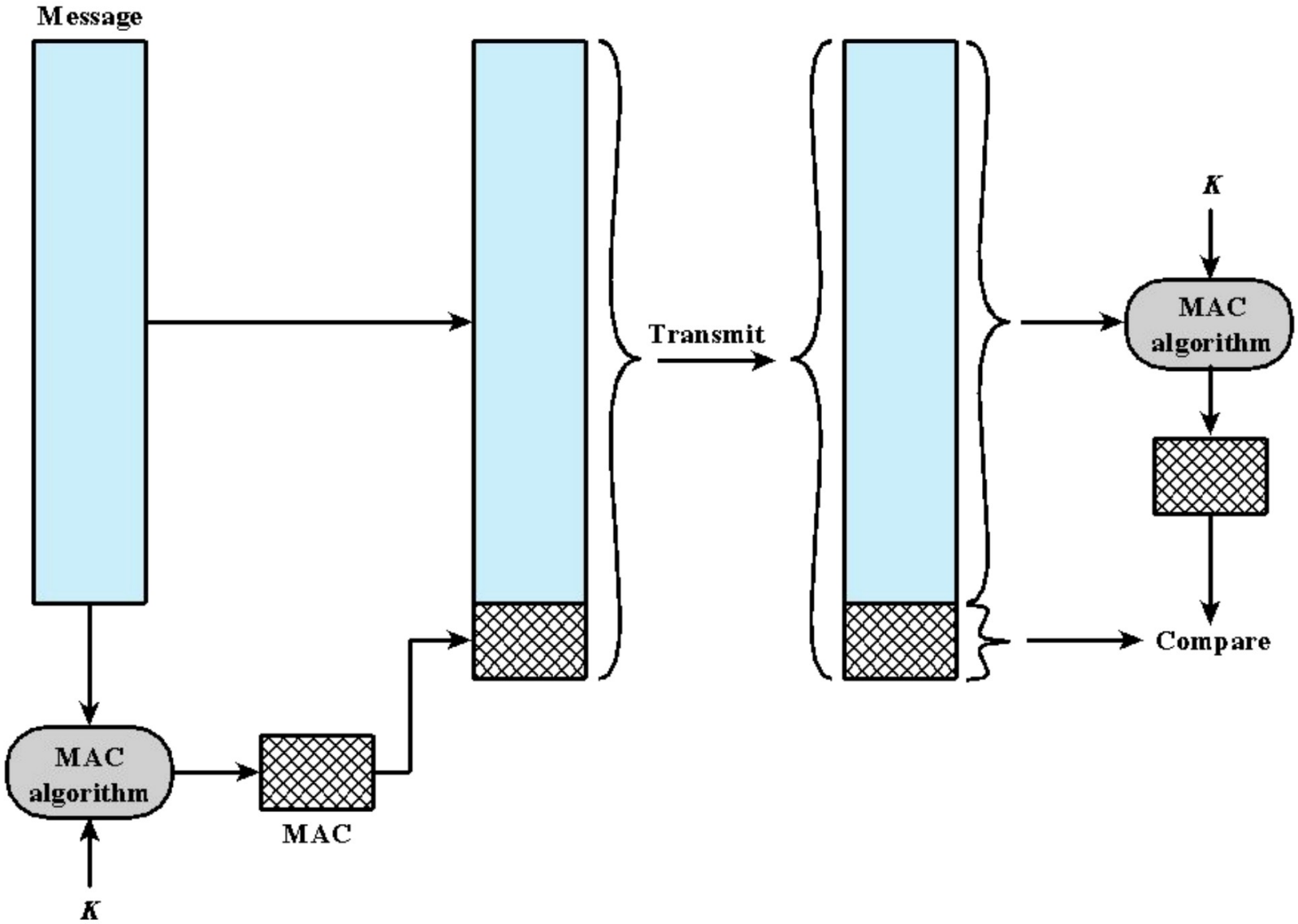
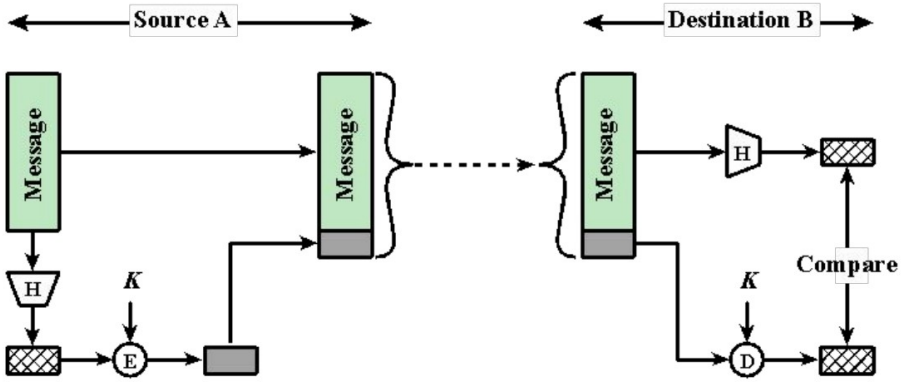
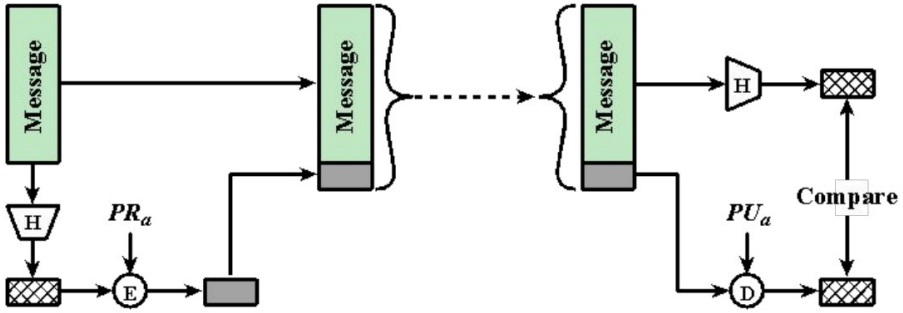


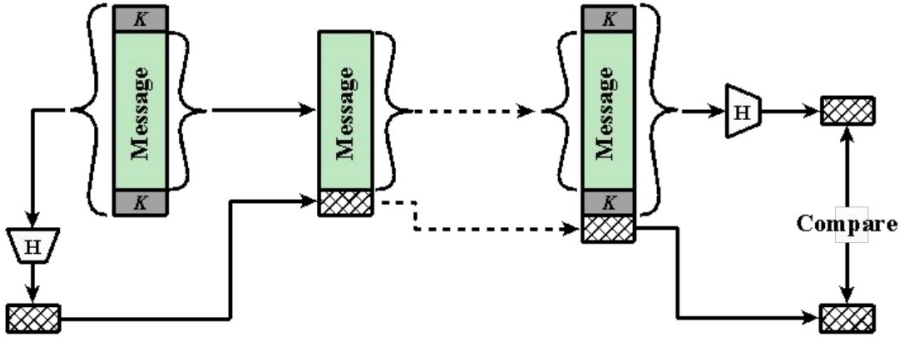
Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).



(a) Using symmetric encryption



(b) Using public-key encryption



(c) Using secret value

Figure 2.5 Message Authentication Using a One-Way Hash Function.

Requisitos de la función hash

- Se puede aplicar a un bloque de datos de cualquier tamaño.
- Produce una salida de longitud fija
- H(x) es relativamente fácil de calcular para cualquier x dado
- Unidireccional o resistente a imágenes previas
  - Es computacionalmente inviable encontrar x tal que H(x) = h
- No es computacionalmente factible encontrar y ≠ x tal que H(y) = H(x)
- Resistente a colisiones o fuerte resistencia a colisiones •
  Computacionalmente no es factible encontrar ningún par (x,y) tal que H(x) = H(y)

Seguridad de las funciones hash

Hay dos enfoques para atacar una función hash segura:

- **Criptoanálisis**
  - Explotar debilidades lógicas en el algoritmo
- **Ataque de fuerza bruta**
  - La fuerza de la función hash depende únicamente de la longitud del código hash producido por el algoritmo.

SHA, el algoritmo hash más utilizado

Aplicaciones adicionales de la función hash segura:

- **Contraseñas**
  - El hash de una contraseña es almacenado por un sistema operativo
- **Detección de intrusiones**
  - Almacenar H(F) para cada archivo en un sistema y proteger los valores hash

Cifrado de clave pública Estructura

Propuesto públicamente por Diffie y Hellman en 1976

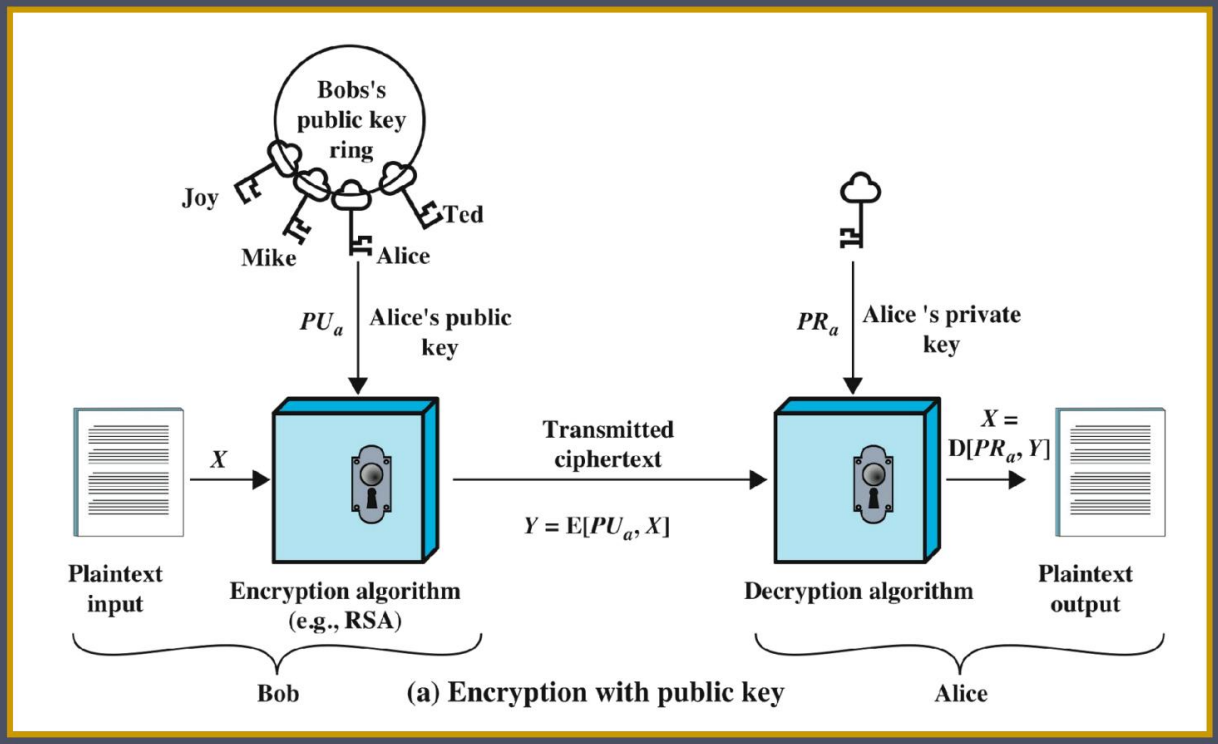
Basado en matemáticas l funciones

Asimétrico

- Utiliza dos teclas independientes
- Clave pública y clave privada
- La clave pública se hace pública para que otros la puedan consultar.

usar

Se necesita algún tipo de protocolo para la distribución.



- Texto sin formato • Mensaje o datos legibles que se introducen en el algoritmo como entrada • Algoritmo de cifrado • Realiza transformaciones en el texto sin formato
- Clave pública y privada • Par de claves, una para el cifrado y otra para el descifrado • Texto cifrado • Mensaje codificado producido como salida
- Clave de descifrado • Produce el texto sin formato original

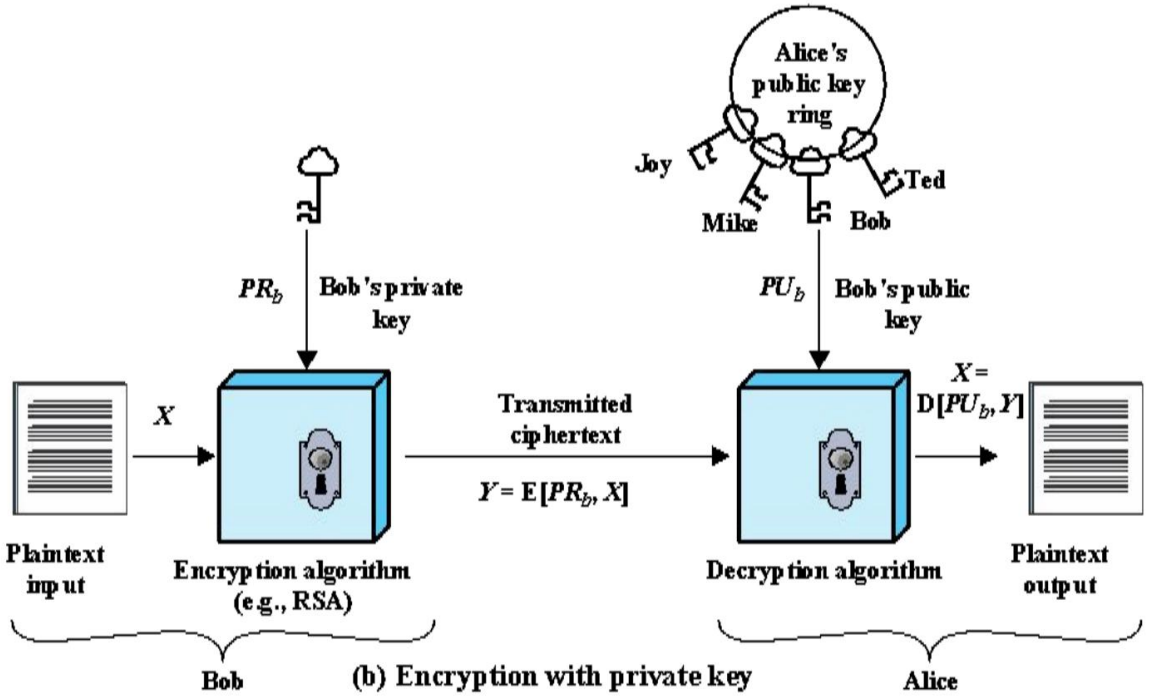


Figure 2.6 Public-Key Cryptography

- El usuario cifra los datos utilizando su propia clave privada
- Cualquiera que conozca la clave pública correspondiente podrá descifrar el mensaje.

Tabla 2.3

Aplicaciones de los criptosistemas de clave pública

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Requisitos para la clave pública

Criptosistemas

Es computacionalmente
fácil crear pares de claves

Útil si se puede usar
cualquiera de las teclas
para cada función

Es computacionalmente
fácil para el remitente
conocer la clave pública
para cifrar los
mensajes

Es computacionalmente
inviable para el
oponente
recuperar el mensaje
original de otra manera

Computacionalmente
fácil para el receptor
que conoce la clave
privada para
descifrar el texto cifrado

Es computacionalmente
inviable para el
oponente
determinar la clave
privada a partir de la clave pública

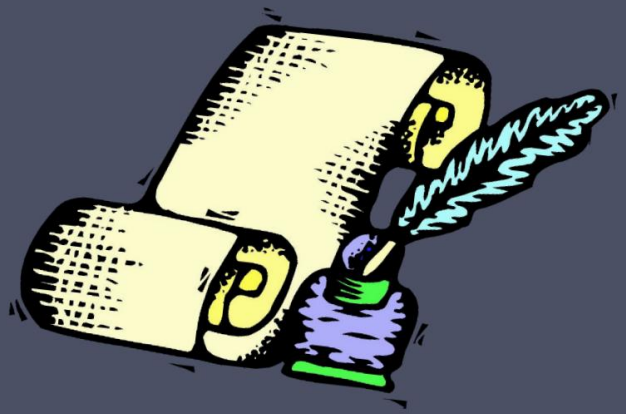
Cifrado asimétrico

Algoritmos

RSA (remachado, Shamir, Adleman)	Desarrollado en 1977	El enfoque más ampliamente aceptado e implementado para el cifrado de clave pública	Cifrado de bloques en el que el texto simple y el texto cifrado son números enteros entre 0 y n-1 para algún valor n.
Algoritmo de intercambio de claves Diffie-Hellman	Permite que dos usuarios lleguen a un acuerdo de forma segura sobre un secreto compartido que puede utilizarse como clave secreta para el cifrado simétrico posterior de mensajes.	Limitado al intercambio de las claves	
Digital Firma Estándar (Sistema de Seguridad Alimentaria)	Proporciona únicamente una función de firma digital con SHA-1	No se puede utilizar para cifrado o intercambio de claves.	
Criptografía de curva elíptica (CEC)	Seguridad como RSA, pero con claves mucho más pequeñas		

Firmas digitales

- Se utiliza para autenticar tanto la fuente como los datos. integridad
- Creado mediante el cifrado del código hash con clave privada
- No proporciona confidencialidad
  - Incluso en el caso de cifrado completo
  - El mensaje está a salvo de alteraciones, pero no de escuchas clandestinas.



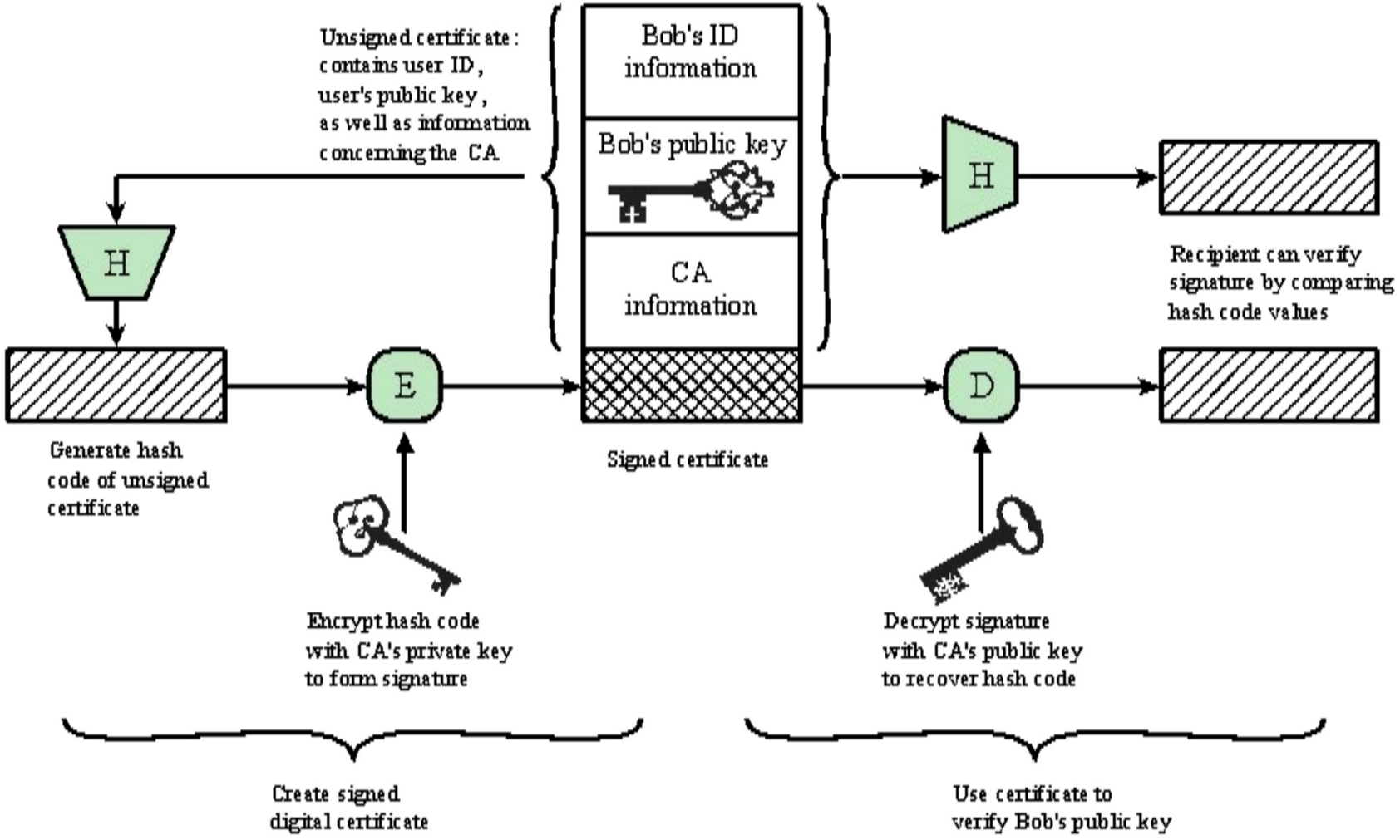
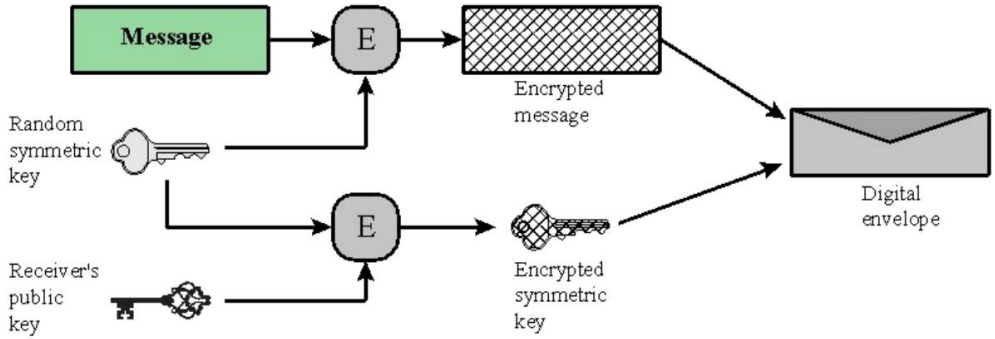


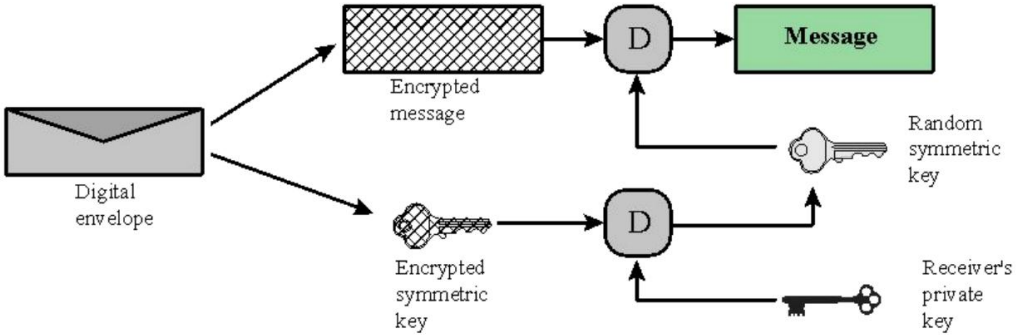
Figure 2.7 Public-Key Certificate Use

Digital Sobres

- Protege un mensaje
  Sin necesidad de acordar primero que el remitente y el receptor tengan la misma clave secreta
- Equivale a lo mismo que un sobre cerrado que contiene una carta sin firmar.



(a) Creation of a digital envelope



(b) Opening a digital envelope

Figure 2.8 Digital Envelopes

aleatorio Números

Los usos incluyen la generación de:

- Claves para algoritmos de clave pública
- Clave de flujo para cifrado de flujo simétrico
- Clave simétrica para usar como clave de sesión temporal o para crear un sobre digital
- Protocolo de enlace para evitar ataques de repetición
- Clave de sesión

Número aleatorio Requisitos

Aleatoriedad

- Criterios:
  - Distribución uniforme
    - La frecuencia de aparición de cada uno de los números debe ser aproximadamente la misma.
  - Independencia
    - Ningún valor de la secuencia puede inferirse de los demás.

Imprevisibilidad

- Cada número es estadísticamente independiente de otros números en el secuencia
- El oponente no debería poder predecir elementos futuros de la secuencia basándose en elementos anteriores.

anónimo versus

Pseudoaleatorio

Las aplicaciones criptográficas generalmente utilizan técnicas algorítmicas para la generación de números aleatorios.

- Los algoritmos son deterministas y, por lo tanto, producen secuencias de números que no son estadísticamente aleatorios.

Los números pseudoaleatorios son:

- Secuencias producidas que satisfacen pruebas de aleatoriedad estadística
- Probablemente sea predecible

Generador de números aleatorios verdaderos (TRNG):

- Utiliza una fuente no determinista para producir aleatoriedad.
- La mayoría opera midiendo procesos naturales impredecibles.
  - p. ej. radiación, descarga de gas, condensadores con fugas
- Cada vez se proporciona más en procesadores modernos

Aplicación práctica:

Cifrado de datos almacenados

Es común cifrar los datos transmitidos

Mucho menos común para los datos almacenados

A menudo hay poca protección más allá de la autenticación del dominio y los controles de acceso al sistema operativo.

Los datos se archivan por períodos indefinidos.

Aunque se borren, hasta que se reutilicen los sectores del disco, los datos son recuperables.

Enfoques para cifrar datos almacenados:

- Utilice un paquete de cifrado disponible comercialmente
- Dispositivo back-end
- Cifrado de cinta basado en biblioteca
- Cifrado de datos de fondo de la computadora portátil o PC

Resumen

- Confidencialidad con cifrado simétrico
  - Cifrado simétrico
  - Algoritmos de cifrado de bloques simétricos
  - Cifrados de flujo
- Autenticación de mensajes y funciones hash
  - Autenticación mediante cifrado simétrico
  - Autenticación de mensajes Sin cifrado de mensajes
  - Funciones hash seguras
  - Otras aplicaciones de las funciones hash
- Aleatorio y números pseudoaleatorios
  - El uso de números aleatorios
  - Aleatorio versus pseudoaleatorio

- Cifrado de clave pública
  - Estructura
  - Aplicaciones de los criptosistemas de clave pública
  - Requisitos para la criptografía de clave pública
  - Algoritmos de cifrado asimétrico
- Firmas digitales y gestión de claves
  - Firma digital
  - Certificados de clave pública
  - Intercambio de claves simétricas mediante cifrado de clave pública
  - Sobres digitales