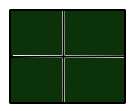
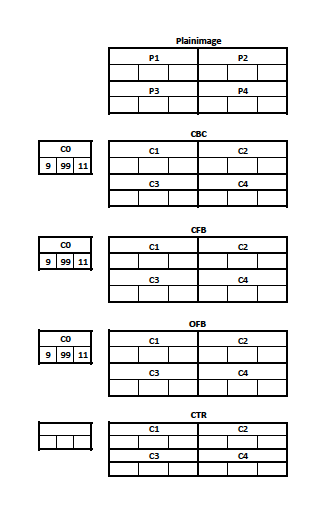
1. Completar los espacios faltantes, colorear con los resultados.

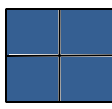


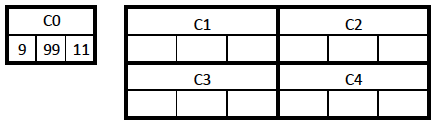
**10 50 9**

**10 50 9**

**10 50 9**

**10 50 9**





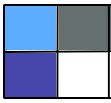
**53 95 146**

**53 95 146**

**53 95 146**

**53 95 146**

ECB

 CBC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C1 | | | C2 | | |
| 93 | 173 | 255 | 101 | 111 | 111 |
| C3 | | | C4 | | |
| 69 | 69 | 199 | 33 | 163 | 199 |

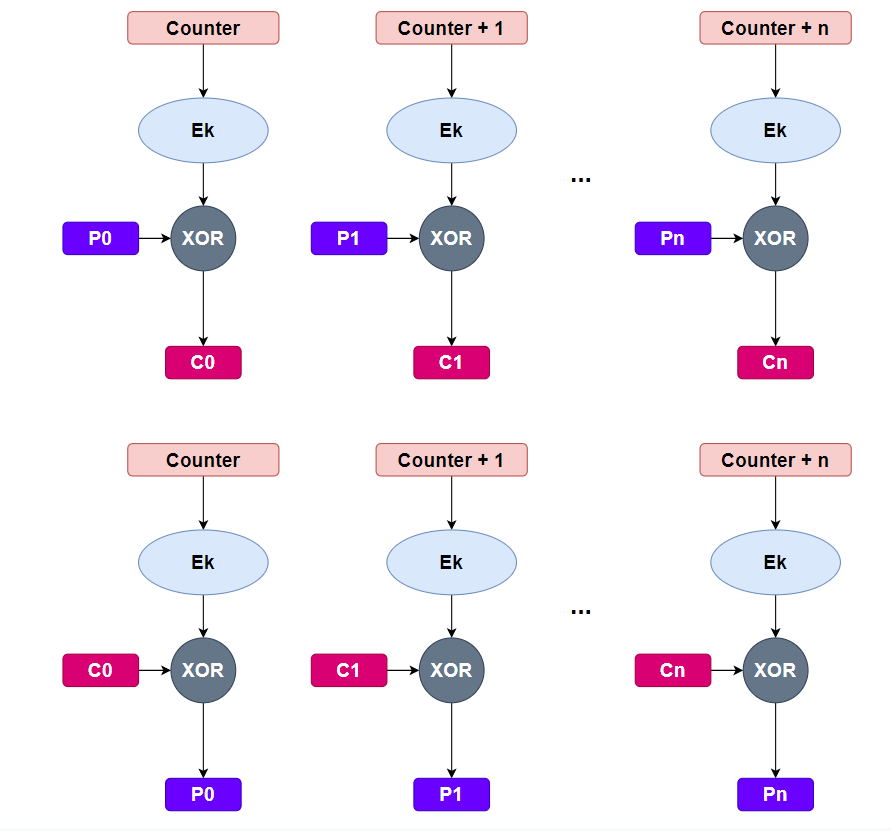
CFB

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C1 | | | C2 | | |
| 4 | 86 | 204 | 42 | 208 | 121 |
| C3 | | | C4 | | |
| 151 | 151 | 47 | 242 | 250 | 206 |

OFB

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C1 | | | C2 | | |
| 4 | 86 | 204 | 31 | 207 | 163 |
| C3 | | | C4 | | |
| 93 | 36 | 116 | 4 | 179 | 120 |

1. Investigar el modo de operación CTR (poner el diagrama de cifrado y descifrado asi como sus funciones) y buscar información para llenar la siguiente tabla



|  |  |  |
| --- | --- | --- |
| Modo de Operación | Ventajas | Desventajas |
| ECB | * Si uno de los bloques se daña los demás no. * El proceso de cifrar o descifrar es sencillo. | * Al ser paralelo, los bloques siguen el mismo patrón * Es fácil de descifrar * Mismo procedimiento de cifrado y descifrado |
| CBC | * El proceso de cifrado es distinto al de descifrado. * El proceso de cifrado o descifrado es más complejo. | * Si se daña un bloque, altera ese y el siguiente. * Gasta muchos recursos. * Como todo cifrador en bloque, el último bloque tiene que ser rellenado. |
| CFB | * La alteración de los bloques en el descifrado no daña a los demás. * Tiene una seguridad de los datos mayor. | * El proceso resulta muy complicado y consume demasiados recursos. |
| OFB | * Debido a su complejidad, tiene alta seguridad de los datos. | * Entre más bloques existan, más complejo es. * El proceso de cifrado y descifrado es el mismo. * Se utiliza sólo C0 para Ek. |
| CTR | * El procesamiento es menos en comparación * La complejidad es media-alta debido al contador | * El proceso de cifrado y descifrado son iguales * El cifrado es paralelo y por lo tanto más débil. |

Nota: Los procedimientos deben realizarse a mano, debes escanear tus notas y juntarlas con este documento o tomar una foto e incluirla como imagen al final de este archivo.

Trabajos sin procedimientos a mano valen 0 puntos.

Al finalizar guarda un sólo archivo como PDF para subirlo a Classroom.

