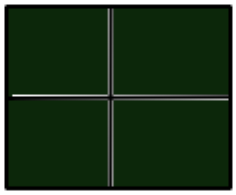
INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre __Sanchez Mendez Edmundo Josue__

# Actividad 8.-Modos de Operación

A) Completar los espacios faltantes, colorear con los resultados.

**Plainimage**

| P1 | | | P2 | | |
|---|---|---|---|---|---|
| 10 | 50 | 9 | 10 | 50 | 9 |
| **P3** | | | **P4** | | |
| 10 | 50 | 9 | 10 | 50 | 9 |

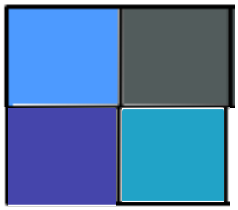


ECB

| C1 | | | C2 | | |
|---|---|---|---|---|---|
| 53 | 95 | 146 | 53 | 95 | 146 |
| C3 | | | C4 | | |
| 53 | 95 | 146 | 53 | 95 | 146 |

CBC

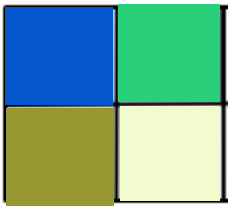
| C1 | | | C2 | | |
|---|---|---|---|---|---|
| 93 | 173 | 255 | 101 | 111 | 111 |
| C3 | | | C4 | | |
| 69 | 69 | 171 | 33 | 163 | 199 |



Nota: CBC calculado en la actividad anterior.

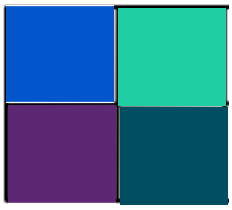
CFB

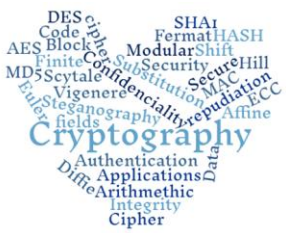
| C1 | | | C2 | | |
|---|---|---|---|---|---|
| 4 | 86 | 204 | 42 | 208 | 121 |
| C3 | | | C4 | | |
| 151 | 151 | 47 | 242 | 250 | 206 |



OFB

| C1 | | | C2 | | |
|---|---|---|---|---|---|
| 4 | 86 | 204 | 31 | 207 | 163 |
| C3 | | | C4 | | |
| 93 | 39 | 116 | 0 | 78 | 98 |






M. en C. Nidia A. Cortez Duarte

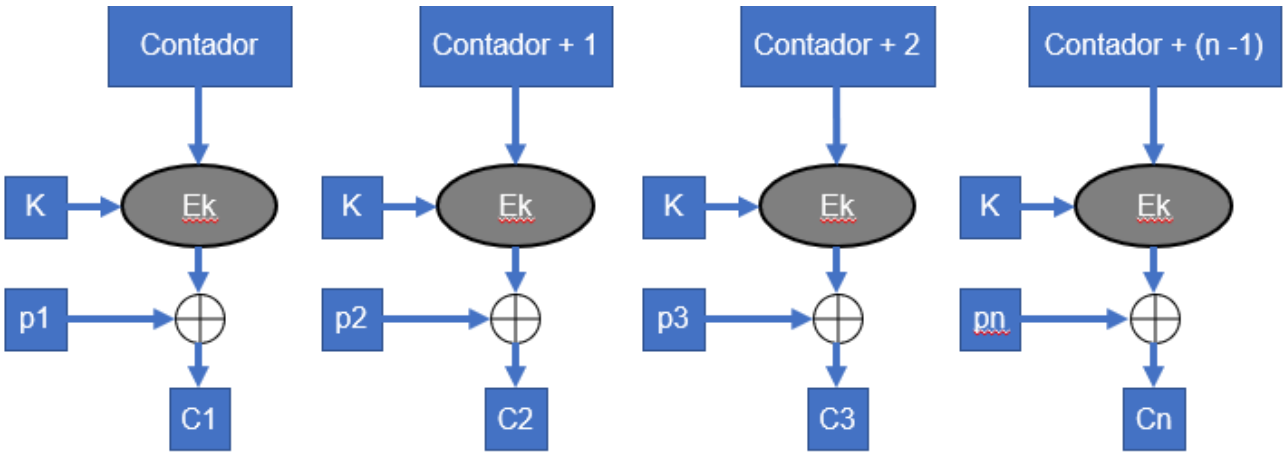
INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre __Sanchez Mendez Edmundo Josue__

# Actividad 8.-Modos de Operación

B) 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 CTR.

Diagrama de cifrado:




Formula de cifrado:

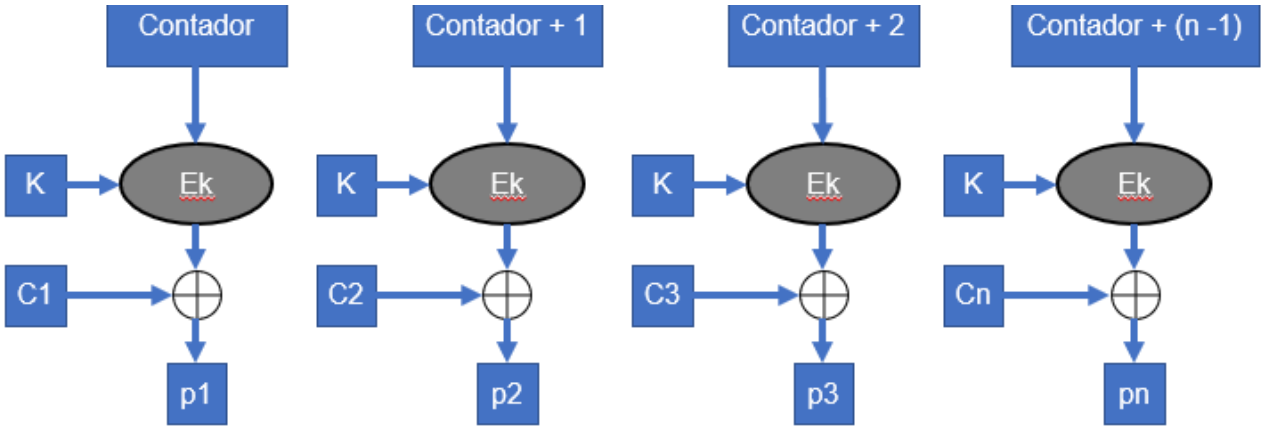
$$C1 = Ek(Contador, K) \text{ XOR } P1$$

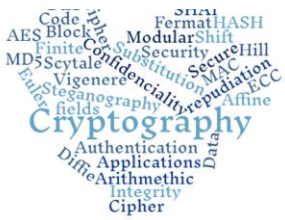
$$C2 = Ek(Contador + 1, K) \text{ XOR } P2$$

$$C3 = Ek(Contador + 2, K) \text{ XOR } P3$$

$$\mathbf{Cn = Ek(Contador + (n - 1), K) \text{ XOR } Pn}$$

Diagrama de cifrado:




M. en C. Nidia A. Cortez Duarte

# Actividad 8.-Modos de Operación

Formula de decifrado:

$$P1 = Ek(Contador, K) \text{ XOR } C1$$

$$P2 = Ek(Contador + 1, K) \text{ XOR } C2$$

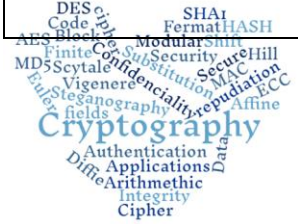
$$P3 = Ek(Contador + 2, K) \text{ XOR } C3$$

$$\mathbf{Pn = Ek(Contador + (n - 1), K) \text{ XOR } Cn}$$

Notas:

- **K** nos representa una llave
- **Contador** nos representa un "nonce", un valor numérico arbitrario que será usado solo una vez en una comunicación.

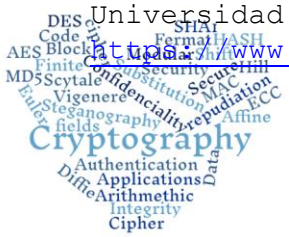
| Modo de Operación | Ventajas | Desventajas |
|---|---|---|
| ECB | Es bastante simple de ser implementado.<br>Si llegase a ver una pérdida de bloques esta no afectara a otros bloques disponibles. Esta ventaja es relevante en el caso de que los bloques se envíen a través de una red como paquetes. Esta resistencia es posible por el hecho de que ningún bloque Ci no depende de ninguno de sus bloques adyacentes. | Debido al tipo de algoritmo de cifrado nos genera un problema y es que si tenemos bloques idénticos tendrán los mismos valores de cifrado en el modo ECB, lo que puede revelar los patrones que tienen los bloques- |
| CBC | Si tenemos bloques idénticos estos no tendrán el mismo cifrado. Esto debido a que el vector de inicialización agrega un factor aleatorio a cada bloque. | No tiene tolerancia a las pérdidas de bloque, esto debido a la dependencia de los bloques, es decir, si perdemos Cj entonces los bloques posteriores no podrán ser cifrados, sin embargo, en el descifrado si perdemos Cj entonces solo no podríamos descifrar Cj+1, pero los posteriores sí.<br>Poca eficiencia en el uso del software debido a la dependencia entre C1 y Cj |
| CFB | Dado que no utiliza un algoritmo de descifrado, | El cifrado no puede tolerar pérdidas de bloques, ni se pueden |



| | | |
|---|---|---|
| | generalmente es más rápido. De igual manera, para bloques idénticos se tendrá diferente cifrado, lo que significa que no revela ningún patrón que pueda existir. | cifrar varios bloques en paralelo. Sin embargo, el descifrado es tolerante a pérdidas y se puede paralelizar. |
| OFB | Dado que los bloques son independientes tanto el cifrado como el descifrado de bloques se pueden realizar en paralelo una vez que se han generado nuestros On. La falta de interdependencia también significa tolerancia a la pérdida en bloques. | Podría llegar a ocurrir que nuestro On empiece a tener el mismo valor, provocando así que nuestro mensaje comenzará a cifrarse con los mismos datos que antes. |
| CTR | Eficiencia en el uso del software ya que elimina dependencias entre Cj-1 y Cj.<br>Eficiencia en el uso del hardware ya que es paralelizable.<br>Nos permite hacer uso del preprocesamiento para el cifrado, ya que en la parte **Ek(Contador + (n – 1), K)** no necesitamos conocer nuestro Pn, así podemos incrementar la velocidad.<br>Al ser independiente podemos hacer el cifrado en un estilo aleatorio ya que tenemos libre acceso a cualquier Pn.<br>No necesitamos como tal una funcion de descifrado o Dk.<br>Mensajes de tamaño arbitrario. | No proporciona integridad al mensaje, aunque no es un propósito del cifrado.<br>Posee propagación de errores ya que, si hay algún cambio en un bit de algún bloque del texto cifrado, entonces después del descifrado el error esta localizado en su parte homologa, pero del texto descifrado.<br>Sensible a errores de usos ya que es de suma importante de que el valor del contador no sea reusado ya que así perderíamos la seguridad. |

Referencias:


- Lipmaa, H., Rogaway, P. and Wagner, D., 2000. CTR-Mode Encryption. [ebook] Universidad de California en Davis, pp.1-3. Available at: http://www.cs.ucdavis.edu/~rogaway/papers/ctr.pdf Accessed 13 April 2021.

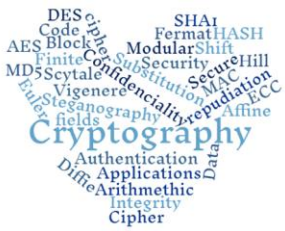
# Actividad 8.-Modos de Operación


- Mustafeez, A., 2020. What is ECB?. [online] Educative: Interactive Courses for Software Developers. Available at: https://www.educative.io/edpresso/what-is-ecb Accessed 13 April 2021.
- Mustafeez, A., 2020. What is CBC?. [online] Educative: Interactive Courses for Software Developers. Available at: https://www.educative.io/edpresso/what-is-cbc Accessed 13 April 2021.
- Mustafeez, A., 2020. What is CFB?. [online] Educative: Interactive Courses for Software Developers. Available at: https://www.educative.io/edpresso/what-is-cfb Accessed 13 April 2021.
- Mustafeez, A., 2020. What is OFB?. [online] Educative: Interactive Courses for Software Developers. Available at: https://www.educative.io/edpresso/what-is-ofb Accessed 14 April 2021.


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.

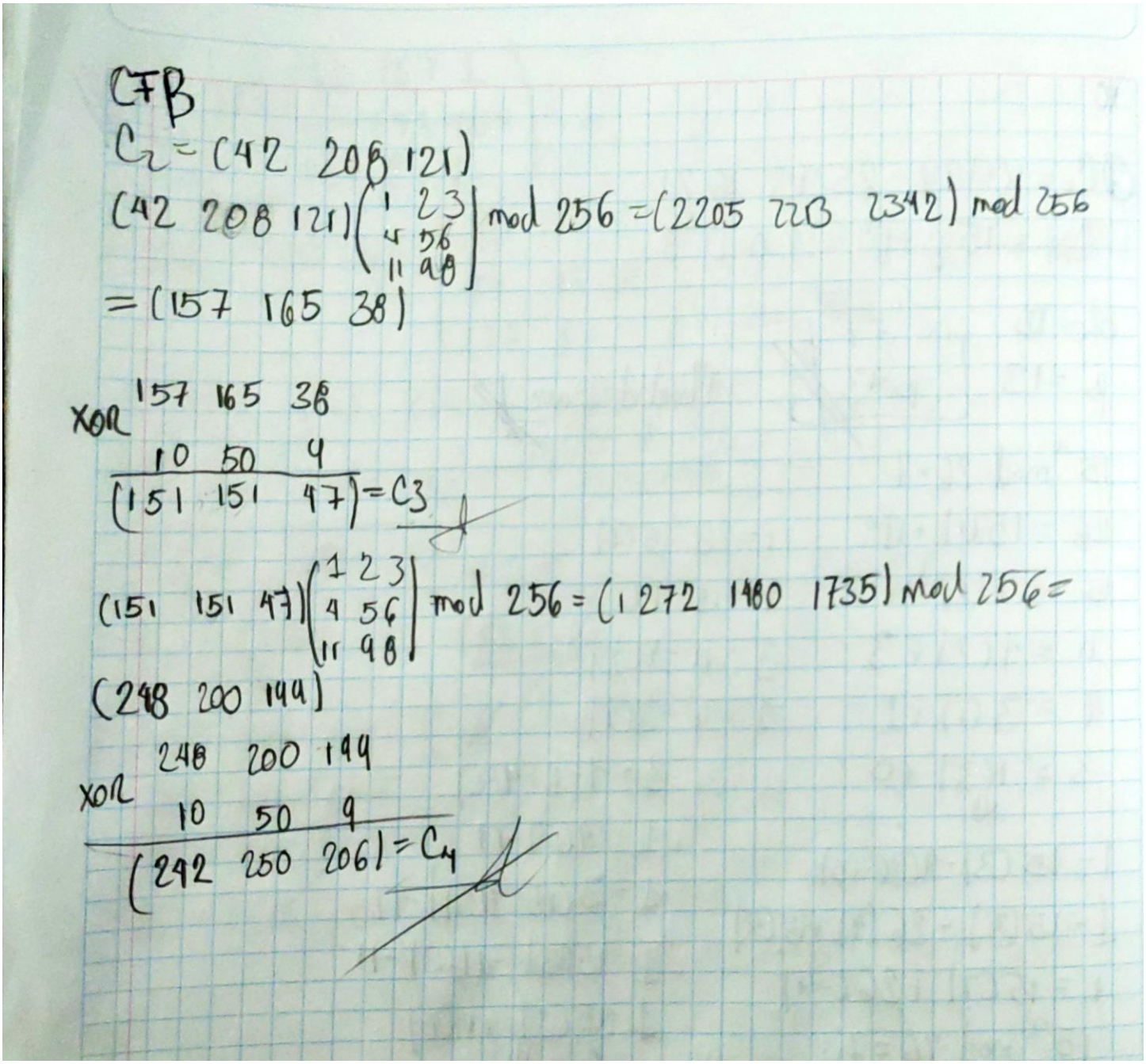
Trabajos sin procedimientos a mano valen 0 puntos.

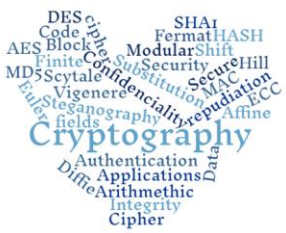
Al finalizar guarda un sólo archivo como PDF para subirlo a Classroom.




M. en C. Nidia A. Cortez Duarte

# Actividad 8.-Modos de Operación



# Actividad 8.-Modos de Operación

OFB

$O_1 = E_K(CO) = (4\ 94\ 11)\begin{pmatrix}1&2&3\\4&5&6\\11&4&8\end{pmatrix} \bmod 256 = (526\ 812\ 709) \bmod 256 = (14\ 100\ 197)$

$O_2 = E_K(E_K(CO)) = (14\ 100\ 197)\begin{pmatrix}1&2&3\\4&5&6\\11&4&8\end{pmatrix} \bmod 256 = (2581\ 2301\ 2210) = (21\ 253\ 170)$

$O_3 = E_K(E_K(E_K(CO))) = (21\ 253\ 170)\begin{pmatrix}1&2&3\\4&5&6\\11&9&8\end{pmatrix} \bmod 256 = (2903\ 2037\ 2941) \bmod 256$

$O_3 = (87\ 21\ 125)$

$O_4 = E_K(O_3) = (87\ 21\ 125)\begin{pmatrix}1&2&3\\4&5&6\\11&9&8\end{pmatrix} \bmod 256 = (1546\ 1404\ 1387) \bmod 256$

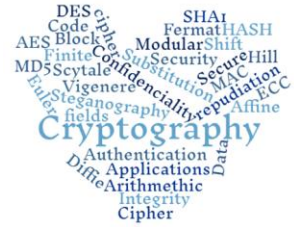
$O_4 = (10\ 124\ 107)$

$C_3$:

87 21 125
XOR
10 50 9
$(93\ 39\ 116) = C_3$

$C_4$: 10

10 124 107
XOR
10 50 9
$(0\ 78\ 98) = C_4$




M. en C. Nidia A. Cortez Duarte