educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

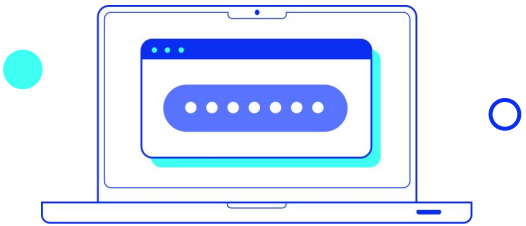
Módulo 2

educación IT
CODE YOUR FUTURE

Criptografía moderna

Fundamentos de la Criptografía moderna

En los criptosistemas clásicos, la seguridad se basa en el secreto del método y en el cifrado de caracteres. **En los criptosistemas modernos, la seguridad se basa en el secreto de la clave y en el cifrado de bits**.



Las bases teóricas de los criptosistemas modernos son:

- **Teoría de la información de Shannon**.
- **Teoría de números**.
- **Teoría de complejidad algorítmica**.

Teoría de la información de Shannon

La teoría de la información propuso el **cifrado mediante clave secreta utilizando las técnicas de difusión y confusión.**

La difusión dispersa las propiedades estadísticas, inherentes al lenguaje en el texto claro. Shannon propuso el uso de transposiciones o permutaciones.

La confusión permite generar caos en el resultado cifrado de tal forma que la dependencia entre texto claro, clave y criptograma sea lo más compleja posible. Shannon propuso la técnica de sustitución.

Teoría de números

La teoría de números estudia las **propiedades de los números enteros** (divisibilidad, módulo, máximo común divisor mediante algoritmo de Euclides, etc.).

Teoría de complejidad algorítmica

La teoría de la complejidad algorítmica nos indica la **fortaleza de un algoritmo**. Estudia la cantidad de pasos necesarios (tiempo de ejecución) y la memoria utilizada. Clasifica los problemas algorítmicos en fáciles o difíciles de tratar.

Dos problemas difíciles de tratar son la factorización de números grandes (PFNG) y el problema del logaritmo discreto (PLD).

Tipos de criptosistemas modernos

Criptografía simétrica

También llamada de **clave secreta**, se utiliza una clave única tanto para descifrar como para cifrar. Se usa principalmente para cifrar bloques o flujos de datos de cualquier tamaño, incluyendo mensajes, archivos, claves de cifrado y contraseñas.

Algoritmos de integridad de datos

Usados para evitar la **alteración de bloques** de datos tales como mensajes.

Criptografía asimétrica

También llamada de **clave pública**, usa una clave privada y secreta para cifrar y otra pública derivada a partir de la primera para descifrar. Se usa para ocultar pequeños bloques de datos, tales como claves de cifrado y valores de funciones de hash usados para firmas digitales.

Protocolos de autenticación

Son esquemas basados en el uso de algoritmos criptográficos diseñados para **autenticar la identidad de las entidades**.

Cifrado homomórfico

Permite **modificar datos cifrados** sin la necesidad de descifrarlos previamente.

Criptografía cuántica

Aun en fase de desarrollo, utiliza **propiedades de la mecánica cuántica** como la polarización de los fotones de luz o el entrelazamiento cuántico para resolver el problema de distribución de claves (QKD, *quantum key distribution*)

Criptografía post cuántica

Aun en fase de desarrollo, se enfoca en **hallar algoritmos criptográficos de clave pública** resistentes a los ataques posibles de una computadora cuántica.

Criptografía simétrica

Criptografía simétrica

Un esquema de criptografía simétrica posee cinco componentes:

Un texto claro

El texto claro, sea cual fuera su fuente, es convertido a una cadena de bits.

Un algoritmo de cifrado

Esta cadena de bits se cifra utilizando un algoritmo de cifrado basado en diversas técnicas derivadas en XOR (o exclusiva) y la clave secreta.

Una clave secreta

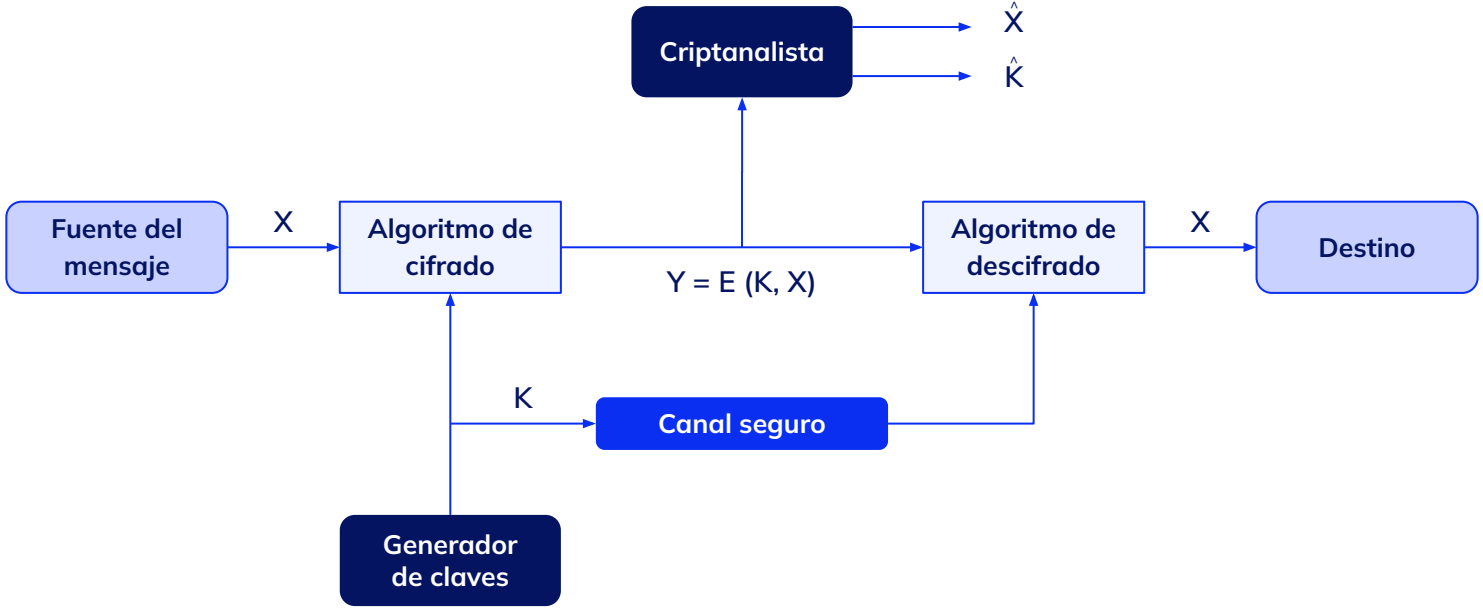
Un texto cifrado

El texto cifrado o criptograma es enviado al receptor.

Un algoritmo de descifrado

El receptor descifra el criptograma aplicando el algoritmo de descifrado, que generalmente es el algoritmo de cifrado aplicado en forma inversa.

Criptografía simétrica



Pasos para cifrar un texto plano

1. Seleccionar un algoritmo de cifrado.
2. Generar una clave de cifrado.
3. Generar un vector de inicialización (IV).
4. Seleccionar el modo de operación del algoritmo de cifrado.
5. Seleccionar el tipo de *padding*.
6. Cifrar el texto plano.

Los algoritmos pueden operar sobre bloques de datos o sobre flujos de datos.

> **Nota**: Dependiendo del algoritmo de cifrado y su modo de operación, algunos de estos pasos pueden no ser necesarios.

Bits de seguridad

- **La seguridad o fortaleza del cifrado se mide en bits de seguridad.**
- La cantidad máxima de bits de seguridad es la longitud de la clave de cifrado.
- **La seguridad real es menor debido a los posibles ataques.**

NIST (*National Institute of Standards and Technology of USA*) recomienda (2021):

- **112 bits de seguridad** deberían ser suficientes hasta 2030.
- **128 bits de seguridad** deberían ser suficientes hasta la próxima revolución en tecnología o matemática.

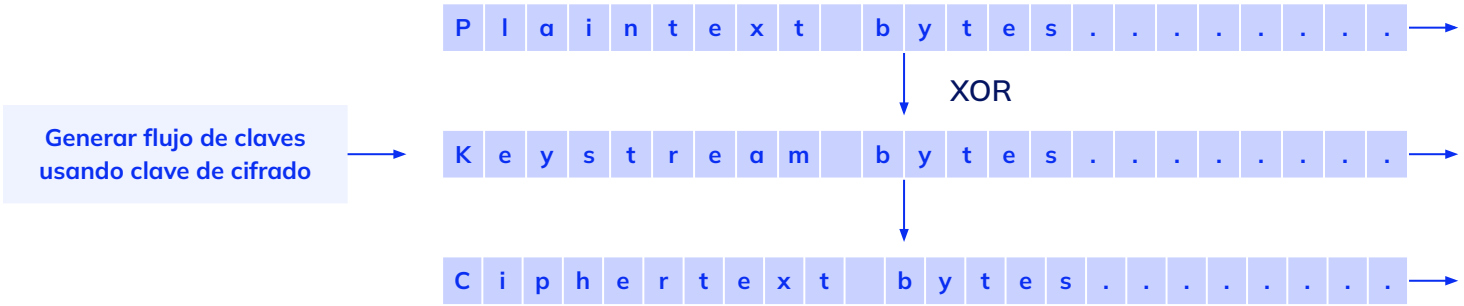
Una de estas revoluciones esperadas dentro de los años venideros es la computación cuántica. Las computadoras cuánticas ya existen, pero no son suficientemente poderosas aún para romper cifrados criptográficos.

Se espera que los algoritmos simétricos decaigan su nivel de seguridad a la mitad. Por ejemplo, el cifrado AES con clave de 256 bits decaerá su nivel de seguridad a 128 bits.

Cifrado por flujo

Los cifrados por flujo operan sobre bits o bytes de datos. No necesitan *padding* ni modos de operación.

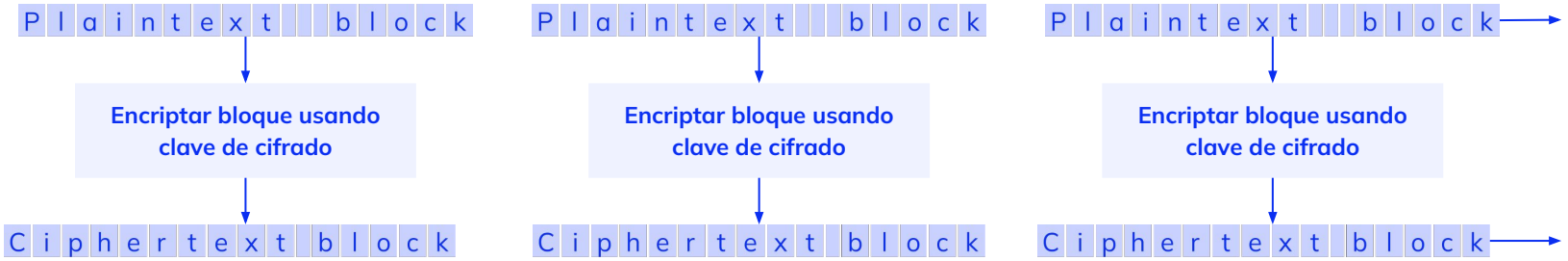
Son más fáciles de utilizar, de implementar y son más rápidos que los cifrados por bloques. Sin embargo, son menos seguros en general.



Cifrado por bloques

En el cifrado por bloques, se subdivide el texto plano en tantos bloques (del tamaño requerido por el algoritmo) **sean necesarios.**

Si el tamaño de los datos es menor al tamaño del bloque, o si no es múltiplo de este, habrá que rellenar un bloque (*padding*).



Cifrado por bloque: modos de operación

En un cifrado por bloques se toma un bloque de tamaño fijo de b bits y una clave y produce un bloque cifrado de b bits. Si la cantidad de texto plano es superior a b, se debe particionar el bloque.

Si se usa la misma clave para múltiples bloques diferentes, pueden producirse fallas en la seguridad.

Los modos de operación existen para poder utilizar el cifrado de bloques en una variedad de aplicaciones diferentes.

En esencia, **un modo de operación es una técnica para mejorar el efecto de un algoritmo criptográfico y adaptarlo a una aplicación.**

Los modos de operación más utilizados son:

- ***Electronic Codebook*** (ECB.)
- ***Cipher Block Chaining*** (CBC).
- ***Cipher Feedback*** (CFB).
- ***Output Feedback*** (OFB).
- ***Counter*** (CTR).

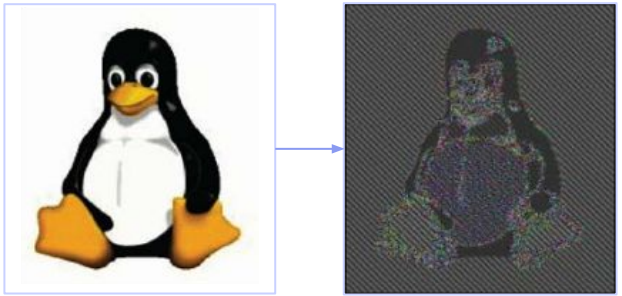
Electronic Codebook (ECB)

Cada bloque es cifrado independientemente del otro con la misma clave.

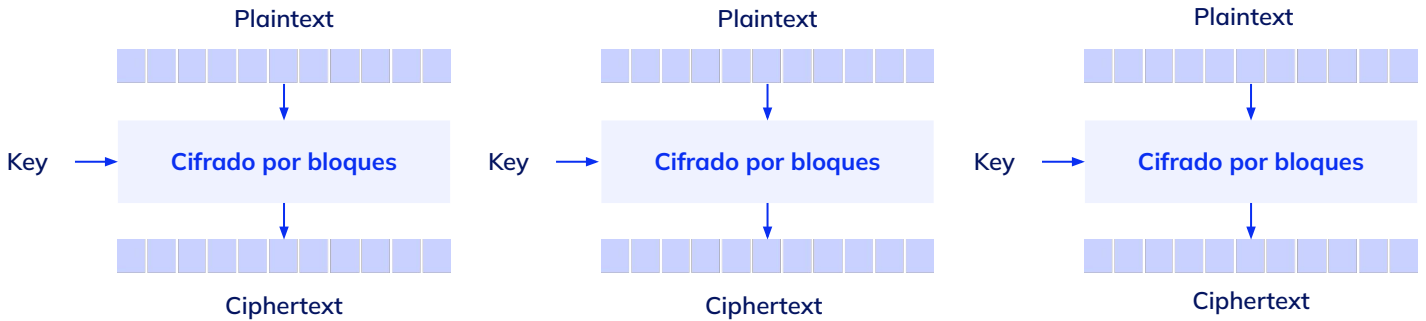
No usa IV ni un bloque previo de texto plano o cifrado.

Se utiliza para transmisión de valores simples (por ejemplo, una clave de cifrado), bases de datos, ficheros de acceso aleatorio. Es resistente a errores.

El mismo texto plano produce siempre el mismo texto cifrado. Es un problema de seguridad porque se preservan los patrones.



Electronic Codebook (ECB)



Cipher Block Chaining (CBC)

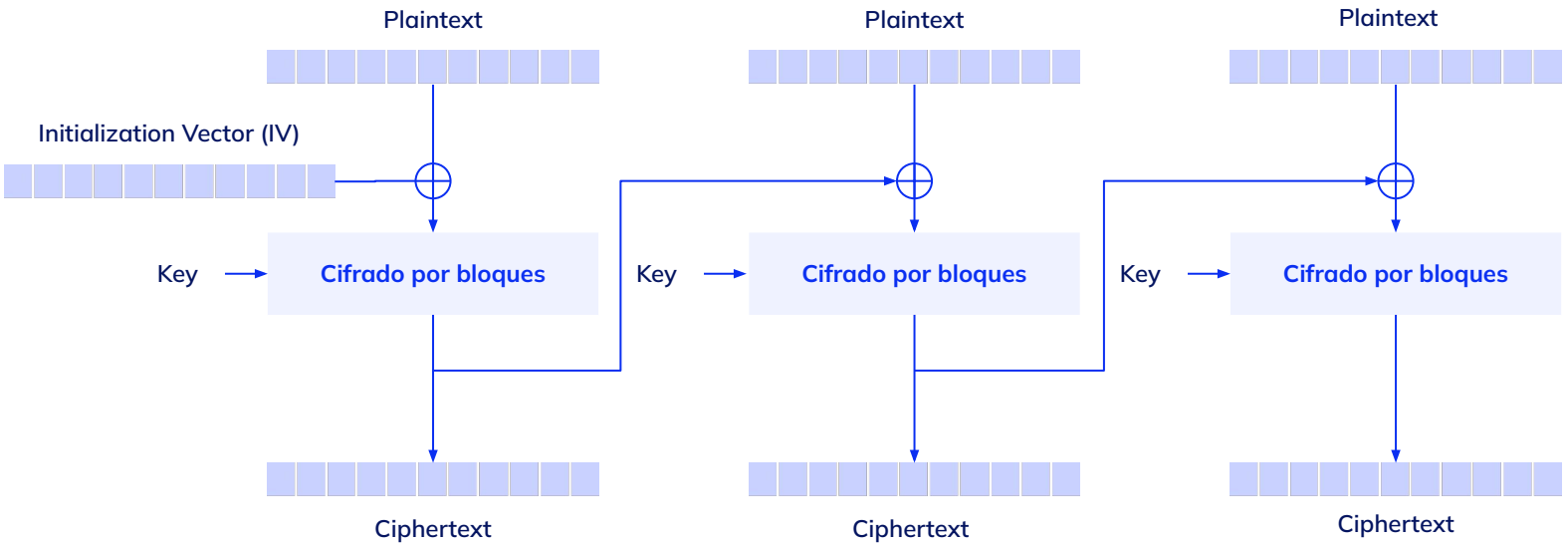
La entrada al algoritmo de cifrado es el XOR del próximo bloque de texto plano y el bloque precedente del texto cifrado.

Se utiliza para transmisiones de propósito general y para autenticación. Evita que un atacante inserte, elimine o reordene bloques del mensaje cifrado.

Usa un IV, que es un bloque de datos generado aleatoriamente con el mismo tamaño del bloque cifrado, pero generalmente no necesita mantenerse en secreto.

Este IV debe almacenarse junto al texto cifrado porque se necesita para el descifrado. Es un *nonce* (*number once*, número único).

Cipher Block Chaining (CBC)



Cipher Feedback (CFB)

Cada bloque es cifrado y luego combinado mediante la operación XOR con el siguiente bloque del mensaje original.

Al igual que el modo CBC, se emplea un IV a la hora de codificar el primer bloque. Con este método, si se produce un error en la transmisión, esta se vuelve a sincronizar de forma automática, a partir del segundo bloque consecutivo que llegue de forma correcta.

Una ventaja importante de este modo de operación radica en el hecho de que la longitud de los bloques del mensaje puede ser menor que la longitud del bloque que acepta el algoritmo de cifrado.

Se utiliza para transmisiones de propósito general y autenticación.

Counter (CTR)

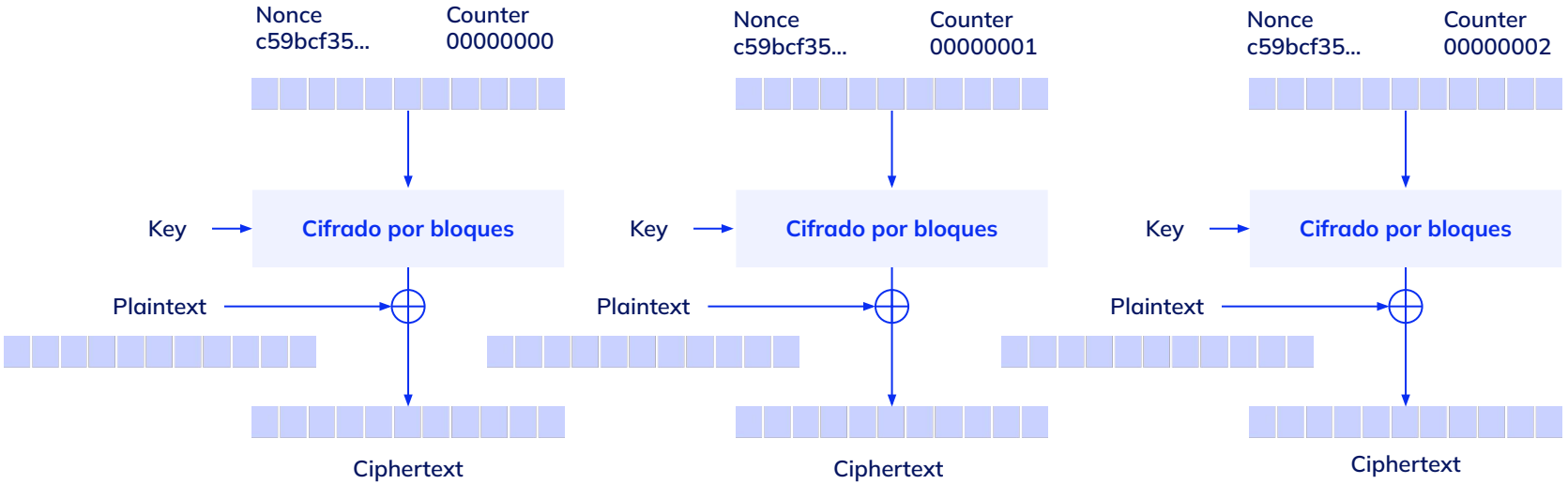
Se cifra una secuencia de bloques del contador.

Cada bloque del contador consiste en un nonce aleatorio de 64 bits concatenado con el entero de 64 bits del contador, que se incrementa bloque a bloque.

Es la base del modo GCM (*Galois/Counter Mode*).

Se utiliza para transmisiones de propósito general y en requerimientos de alta velocidad.

Counter (CTR): *mode encryption*



Galois/Counter Mode (GCM)

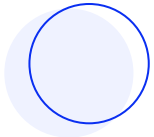
El texto cifrado se produce como en el modo CTR, con la diferencia que además de cifrar el texto, auténtica al criptograma.

Un oráculo es un programa, dispositivo o red que posee una clave de cifrado y es capaz de usarla.

La detección de cambios es importante porque muchos ataques funcionan cambiando el texto cifrado, y alimentando con estos textos cifrados modificados a un oráculo, para analizar su respuesta.

GCM solo funciona con bloques de 128 bits y requiere un IV de 96 bits. Es imposible de usar con algoritmos antiguos con bloques de 64 bits.

GCM es vulnerable a varios ataques si se reutiliza el par clave – IV. Como respuesta a esta debilidad, se inventó el modo AES-GCM-SIV.



Otros modos de operación

- **AES-GCM_SIV** (*Advanced Encryption Standard in Galois/Counter Mode with a Synthetic Initialization Vector*): es una variante del algoritmo de cifrado AES con GCM. Resiste el mal uso de la clave y el IV, asegurándose que el mismo IV no sea usado con mensajes distintos.

  Una desventaja es que el algoritmo necesita dos pasadas sobre el texto plano, incrementando el tiempo de operación.

- Otros modos de operación:
  - **CBC propagado** (PCBC).
  - ***Output feedback*** (OFB).
  - ***Counter with CBC-MAC*** (CCM).
  - **Carter-Wegman + CTR** (CWC).
  - ***Sophie Germain Counter*** (SGCM).

  No son muy populares.

¿Cuál modo de operación utilizar?

- ***Galois/Counter Mode*** (GCM): soporta autenticación y cifrado, no requiere padding, permite precalcular el flujo de claves y paralelizar el cifrado/descifrado. Si lo usa, asegúrese de no usar el IV más de una vez.
- ***Cipher Block Chaining*** (CBC): el estándar de facto anterior. Necesita padding aplicado al texto plano.

Padding para cifrado de bloques

Existen distintos tipos. El más habitual es el **PKCS#7** (*Public Key Cryptography Standard Number 7*) también denominado PKCS7 o PKCS o *padding* estándar de bloques.

Consiste de `N` bytes con el mismo valor `N` cada uno.

> **Por ejemplo**
>
> Si el último bloque de texto plano tiene 10 bytes de datos y 6 libres (tamaño de bloque 16 bytes), podría rellenarse con 6 bytes cada uno con el valor 0x06.

Si la longitud del texto plano es múltiplo del tamaño del bloque, PKCS#7 igualmente agrega *padding* porque en caso contrario, tras el descifrado del último bloque podría ser imposible detectar si el último byte pertenece al texto plano o al pad.

PKCS#7 se denomina a veces **PKCS#5.** Usa el mismo principio de relleno (`N` bytes de valor `N`) pero solamente está definido para **bloques de más de 64 bits.**

Desventaja

La desventaja de PKCS#7 es que el texto cifrado es susceptible de ataque de oráculo al *padding*. Este ataque solamente es posible si el atacante puede forzar el cifrado de una gran cantidad de texto plano controlado por él con la misma clave de cifrado.

¡Sigamos trabajando!