GUÍA 2: CRIPTOGRAFÍA SIMÉTRICA

Ejercicio 1:

Sea un Criptosistema con las siguientes características:

Espacio de Mensajes: $\mathcal{M}=\{a,b\}$

$$P[M=a]=0{,}25; P[M=b]=0{,}75$$

Espacio de Claves: $\mathcal{K}=\{k1,k2,k3\}$, donde **Gen** genera una clave según las siguientes probabilidades:

$$P[K=k1]=0{,}5; P[K=k2]=P[K=k3]=0{,}25$$

El algoritmo **Enc** está definido por la tabla:

	a	**b**
k1	1	2
k2	2	3
k3	3	4

Por lo que el Espacio de Cifrados, $\mathbf{C}=\{Enc_k(x)/\ x\in M \wedge k\in K\}$ ***resulta ser {1,2,3,4}***

Se pide:

a) Hallar la distribución de probabilidades de **C.**(espacio de cifrados)
b) Demostrar de las cuatro maneras vistas en la teoría, que el sistema no tiene secreto perfecto.

Ejercicio 2:

Probar o encontrar un contraejemplo de la siguiente afirmación:

En un criptosistema que posee la propiedad de ***secreto perfecto*** *se cumple que para toda distribución sobre el espacio de mensajes* M *, para todo* $m,m'\in M$ *y para todo* $c\in C$ *,*

$$\Pr[M=m\,|\,C=c]=\Pr[M=m'|\,C=c]$$

Ejercicio 3:

Para los siguientes ejercicios, considerar el alfabeto inglés (26 símbolos)

a) Demostrar que si se encripta un solo símbolo, entonces el cifrado de rotación tiene secreto perfecto.

b) ¿Cuál es el mayor tamaño que puede tener el espacio de textos planos M **como para que el cifrado de sustitución monoalfabética posea secreto perfecto?**

c) Mostrar cómo usar el cifrado de Vigenére para encriptar una palabra de longitud t y tener secreto perfecto.

Ejercicio 4:

Dado un criptosistema $\pi=(Gen,Enc,Dec)$ **de Vigenere, sobre un espacio de mensajes** $M=\Sigma^3$ **, donde** Σ **es el alfabeto inglés. El algoritmo** Gen **elige primero el período t de la clave en forma aleatoria y uniforme, dentro del rango** $t\in\{1,2,3\}$ **. Luego, elige la clave k dentro de** Σ^* **, tal que** $|k|=t$ **.**

a) Mostrar un ejemplo de cómo el criptosistema cifra un mensaje.

b) Calcular la probabilidad de éxito del experimento $\mathrm{PrivK}^{eav}_{A,\pi}$ **para un adversario que hace lo siguiente:**

- A emite primero los mensajes $\{m_0=aab, m_1=abb\}$
- Al recibir el cifrado c A emite '0' si el primer símbolo de c es igual al segundo, y emite '1' en caso contrario

c) De acuerdo a lo calculado en el punto (b) ¿tiene secreto perfecto?

Ejercicio 5:

Demostrar que los siguientes cifrados son vulnerables a un ataque de **texto plano elegido (chosen-plaintext attack).**

- **cifrado de sustitución monoalfabética**

- cifrado de Vigenère

Ejercicio 6:

Con el modo ECB, si hay un error en un bloque del texto cifrado transmitido, solamente afecta al bloque de texto claro correspondiente.

a) En el modo CBC (ver figura) un error de un bit en P1, a través de cuántos bloques de texto cifrado se propaga?

b) En el modo CBC, un error de un bit en C1, a través de cuántos bloques de texto descrifrado se propaga?

c) Si se produce un error de un bit en la transmisión de un carácter del texto cifrado en modo CFB de ocho bits, ¿hasta dónde se propaga el error?

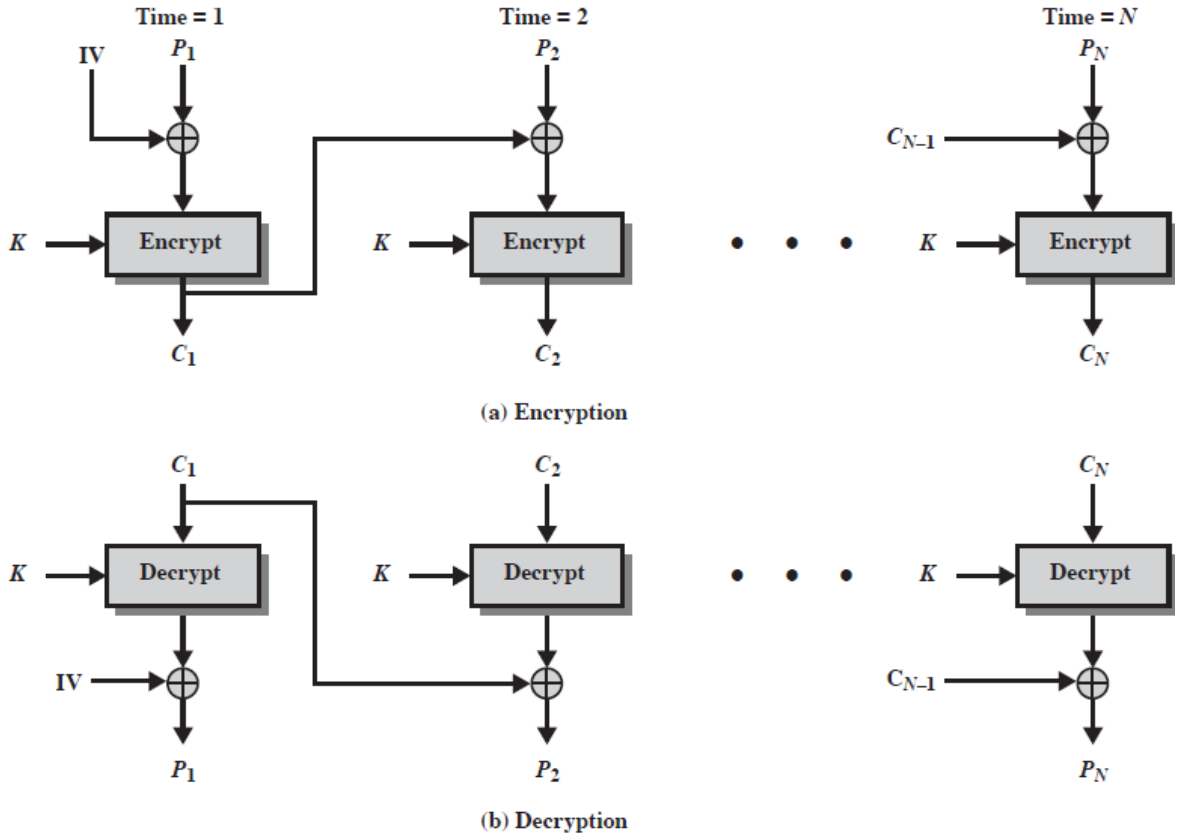

Figure 2.9 Cipher Block Chaining (CBC) Mode

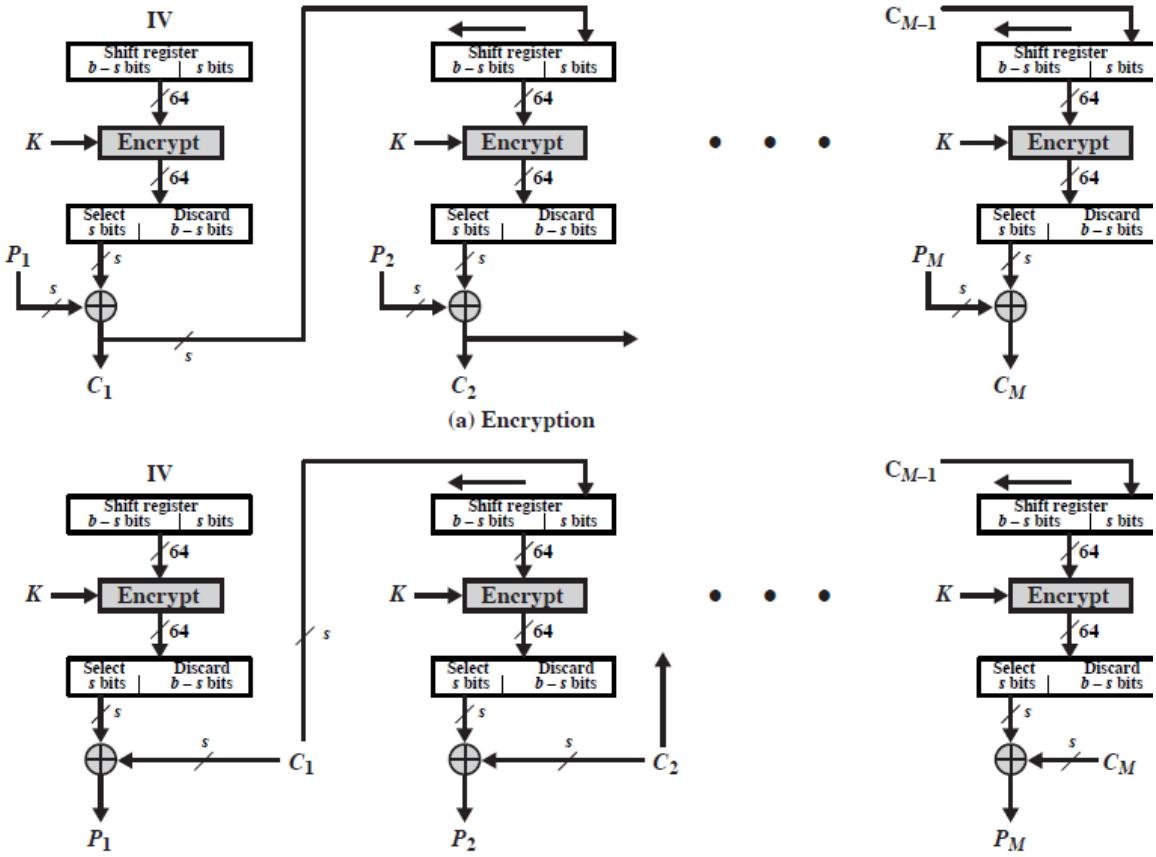

Figure 2.10 *s*-bit Cipher Feedback (CFB) Mode

Ejercicio 7:

Considerando el siguiente cifrado de Bloque:

$$E(K,M) = (M * K)(\mathrm{mod}\,32)$$

a) ¿cuál es el tamaño del bloque? ¿cuál es el espacio efectivo de la clave?
b) Encriptar el mensaje 24 17 26 25 12 usando modo CBC con vector de inicialización IV = 19 y K = 7.
c) Desencriptar en modo CBC.

Ejercicio 8:

Una clave débil para DES es una clave K tal que $E_k(E_k(x)) = x, \forall x$

Analizar por qué una clave formada por todos sus bits en 0, o todos sus bits en 1, es una clave débil de DES. ¿Cuáles serían otras dos claves débiles?