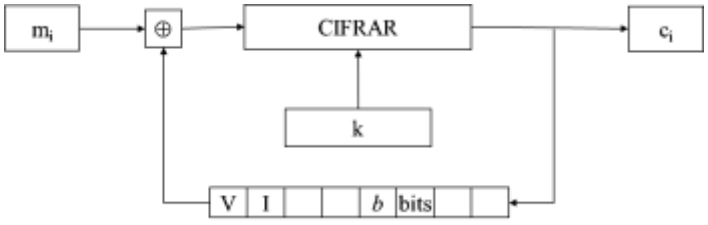
Ejercicios:
Cifrado en bloque con clave secreta

4.1) Supongamos que las claves que utilizamos para cifrar con AES128 están constituidas por sólo dieciséis letras mayúsculas del alfabeto castellano en código ASCII.
a) ¿Cuántas horas tardaremos en obtener la clave utilizada por búsqueda exhaustiva si suponemos que habrá que probar aproximadamente la mitad de todas las claves posibles y que el ordenador que utilizamos es capaz de comprobar la bondad de una clave en una millonésima de segundo?
b) ¿Y si la clave puede tener tanto letras mayúsculas como minúsculas?
c) ¿Y si además de letras puede contener números?

4.2) En los algoritmos de cifrado en bloque, por lo general, se utiliza un algoritmo de expansión de clave. Explica, brevemente, cual es la finalidad de esta expansión de clave.

4.3) Explica, brevemente, las características principales de AES: tipo de cifrado, tamaños de bloque y clave. Para un cifrador en bloque de *b* bits de tamaño de bloque, en el modo de cifrado CBC, para empezar se genera un vector inicial VI aleatorio de *b* bits con el que se carga el registro.
Cada bloque m_i de *b* bits del texto en claro se cifra con la misma clave k y el bloque de salida c_i se realimenta hacia la entrada mediante el registro de *b* bits.
Para cifrar se aplica la recurrencia
$c_1 = E_k(m_1 \oplus VI)$; $c_i = E_k(m_i \oplus c_{i-1})$, para i = 2,3,···,n;
donde n es el número de bloques a cifrar.



Explica, brevemente, cómo se descifra escribiendo las ecuaciones de recurrencia.

4.4) ¿En el algoritmo AES, cuál es el resultado de aplicar la función *DesplazarFila (ShiftRows)* a la matriz de estado

C2	**CB**	**C9**	**50**
89	**02**	**F4**	**69**
6E	**63**	**64**	**26**
27	**23**	**9A**	**FB**

4.5) Explica, brevemente, las diferencias fundamentales entre cifradores en flujo y cifradores en bloque con clave secreta. Indica en qué tipo de tratamiento de la información los utilizarías y qué algoritmos.

4.6) Supongamos que las claves que utilizamos para cifrar con el DES están constituidas por sólo siete letras mayúsculas del alfabeto castellano en código ASCII.

a) ¿Cuántas horas tardaremos en obtener la clave utilizada por búsqueda exhaustiva si suponemos que habrá que probar aproximadamente la mitad de todas las claves posibles y que el ordenador que utilizamos es capaz de comprobar la bondad de una clave en una millonésima de segundo?

b) ¿Y si la clave puede tener tanto letras mayúsculas como minúsculas?

c) ¿Y si además de letras puede contener números?