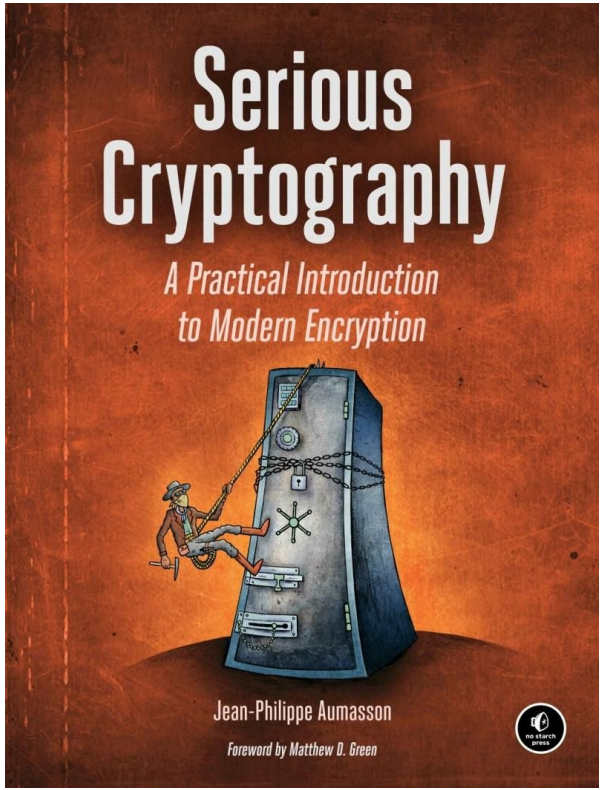
Criptografía Moderna I: Hashing y Cripto Simétrica

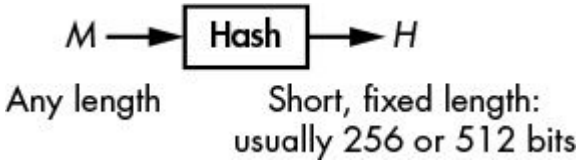
CC5325 - Taller de Hacking Competitivo

Problemas de Criptografía Moderna

- Poco resolvibles con herramientas (¡aunque de más que existen algunas!).
- Requieren entender un poco de cómo funcionan primitivas criptográficas (y qué cosas pueden salir mal).
- Esta unidad **no reemplaza** un curso formal de criptografía (tomen CC5301 - Intro a la Criptografía Moderna si les interesa aprender bien este tema).
- Libro útil: **Serious Cryptography de Jean-Philippe Aumasson**



Hashing



- Cambio chico en M -> Cambio grande en H
- Muy difícil calcular $Hash^{-1}(H)$
- Muy difícil encontrar colisiones

	MD5	SHA1	SHA3-256
"" (String vacío)	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	a7ffc6f8bf1ed76651c14756a061d662f580ff4de43b49fa82d80a4b80f8434a
"hola"	4d186321c1a7f0f354b297e8914ab240	99800b85d3383e3a2fb45eb7d0066a4879a9dad0	c0067d4af4e87f00dbac63b6156828237059172d1bbeac67427345d6a9fda484
"password"	5f4dcc3b5aa765d61d8327deb882cf99	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	c0067d4af4e87f00dbac63b6156828237059172d1bbeac67427345d6a9fda484

Rainbow Tables

5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

password

¡Muy pesadas!

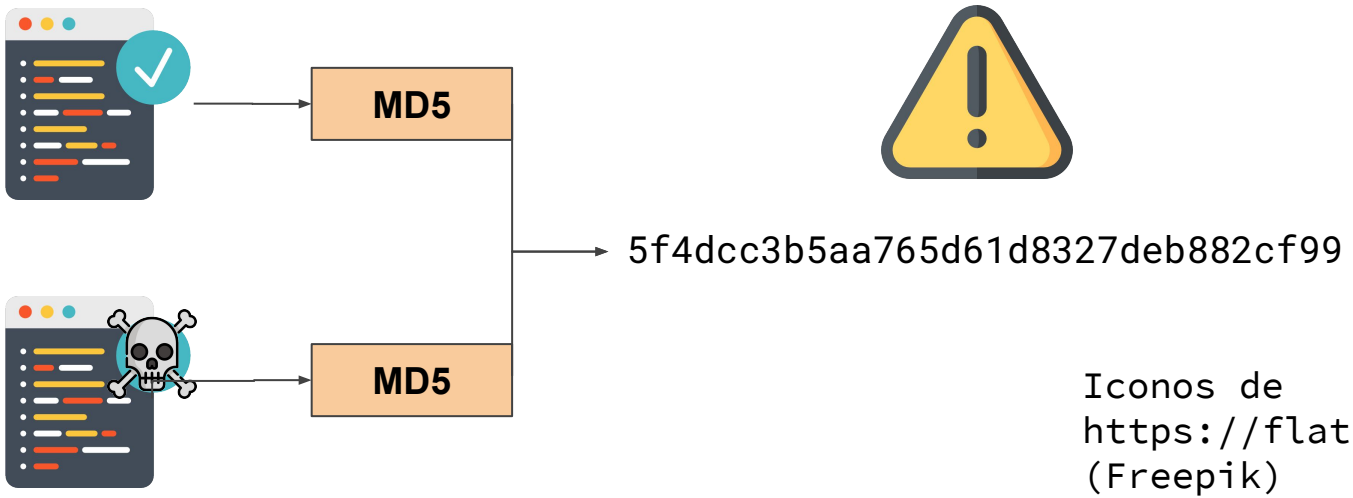
RT de largo 8, con alfabeto de 62 caracteres [A-Za-z0-9], con 1 byte por caracter = 62^8 bytes, lo cual es casi **200 tebibytes***

***Existen optimizaciones que permiten bajar el tamaño de la tabla.**

Otros problemas en seguridad de hashing

Vulnerabilidades en algoritmos

- Colisiones de Hash



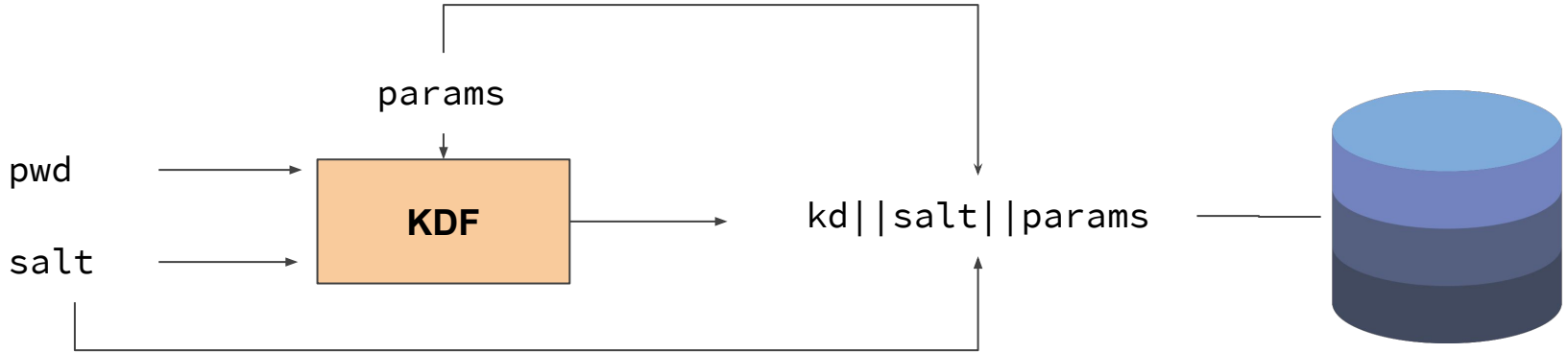
Iconos de
https://flaticon.com
(Freepik)

KDF (Key Derivation Functions)

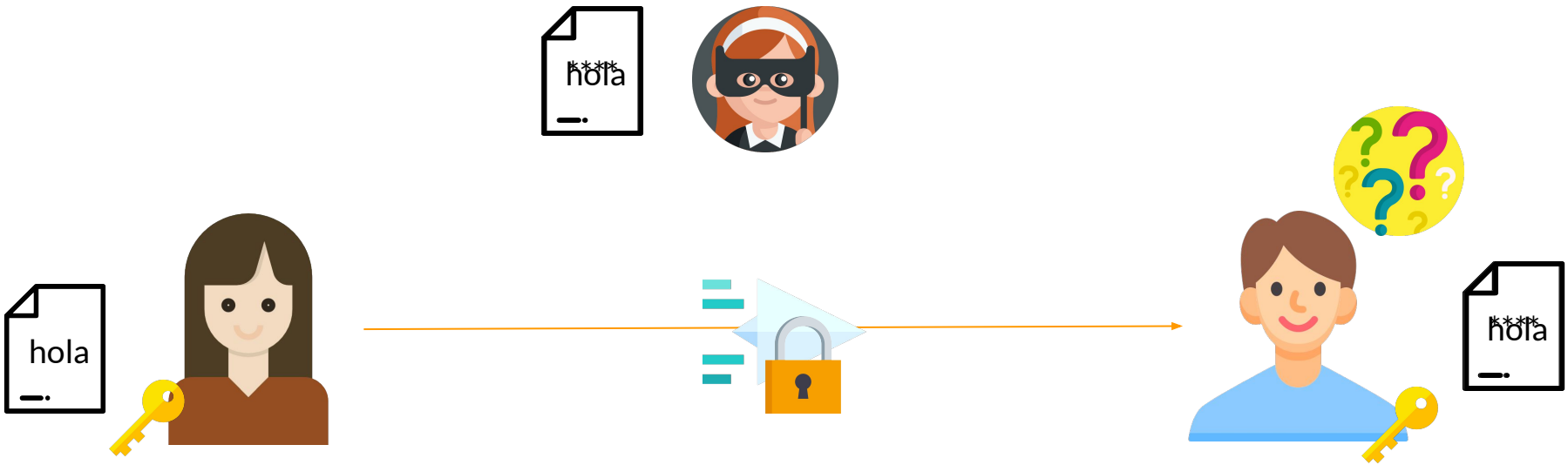
imagen de Base de Datos por smashicons en https://flaticon.com

---

- Contraseñas se "salan" con un valor aleatorio, el cual se combina con la contraseña
  - "hash" producido para dos usuarios concontraseñas iguales no será igual
- Su validación requiere harto poder de cómputo (demora segundos en validar)
  - Mayor uso de RAM o una gran cantidad de iteraciones.



Criptografía Simétrica



Iconos de https://flaticon.com (Freepik)

One Time Pad

- Forma "irrompible" de descifrar un mensaje
- Dado un stream de bits B realmente aleatorio y a disposición de Alicia y Bob, se define cada bit **i** del texto cifrado **C** como **C_i = P_i xor B_i**

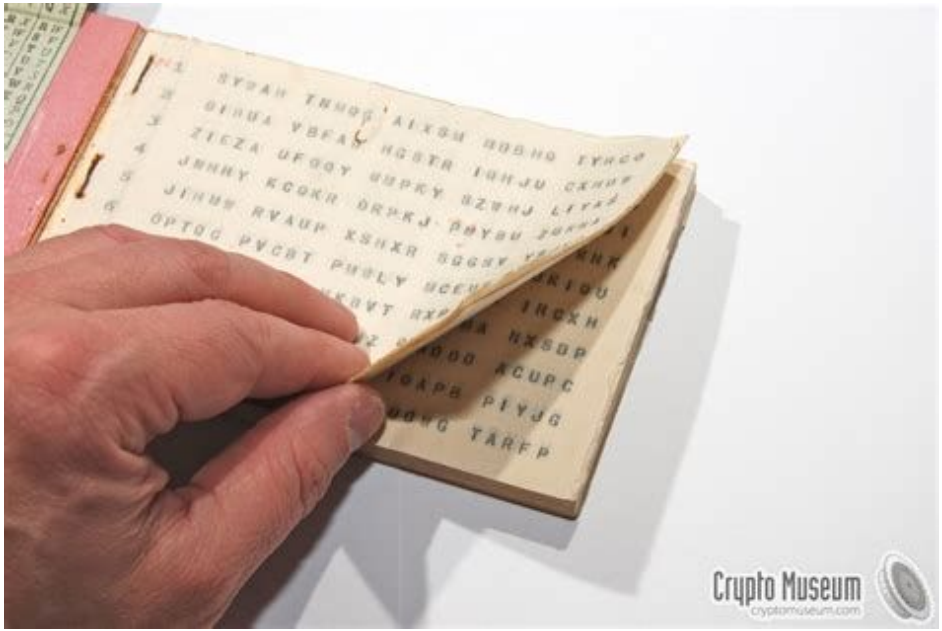
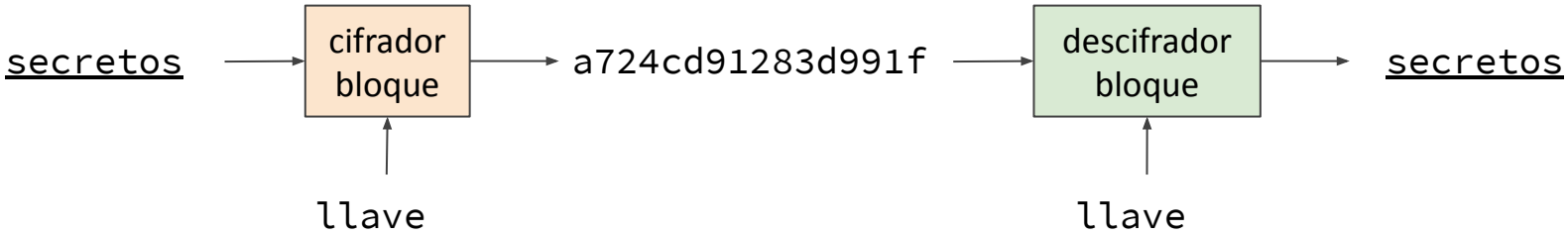


Imagen de cryptomuseum.com

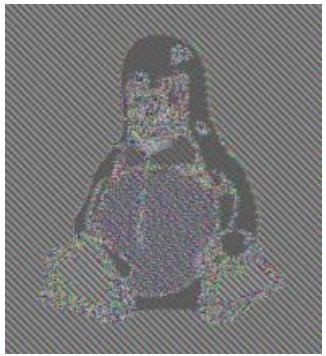
Cifradores de Bloque

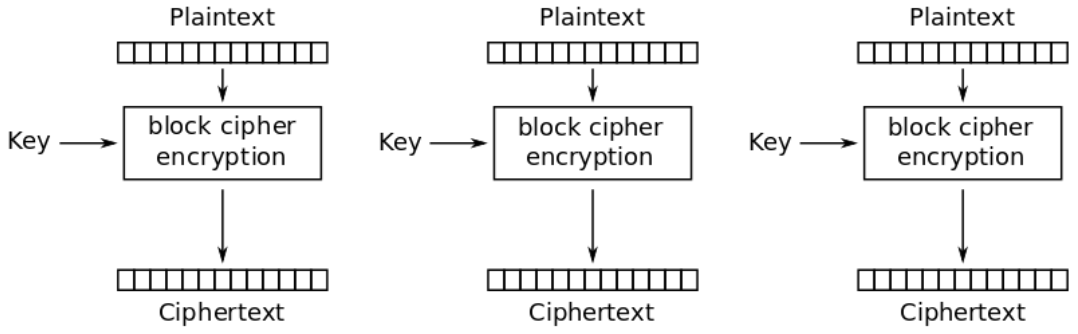
- Texto a cifrar debe tener un tamaño fijo.
  - Si es más chico, se rellena con algún caracter **(Padding)**
- Luego el texto se mete a un "cifrador de bloque", el cual toma de parámetro una **llave secreta.**
  - Todos los bytes del texto plano afectan a todos los bytes del texto cifrado (cambiar una letra cambia muy probablemente todo el cifrado)



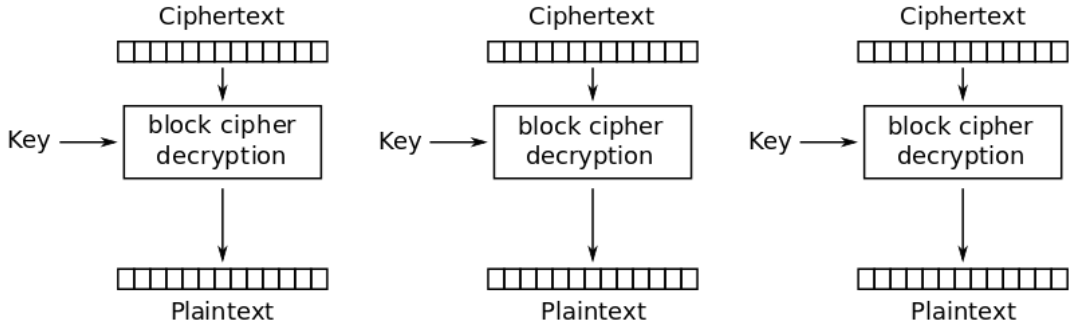
Modos de Cifrado

ECB:





Electronic Codebook (ECB) mode encryption

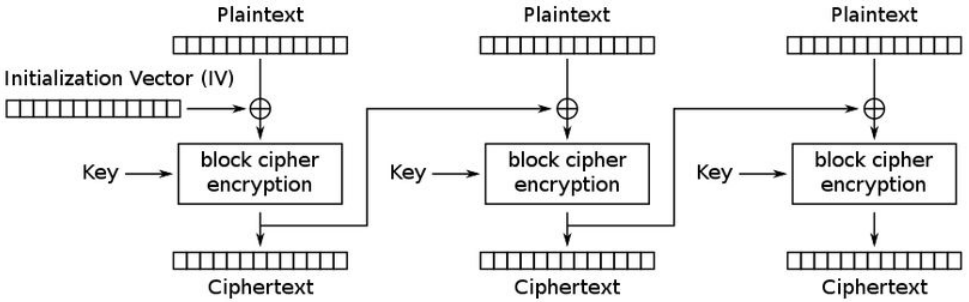


Electronic Codebook (ECB) mode decryption

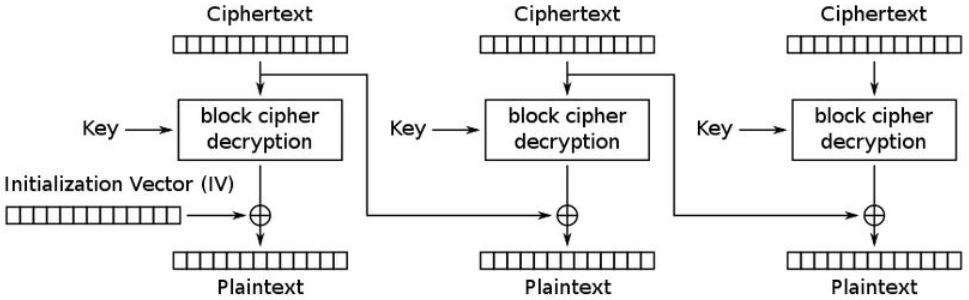
Modos de Cifrado

Block Cipher Chaining (CBC)

IV: Vector de Inicialización (público, aleatorio)



Cipher Block Chaining (CBC) mode encryption

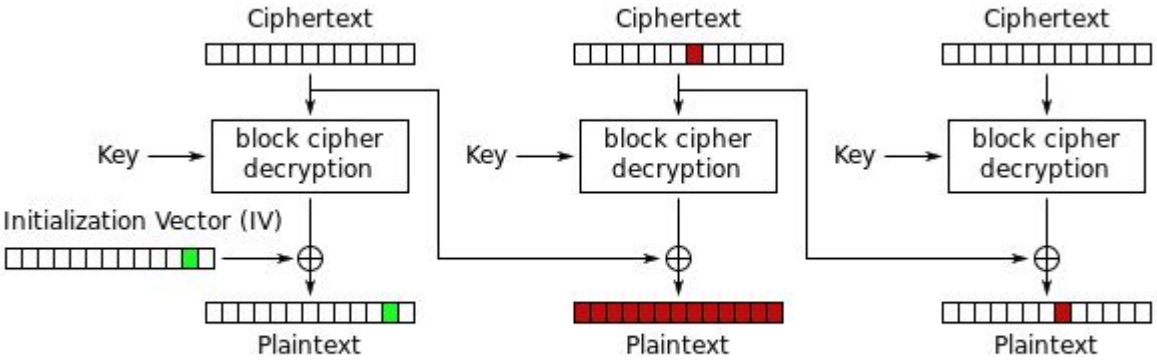


Cipher Block Chaining (CBC) mode decryption

¿Y si repito el IV?

Bit Flipping Attack

https://crypto.stackexchange.com/questions/66085/bit-flipping-attack-on-cbc-mode

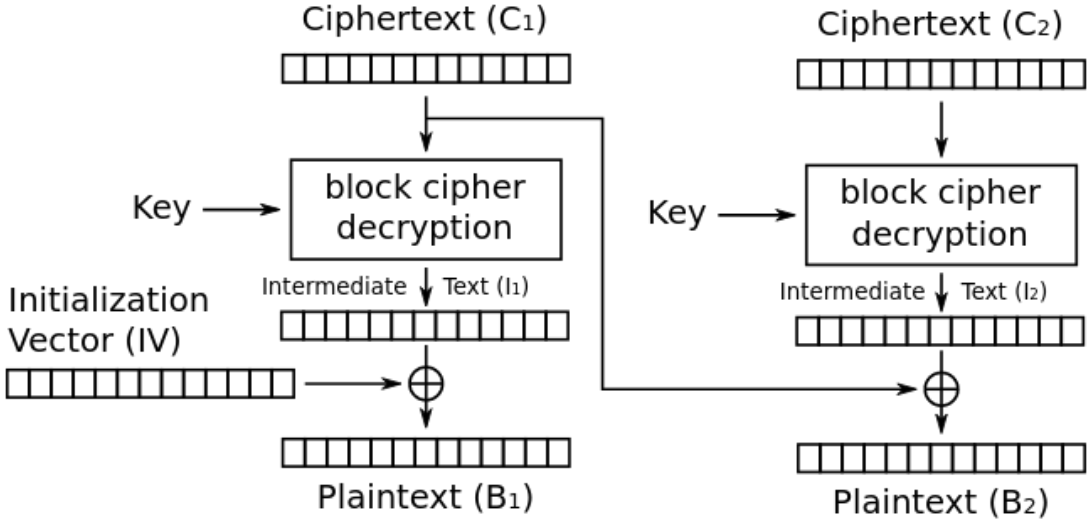


Cipher Block Chaining (CBC) mode decryption

¿Y si filtro información en caso de error?

Padding Oracle Attack

https://users.dcc.uchile.cl/~eriveros/cc5312/anexos/padding-oracle/

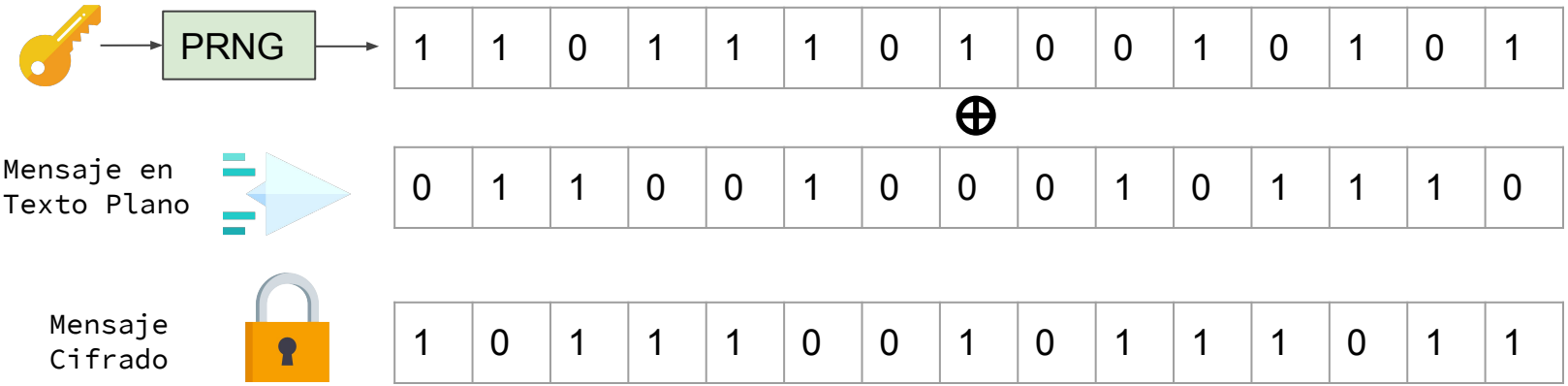


Padding PKCS#7:
Repetir **n** veces el byte **n**, donde **n** es la cantidad de bytes que faltan para completar el último bloque (**n** pertenece a **[1..BlockLen]**).
(Si el mensaje cabe exactamente en **K** bloques, se agrega un bloque extra con **BlockLen** bytes de valor **BlockLen.)**

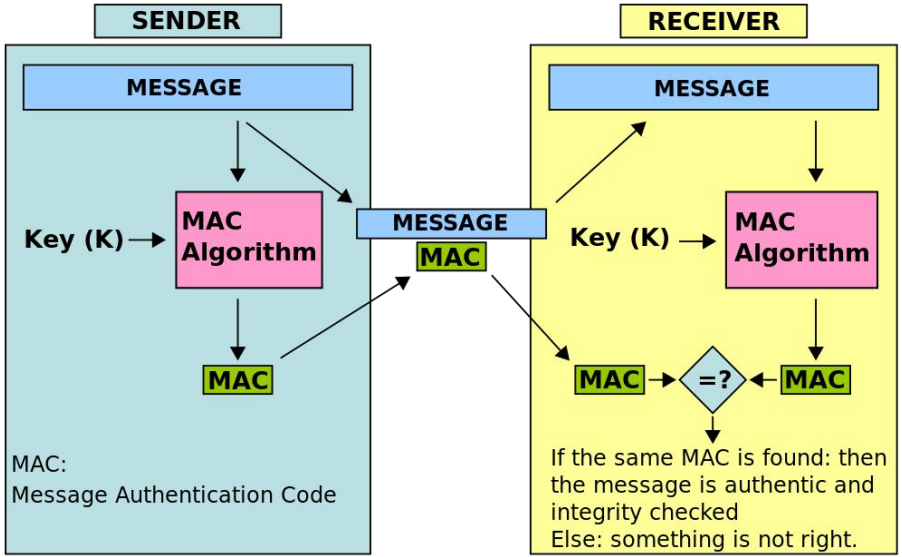
```
hello world!\0x4\0x4\0x4\0x4
```

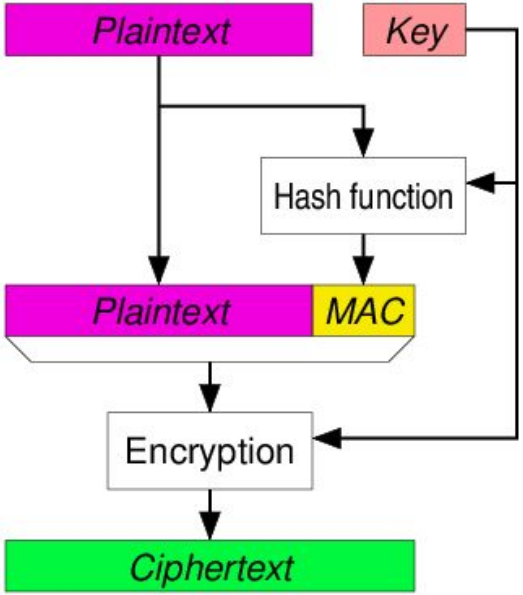
Cifradores de Flujo

- Llave actúa como "semilla" en un generador pseudoaleatorio.
- Luego, cada bit del mensaje se XORea con cada bit del generador pseudoaleatorio.
- **Si logro determinar el estado interno del cifrador, puedo romper el cifrado.**



Autentificación de Mensajes (MAC)





¿En qué debo fijarme en los CTF de Criptografía?

- Malas implementaciones
  - **En especial implementaciones caseras**
- Vulnerabilidades conocidas
  - **Buscar ataques conocidos al algoritmo utilizado**
- Canales laterales
  - **¿Algún comportamiento secundario me revela info útil?**
- Valores calculables por fuerza bruta fácilmente
  - **Parámetros en rangos chicos o que dependen de otros.**