Semana 12: Encriptación

Criptografía

Aprendizajes esperados

Contenidos:

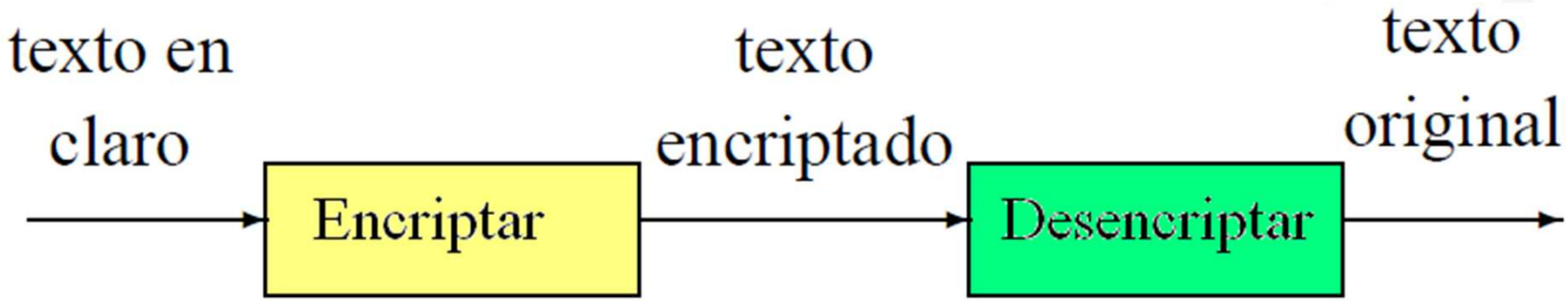
- Conceptos básicos de criptografía
- Tipos de cifradores
- Cifrado de bloques

Conceptos básicos

• Un mensaje en su estado original consiste de **TEXTO EN CLARO**. Se “disfraza” por un proceso de **ENCRIPTACIÓN**, el cual produce **TEXTO ENCRIPTADO**.

•El proceso inverso de la **ENCRIPTACIÓN** es la **DESENCRIPTACIÓN**.

Conceptos básicos



Conceptos básicos

- Usualmente, M representa el texto en claro (no necesariamente es “texto”), C el texto encriptado.
- Notar que C puede ser más largo que M.
- Entonces, la **encriptación** es una función tal que E(M) = C, y la **desencriptación** es una función en la que D(C) = M.

Conceptos básicos

- Además, se requiere que: D(E(M)) = M.
- Las funciones E y D son implementadas por un **ALGORITMO CRIPTOGRÁFICO** (o **ALGORITMO DE CIFRADO**).

Conceptos básicos

- Además, se requiere que: D(E(M)) = M.
- Las funciones E y D son implementadas por un **ALGORITMO CRIPTOGRÁFICO** (o **ALGORITMO DE CIFRADO**).

Conceptos básicos

- El algoritmo NO debe depender por su seguridad, del hecho que sea desconocido por el adversario. Por lo tanto, todo algoritmo moderno depende de una **clave** (**key**), escogida al azar de un espacio grande.
- Con esto, $E_k(M)=C$, $D_k(C)=M$ y $D_k(E_k(M))=M$.

Conceptos básicos

- Las **claves** han de permanecer seguras. Si se compromete la seguridad de las claves empleadas en el sistema, NO importa lo seguro o infranqueable que éste sea, terminará por caer tarde o temprano.
- Existen ciertas **claves**, denominadas **claves débiles**, que comprometen la seguridad.

Conceptos básicos

- La **clave k**, es una **clave débil**, si deja el criptograma igual que el texto plano, o muy parecido al texto plano, es decir, $E_k(M)=M$.
- En un buen criptosistema la cantidad de este tipo de claves es nula o muy pequeña, comparada con la cantidad total de claves, con lo cual la probabilidad de utilizar una de estas claves es nula o prácticamente nula.

Criptoanálisis

• El **CRIPTOANÁLISIS** es la ciencia de recuperar el mensaje original sin tener acceso a la clave (si la clave se revela por otros medios se llama un **compromiso**).

•Un intento de criptoanálisis es un **ataque** a la seguridad.

•Hay cuatro tipos principales:

Criptoanálisis

- **Sólo texto cifrado** – sólo se conoce el algoritmo/ texto cifrado.
- **Conoce texto plano** – conoce/sospecha texto plano y texto cifrado.
- **Texto plano elegido** – selecciona texto plano y obtiene texto cifrado para atacar el cifrador.
- **Texto cifrado elegido** – selecciona texto cifrado y obtiene texto plano para atacar el cifrador.

Criptoanálisis

- **Texto elegido** – selecciona ya sea texto plano o cifrado para encriptar o desencriptar y atacar el cifrador.

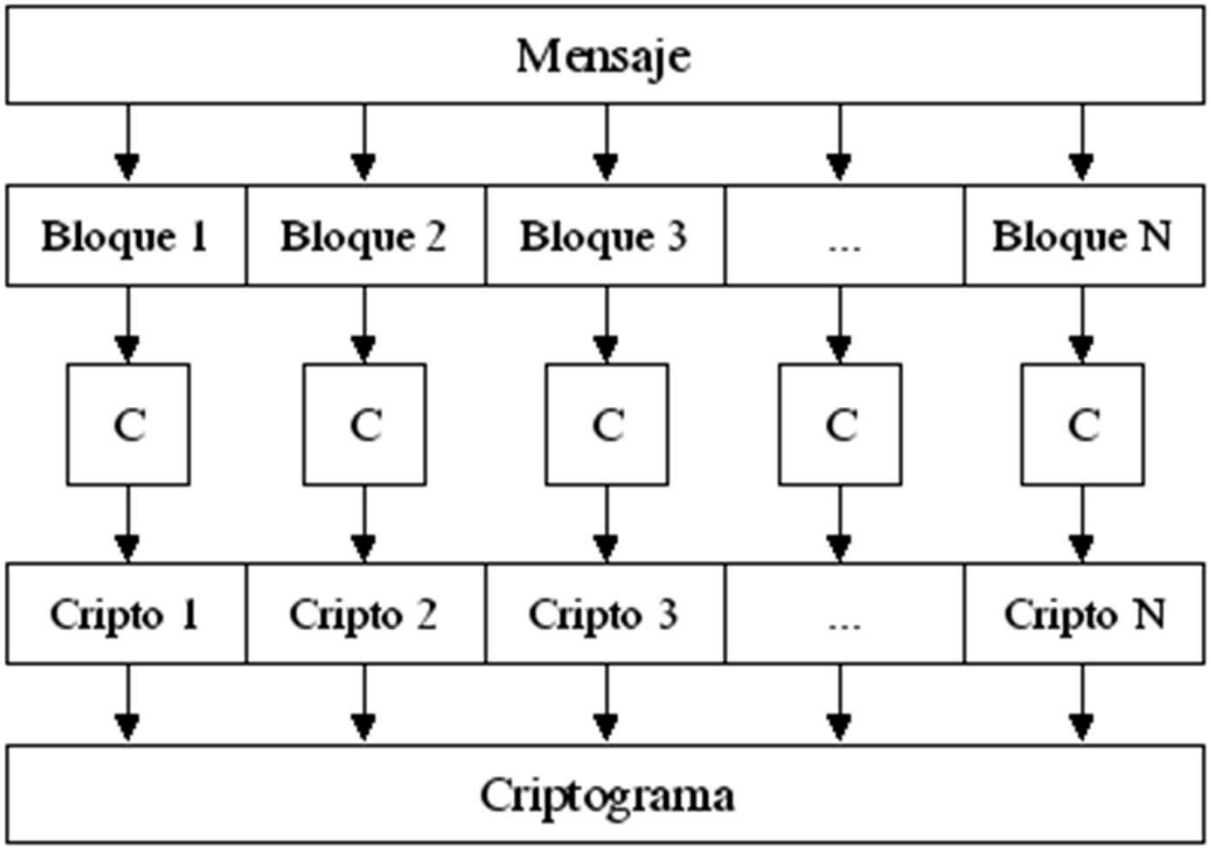
Cifrado de bloques

- Los algoritmos de **cifrado por bloques** emplean bloques de tamaño fijo del texto en claro y crean un bloque de tamaño fijo de texto cifrado, por lo general de igual tamaño que la entrada.
- Dicho tamaño de bloque debe ser grande, así se evitan ataques de texto cifrado.

Cifrado de bloques

• El esquema de funcionamiento general de los **sistemas de cifrado de bloques** es bastante simple, se divide la información a cifrar en bloques de un mismo tamaño y a cada uno de ellos se le aplican una serie de transformaciones para producir el correspondiente bloque de texto cifrado. Esquemáticamente:

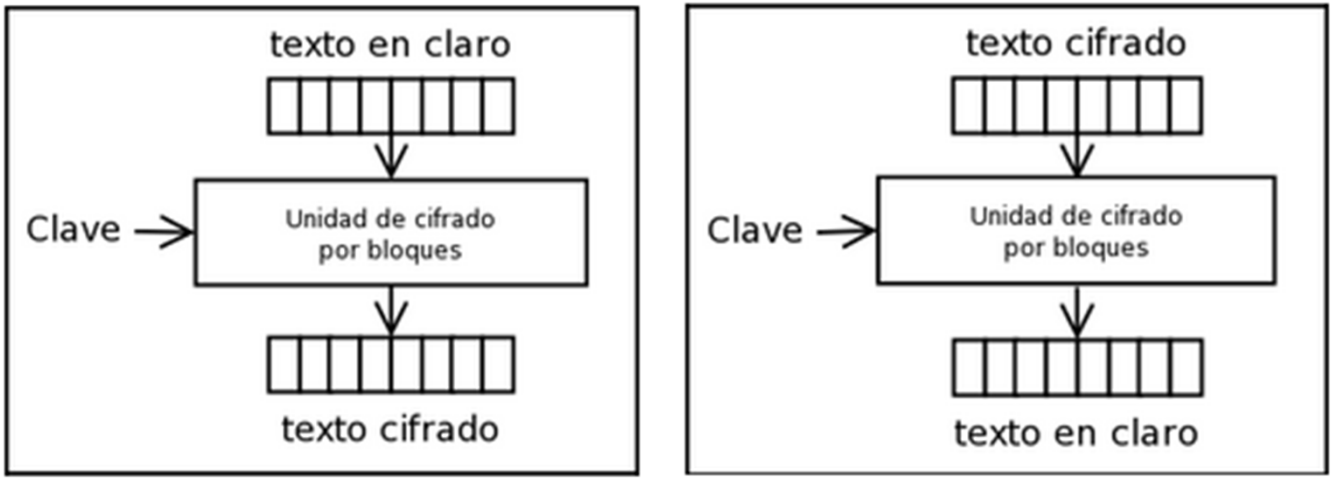
Sistemas de cifrado de bloques



Cifrado de bloques

- En tanto, la asignación de bloques de entrada a bloques de salida debe ser uno a uno, haciendo así el proceso reversible y pareciendo aleatoria.
- Para la asignación de bloques, los **algoritmos de cifrado simétrico** realizan sustituciones y permutaciones en el texto en claro hasta obtener el texto cifrado.

Cifrado de bloques



Tipos de cifradores

- Actualmente, la criptografía se puede entender como el conjunto de técnicas que resuelven los siguientes problemas de seguridad de la información: la **autenticidad**, la **integridad**, la **confidencialidad** y el **no rechazo**.
- Desde este punto de vista, la criptografía se divide en dos grandes ramas: la **criptografía simétrica** y la **asimétrica**.

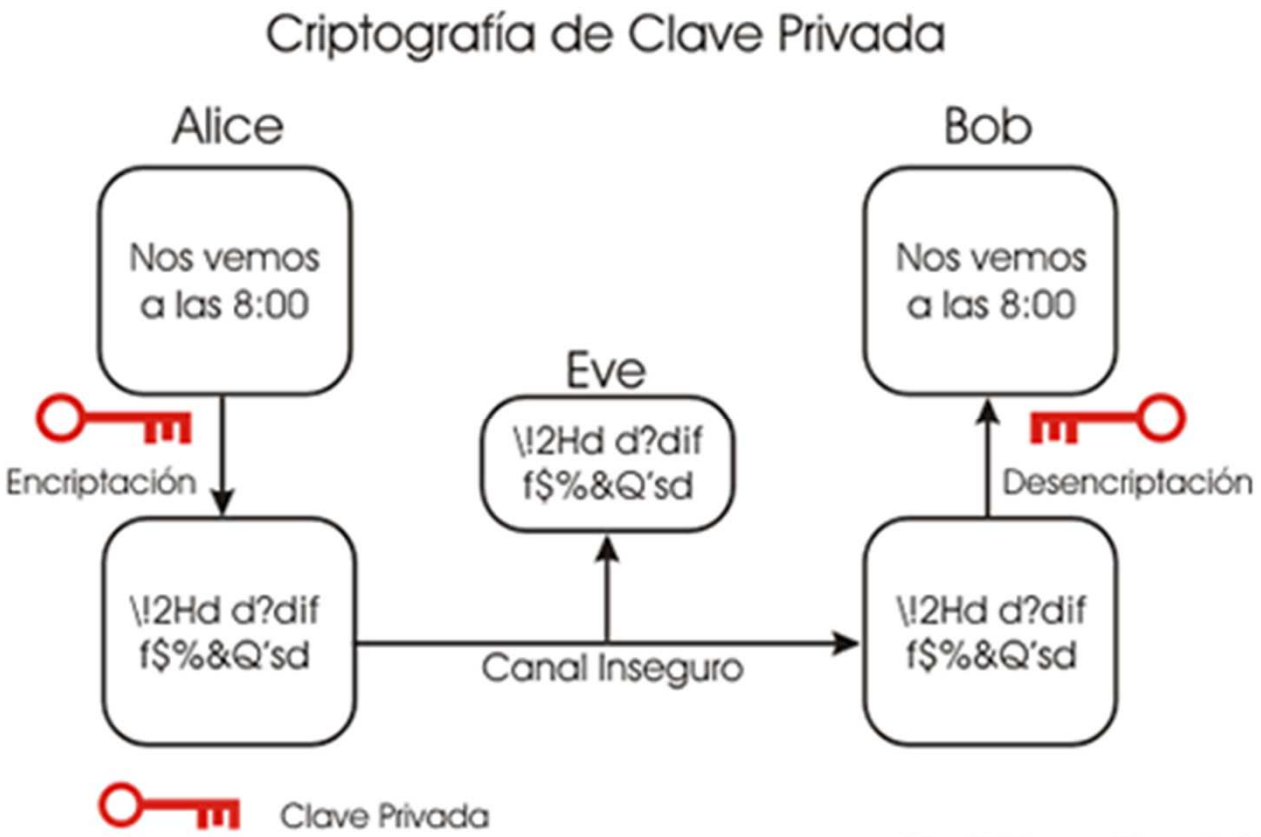
Tipos de cifradores

- Esencialmente, con la primera se resuelven los problemas de confidencialidad e integridad, mientras que con la segunda se resuelven los de autenticidad y no rechazo.
- En general, el proceso criptográfico se aplica a un mensaje de entrada (mensaje original), y da como resultado el **mensaje cifrado**.

Tipos de cifradores

- Este mensaje cifrado sólo se puede descifrar (para conocer su contenido) con la **clave correspondiente**.
- La principal diferencia entre la **criptografía simétrica** y **asimétrica**, es que en la simétrica la clave de cifrar y descifrar es la misma, mientras que en la asimétrica se tiene una clave para cifrar y otra diferente para descifrar.

Tipos de cifradores

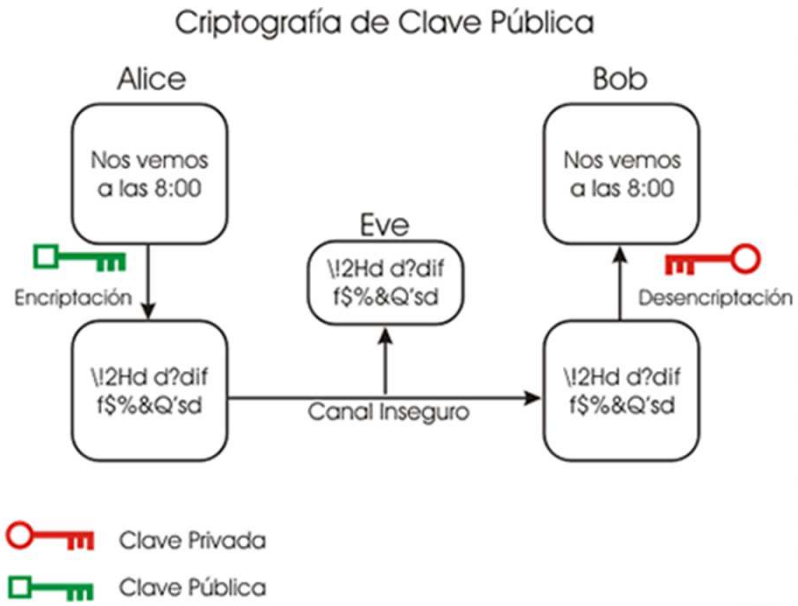


Tipos de cifradores

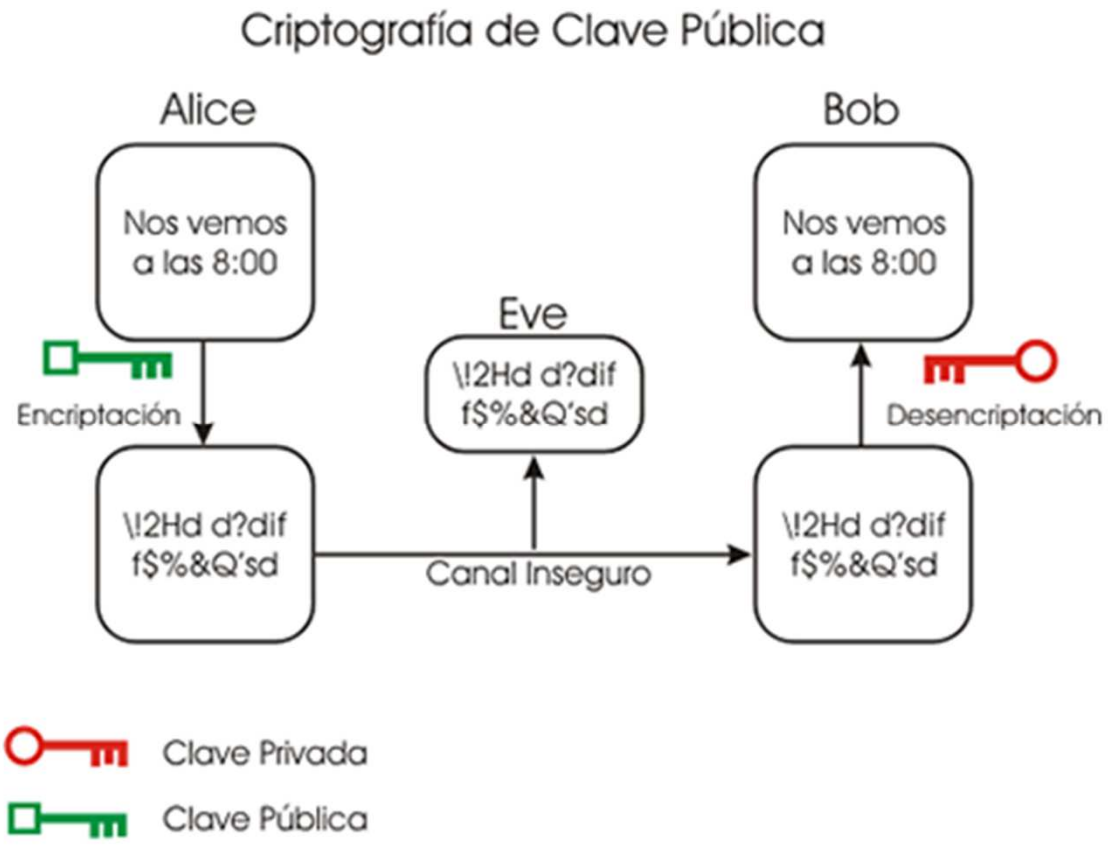
- En la **criptografía asimétrica** hay dos claves, una **pública** y otra **privada**.
- La **clave privada** no se puede obtener a partir de la **clave pública**.
- La **clave publica** puede enviarse a cualquier persona, la puede conocer todo el mundo.

Tipos de cifradores

- La **clave privada** únicamente determina ser conocida por su dueño y nunca debe ser revelada. Ambas claves están coordinadas.



Tipos de cifradores



Tipos de cifradores

- A la **criptografía simétrica** pertenecen los **cifradores de bloques**, los **cifradores de flujo** y las **funciones de hash**.
- Los **cifradores de flujo** se denominan así porque cifran bit por bit o byte por byte (ejemplos de **cifradores de flujo** son: **RC4**, **Seal**).

Tipos de cifradores

- De los **cifradores de bloques** (recordar que se llaman así porque cifran de bloque en bloque de, digamos, 64 bits), podemos citar al famoso **DES** (**Data Encryption Standar**); actualmente, se usa una versión más robusta, denominada **Triple-DES** (consistente en aplicar tres veces **DES**).

Tipos de cifradores

- De manera estándar el cifrado de mensajes se suele realizar utilizando la **criptografía simétrica** ya que permite realizar un cifrado muy rápido para mensajes de gran tamaño.
- Pero como hemos visto, se necesita previamente el intercambio seguro entre las partes de la clave y éste es su punto débil.

Tipos de cifradores

- La **criptografía asimétrica** o **de clave pública** resuelve satisfactoriamente el problema del intercambio de las claves, pero tiene el inconveniente de que consume mucho más tiempo de proceso, lo que la hace más lenta que la **simétrica**.

Resumen

- La