GUÍA 2: CRIPTOGRAFÍA SIMÉTRICA - SOLUCIONES

Ejercicio 1:

Corresponde al **ejemplo 2** del apunte "Probabilidad y Criptografía".

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

El **experimento** $\mathrm{PrivK}_{A,\pi}^{eav}$ experimento podría hacerse de la siguiente manera:

1) El adversario emite $m_0 = a$ y $m_1 = b$.
2) Al recibir un cifrado igual a "1", elige b'=0. Caso contrario, elige b' = 1.

b = 0 (m = 'a')	Si cifra con k =	El cifrado es c =	El adversario elige b' =	
	k1	**1**	0 (porque vio "**1**")	¡ACIERTA!
	k2	**2**	1 (porque **no** vio "**1**")	no acierta
	k3	**3**	1 (porque **no** vio "**1**")	no acierta

Es decir, que *A* elige correctamente b'=0 cuando b = 0, sólo en el 50% de los casos (Pr(k=k1) = 0,5)

b = 1 (m = 'b')	Si cifra con k =	El cifrado es c =	El adversario elige b' =	
	k1	**2**	1 (porque **no** vio "**1**")	¡ACIERTA!
	k2	**3**	1 (porque **no** vio "**1**")	¡ACIERTA!
	k3	**4**	1 (porque **no** vio "**1**")	¡ACIERTA!

Es decir, que *A* elige correctamente b'=1 cuando b = 1, en todos los casos.

Calculamos la probabilidad de éxito del experimento:

$$\Pr\left[\mathrm{PrivK}_{\mathrm{A},\pi}^{\mathrm{CPA}}(n) = 1\right] = \left[\Pr(b' = 0 \wedge b = 0)\right] + \left[\Pr(b' = 1 \wedge b = 1)\right]$$

$$\Rightarrow \Pr\left[\mathrm{PrivK}_{\mathrm{A},\pi}^{\mathrm{CPA}}(n) = 1\right] = \left[\Pr(b = 0)\cdot\Pr(b' = 0 \mid b = 0)\right] + \left[\Pr(b = 1)\cdot\Pr(b' = 1 \mid b = 1)\right]$$

$$\Rightarrow \Pr\left[\mathrm{PrivK}_{\mathrm{A},\pi}^{\mathrm{CPA}}(n) = 1\right] = \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot 1$$

$$\Rightarrow \Pr\left[\mathrm{PrivK}_{\mathrm{A},\pi}^{\mathrm{CPA}}(n) = 1\right] = 0{,}75$$

Como el experimento tiene éxito con probabilidad mayor que 0,5, el esquema no es seguro.

Ejercicio 2:

Teniendo en cuenta: ***[Katz Cap. 2, definición 2.1]***

Un criptosistema que posee la propiedad de secreto perfecto cumple que para toda distribución sobre el espacio de mensajes M, para todo $m \in M$ y para todo $c \in C$, $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Si $\Pr[M = m]$ fuera igual a $\Pr[M = m']$, entonces se cumpliría lo que dice el enunciado del ejercicio.

Sin embargo, no necesariamente esas probabilidades son iguales.

Por lo tanto, no se cumple la afirmación.

Ejemplo:

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

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

Espacio de Claves: $\mathcal{K}=\{k1,k2\}$

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

Espacio de Cifrados: C=$\{Enc_k(x) / x \in M \wedge k \in K\}$=$\{c,d\}$

Donde Enc está dado por la tabla:

	a	**b**
k1	c	d
k2	d	c

$P[C=c]=P[K=k1]\cdot P[M=a]+P[K=k2]\cdot P[M=b]$=0,5.0,25+0,5.0,75 = 0,5
$P[C=d]=P[K=k1]\cdot P[M=b]+P[K=k2]\cdot P[M=a]$=0,5.0,75+0,5.0,25 = 0,5

$P[C=c \mid M=a]=P[K=k1]=0{,}5$
$P[C=c \mid M=b]=P[K=k2]=0{,}5$
$P[C=d \mid M=a]=P[K=k2]=0{,}5$
$P[C=d \mid M=b]=P[K=k1]=0{,}5$

Se observa que se cumple $P[C=y \mid M=x]=P[C=y]\ \forall y \forall x$, por lo que **hay secreto perfecto**

A su vez,
$P[M=a \mid C=c]=(P[M=a]P[K=k1])/P[C=c]=(0{,}25\cdot 0{,}5)/0{,}5=0{,}25$
$P[M=a \mid C=d]=(P[M=a]P[K=k2])/P[C=d]=(0{,}25\cdot 0{,}5)/0{,}5=0{,}25$
$P[M=b \mid C=c]=(P[M=b]P[K=k2])/P[C=c]=0{,}75$
$P[M=b \mid C=d]=(P[M=b]P[K=k1])/P[C=d]=0{,}75$

Se observa que se cumple $P[M=x \mid C=y]=P[M=x]\ \forall y \forall x$, por lo que **hay secreto perfecto.**

Pero puede verse que $P[M=a \mid C=y]$ no es igual a $P[M=b \mid C=y]$

Ejercicio 3:

a. La demostración es similar a la que ofrece Katz para el cifrado de One Time Pad:

$\Pr[C=c \mid M=m]=\Pr[M+K\equiv c(26) \mid M=m]$

$=\Pr[m+K\equiv c(26)]=\Pr[K\equiv(c-m)(26)]=\dfrac{1}{26}$ (porque la clave se elige en forma aleatoria y uniforme en el conjunto $\{0,1,\ldots 25\}$

Como esto se da para todo m, resulta que:

$$\Pr[C=c \mid M=m_0]=\frac{1}{26}=\Pr[C=c \mid M=m_1]$$

b. Una condición necesaria es que el espacio de claves sea de tamaño mayor o igual al espacio de mensajes, ($\#K \geq \#M$)

En este caso el espacio de claves es de $26!$, así que el espacio de mensajes debe ser, como máximo de $\#M \leq 26!$

Pero **no es suficiente** exigir eso para lograr el secreto perfecto.

<u>Mensajes de una sola letra:</u>

Sea el caso de $M=\{a,b,c,d,\ldots.z\} \Rightarrow \#M=26 \Rightarrow P[M=m]=\dfrac{1}{26}$

Como el espacio de claves es el conjunto de todas las permutaciones del alfabeto, resulta que:

$\#K=26! \Rightarrow P[K=k]=\dfrac{1}{26!}$

El algoritmo de encripción está dado por la aplicación de dichas permutaciones:

	a	**b**	**c**	**...**	**z**

K_1	a	b	c	…	z
K_2	a	c	b	…	z
K_3	a	d	c	…	z
…					
$K_{26!}$	z	a	b	…	y

Se observa que $Enc_{k1}('a') = Enc_{k2}('a') = ...Enc_{k25!}('a') = 'a'$.

De manera similar, habrá 25! Encripciones de un mensaje que resultan en el mismo cifrado.

Es decir $Enc_{ki}(x) = y$ para 25! Claves ki distintas.

Entonces,

$$P[C = y] = \sum_{ki:Enc_{ki}('a')=y} P[M = 'a'] \cdot P[K = ki] + \sum_{ki:Enc_{ki}('b')=y} P[M = 'b'] \cdot P[K = ki] + \ldots + \sum_{ki:Enc_{ki}('z')=y} P[M = 'z'] \cdot P[K = ki]$$

$$P[C = y] = \frac{1}{26} \cdot \frac{1}{26!} \cdot 25! + \frac{1}{26} \cdot \frac{1}{26!} \cdot 25! + \ldots + \frac{1}{26} \cdot \frac{1}{26!} \cdot 25!$$

$$P[C = y] = \frac{1}{26} \cdot \frac{1}{26!} \cdot 25! \cdot 26$$

$$P[C = y] = \frac{1}{26}$$

Por otro lado,

$$P[M = x \mid C = y] = \left(P[M = x] \cdot \sum_{ki:Dec_{ki}(y)=x} P[K = ki] \right) / P[C = y]$$

$$P[M = x \mid C = y] = \left(\frac{1}{26} \cdot \frac{1}{26!} \cdot 25! \right) / \left(\frac{1}{26} \right)$$

$$P[M = x \mid C = y] = \frac{1}{26}$$

Se observa que se cumple $P[M = x \mid C = y] = P[M = x] \ \forall y \forall x$, por lo que **hay secreto perfecto.**

<u>Mensajes de dos letras:</u>

Sea el caso de $M = \{aa, ab, ac, ad, ...zz\} \Rightarrow \# M = 26^2 \Rightarrow P[M = m] = \frac{1}{26^2}$

Como el espacio de claves es el conjunto de todas las permutaciones del alfabeto, resulta que:

$$\# K = 26! \Rightarrow P[K = k] = \frac{1}{26!}$$

El algoritmo de encripción está dado por la aplicación de dichas permutaciones:

	aa	**ab**	**ac**	**…**	**zz**
K_1	aa	ab	ac	…	zz
K_2	aa	ac	ab	…	zz
K_3	aa	ad	ac	…	zz
…					
$K_{26!}$	zz	za	zb	…	yy

Se observa que $Enc_{k1}('aa') = Enc_{k2}('aa') = ...Enc_{k25!}('aa') = 'aa'$.

De manera similar, habrá 25! Encripciones de un mensaje que resultan en el mismo cifrado.

Es decir $Enc_{ki}(x) = y$ para 25! Claves ki distintas.

Sea por ejemplo $y = 'aa'$

$$P[C='aa']=\sum_{ki:Enc_{ki}('aa')=y} P[M='aa']\cdot P[K=ki]+\sum_{ki:Enc_{ki}('ab')=y} P[M='ab']\cdot P[K=ki]+\ldots+\sum_{ki:Enc_{ki}('zz')=y} P[M='zz']\cdot P[K=ki]$$

$$P[C='aa']=\frac{1}{26^2}\cdot\frac{1}{26!}\cdot 25!+\frac{1}{26^2}\cdot 0+\ldots+\frac{1}{26^2}\cdot\frac{1}{26!}\cdot 25!$$

$$P[C='aa']=\frac{1}{26^2}\cdot\frac{1}{26!}\cdot 25!\cdot 26$$

$$P[C='aa']=\frac{1}{26^2}$$

Por otro lado,

$$P[M='aa'|\,C='aa']=\left(P[M='aa']\cdot\sum_{ki:Dec_{ki}('aa')='aa'} P[K=ki]\right)/\,P[C='aa']$$

$$P[M='aa'|\,C='aa']=\left(\frac{1}{26^2}\cdot\frac{1}{26!}\cdot 25!\right)/\left(\frac{1}{26^2}\right)$$

$$P[M='aa'|\,C='aa']=\frac{1}{26}$$

Se observa que $P[M='aa'|\,C='aa']\neq P[M='aa']$ por lo que **NO hay secreto perfecto.**

El experimento $\mathrm{PrivK}_{A,\pi}^{eav}$ también detecta que no hay secreto perfecto. Si el adversario emite $m_0=aa$ y $m_1=ab$, al recibir un cifrado con dos símbolos iguales puede decir que el mensaje cifrado fue el $m_0=aa$ con certeza.

<u>Mensajes de dos letras, excluyendo mensajes de dos letras iguales</u>

Sea el caso de $M=\{ab,ac,ad,....yz\}\Rightarrow \# M=26\bullet 25\Rightarrow P[M=m]=\frac{1}{26\cdot 25}$

Seguimos teniendo $\# K=26!\Rightarrow P[K=k]=\frac{1}{26!}$

El algoritmo de encripción está dado por la aplicación de dichas permutaciones.

Se observa que $Enc_{k1}('ab')=Enc_{k27}('ab')=...Enc_{k...}('ab')='ab'$ en 24! ocasiones

Es decir $Enc_{ki}(x)=y$ para 24! Claves ki distintas.

Sea por ejemplo $y=y_1y_2$

$$P[C=y]=\sum_{ki:Enc_{ki}('ab')=y} P[M='ab']\cdot P[K=ki]+\sum_{ki:Enc_{ki}('ac')=y} P[M='ac']\cdot P[K=ki]+\ldots+\sum_{ki:Enc_{ki}('yz')=y} P[M='yz']\cdot P[K=ki]$$

$$P[C=y]=\frac{1}{26\cdot 25}\cdot\frac{1}{26!}\cdot 24!+\frac{1}{26\cdot 25}\cdot\frac{1}{26!}\cdot 24!+\ldots+\frac{1}{26\cdot 25}\cdot\frac{1}{26!}\cdot 24!$$

$$P[C=y]=\frac{1}{26\cdot 25}\cdot\frac{1}{26!}\cdot 24!\cdot(26\cdot 25)$$

$$P[C=y]=\frac{1}{26\cdot 25}$$

Por otro lado,

$$P[M=x\,|\,C=y]=\left(P[M=x]\cdot\sum_{ki:Dec_{ki}(y')=x} P[K=ki]\right)/\,P[C=y]$$

$$P[M=x\mid C=y]=\left(\frac{1}{26\cdot 25}\cdot\frac{1}{26!}\cdot 24!\right)/\left(\frac{1}{26\cdot 25}\right)$$
$$P[M=x\mid C=y]=\left(\frac{1}{26!}\cdot 24!\right)$$
$$P[M=x\mid C=y]=\left(\frac{1}{26\cdot 25}\right)$$

Se observa que $P[M=x\mid C=y]=P[M=x]$ por lo que **SI hay secreto perfecto.**

Extendiendo esta idea, se concluye que el mayor tamaño que puede tener el espacio de textos planos M para tener secreto perfecto es 26!, y sólo deberán estar las palabras de longitud 26, donde cada símbolo se usa una sola vez, para que haya secreto perfecto.

c. La clave debería ser de, por lo menos, longitud t. Se puede hacer un análisis similar al de los puntos anteriores.

Ejercicio 4:

a) Gen= elige t al azar (por ejemplo t = 2). Luego elige k al azar, de longitud 2, dentro de Σ^*. Por ejemplo, **k=da**.

Si el mensaje **m = bar**, entonces:
m=bar
k=dad
c=eau

b) Hay que tener en cuenta lo siguiente:

- b = 0 se elige con probabilidad 0,5; b = 1 se elige con probabilidad = 0,5.
- Los mensajes elegidos por A pueden resultar en los siguientes cifrados:

Si $|k|=1$:

$Enc_k(m_0=aab)=c_1c_1c_2$ y $Enc_k(m_1=abb)=c_1c_2c_2$

Si $|k|=2$:

$Enc_k(m_0=aab)=c_1c_2c_3$ (eventualmente $c_1=c_2$, si $k_1=k_2$) y $Enc_k(m_1=abb)=c_1c_4c_3$

Si $|k|=3$:

$Enc_k(m_0=aab)=c_1c_2c_3$ (eventualmente $c_1=c_2$, si $k_1=k_2$) y $Enc_k(m_1=abb)=c_1c_4c_3$

Las claves de longitud 1 se eligen con probabilidad $\frac{1}{3}$, y son 26.

Las claves de longitud 2 se eligen con probabilidad $\frac{1}{3}$, y son 26^2

Las claves de longitud 3 se eligen con probabilidad $\frac{1}{3}$, y son 26^3

Para que el experimento $\mathrm{PrivK}_{A,\pi}^{eav}$ tenga éxito, tiene que ocurrir que A emita 0 y el mensaje recibido haya sido m_0, o bien que que A emita 1 y el mensaje recibido haya sido m_1
Así que se evaluará cuál es la probabilidad de que eso ocurra.

Probabilidad de que A emita 0 y el mensaje recibido haya sido m_0.

Como A emite 0 siempre que los dos primeros símbolos del cifrado sean iguales.

- En el caso de que la clave tenga longitud 1, acertará siempre (en 26 de los 26 casos).
- En el caso de que la clave sea de longitud 2, acertará si la clave tiene los dos primeros símbolos iguales, esto es en 26 de los 26^2 casos.
- En el caso de que la clave sea de longitud 3, acertará si la clave tiene los dos primeros símbolos iguales, esto es en 26^2 de los 26^3 casos.

Es decir que la probabilidad de acertar es:

$$\frac{1}{2}\left(\frac{1}{3}\frac{26}{26}+\frac{1}{3}\cdot\frac{26}{26^2}+\frac{1}{3}\cdot\frac{26^2}{26^3}\right)=\frac{1}{2}\left(\frac{1}{3}+\frac{1}{3}\frac{1}{26}+\frac{1}{3}\cdot\frac{1}{26}\right)=0{,}5\cdot 0{,}3589=0{,}17945$$

Probabilidad de que A emita 1 y el mensaje recibido haya sido m_1.

Si la clave tiene longitud 1, acertará siempre.

En el caso de que la clave sea de longitud 2 **no** acertará cuando los símbolos de k sean consecutivos (es decir si $k_1 = k_2 + 1$, entonces $Enc_k(m_1 = abb) = c_1c_1c_3$). Esto ocurre en 26 ocasiones, por lo tanto interesarán los restantes casos que son 26^2-26=26.25, de los 26 casos.

En el caso de que la clave sea de longitud 3 **no** acertará cuando los símbolos de k sean consecutivos (es decir si $k_1 = k_2 + 1$, entonces $Enc_k(m_1 = abb) = c_1c_1c_3$). Esto ocurre en 26^2 ocasiones, por lo tanto interesarán los restantes casos que son 26^3-26^2=26^2.25, de los 26^3 casos.

Es decir que la probabilidad de acertar es:

$$\frac{1}{2}\left(\frac{1}{3}\frac{26}{26}+\frac{1}{3}\cdot\frac{26.25}{26^2}+\frac{1}{3}\cdot\frac{26^2.25}{26^3}\right)=\frac{1}{2}\left(\frac{1}{3}+\frac{1}{3}\frac{25}{26}+\frac{1}{3}\cdot\frac{25}{26}\right)=0{,}5\cdot 0{,}9743=0{,}48715$$

De lo anterior se desprende que $\Pr\left[\mathrm{PrivK}_{A,\pi}^{eav}=1\right]=0{,}6666$

c) Como la probabilidad **no es 0,5**, el esquema **no** tiene secreto perfecto.

Ejercicio 5:

Teniendo en cuenta: ***[Katz Cap. 3]***

Un esquema de encripción de clave privada $\pi =$ **(Gen, Enc, Dec),** tiene encripciones indistinguibles ante CPA si para todo **adversario PPT A** existe una función despreciable **negl** tal que:

$$\Pr\left[\mathrm{PrivK}_{A,\pi}^{\mathrm{CPA}}(n)=1\right]\le\frac{1}{2}+negl(n)$$

donde el experimento $\mathrm{PrivK}_{A,\pi}^{\mathrm{CPA}}(n)$: consiste en los siguientes pasos:

- Se genera una **clave k** mediante **Gen(1^n)**
- El **adversario A** tiene acceso a **$Enc_k(.)$** , y emite un par de mensajes **m_0** y **m_1**, de igual longitud.
- Se elige un bit aleatorio **b←{0,1}.**
  Se calcula un cifrado **c←$Enc_k(m_b)$** y se lo entrega a **A**. (c = challenge ciphertext).
- **A** sigue teniendo acceso a través del oráculo a **$Enc_k(.)$** y emite un bit **b'**
- Si **b'=b**, la salida del experimento es 1 (ÉXITO). Sino, es 0.

Hay que mostrar entonces que un adversario puede tener ÉXITO con probabilidad mayor que 0,5.

- **cifrado de sustitución monoalfabética**

<u>(Asumiendo Alfabeto Inglés de 26 símbolos)</u>

<u>Mensajes de longitud 1.</u>

La clave k se elige en forma uniforme dentro de un espacio de tamaño 26!

El algoritmo de encripción está dado por la aplicación de dichas permutaciones:

	a	b	c	…	z
K_1	a	b	c	…	z
K_2	a	c	b	…	z
K_3	a	d	c	…	z
…					
$K_{26!}$	z	a	b	…	y

El adversario podría pedir al oráculo la encripción de todos los símbolos de Σ menos la de m_0 y m_1.que se usarán para el experimento. Por ejemplo, $m_0 = "a"$ y $m_1 = "b"$.

Luego, el adversario emite el par de mensajes m_0 y m_1 y recibe un cifrado c que corresponde a

$Enc_k(m_b)$ con $P(b=0)=P(b=1)=\frac{1}{2}$

Como hizo la encripción con el oráculo de todos los demás símbolos, se sabe cómo se encriptó de la 'c' a la 'z'. Por ejemplo, podría ser que de la 'c' a la 'z' se encriptó:

c	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
c	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*

Pero entonces las encripciones posibles para a y b son:

a	**b**
a	b
b	a

Suponemos que el adversario elige 0 cuando ve $c=\text{"}a\text{"}$ a y 1 en caso contrario.

$\Pr\left[\text{PrivK}_{A,\pi}^{CPA}(n)=1\right]=\left[\Pr(b'=0 \wedge b=0)\right]+\left[\Pr(b'=1 \wedge b=1)\right]$

$\Rightarrow= \Pr(b=0)\cdot\left[\Pr(b'=0 \mid b=0)\right]+\Pr(b=1)\cdot\left[\Pr(b'=1 \mid b=1)\right]$

$\Rightarrow= \frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}$

$\Rightarrow= 0{,}5$

Este análisis es el mismo para cualquier par de mensajes de longitud 1 cualquiera sea el resultado entregado por el oráculo.

Tiene éxito el experimento con probabilidad 0,5, por lo que es indistinguible ante Ataque de Texto Plano Elegido (CPA) para mensajes de longitud 1.

<u>Mensajes de longitud mayor que 1.</u>

El adversario emite, por ejemplo, $m_0=aa$ y $m_1=ab$.

Con probabilidades iguales puede recibir $Enc(m_0)$ si b = 0, o $Enc(m_1)$ si b = 1.

El adversario emite b' = 0 si en el cifrado recibido los dos símbolos son iguales, o b'=1 en caso contrario.

Como la encripción por sustitución monoalfabética es una función biyectiva, la única manera de que el cifrado resulte en dos símbolos iguales es si lo que se cifró es $m_0=aa$

Por lo tanto: $\Pr\left[\text{PrivK}_{A,\pi}^{CPA}(n)=1\right]=\frac{1}{2}\left[\Pr(b'=0 \mid b=0)\right]+\frac{1}{2}\left[\Pr(b'=1 \mid b=1)\right]=\frac{1}{2}\cdot 1+\frac{1}{2}\cdot 1=1$

Como el experimento tiene éxito siempre, sin siquiera haber consultado el oráculo, el esquema **no** es seguro ante Ataques de Texto Plano Elegido.

- **cifrado de Vigenère**

El adversario tiene posibilidades de consultar al oráculo para encriptar cualquier mensaje de su elección. Por lo tanto, puede pedir la encripción de $m=a$, $m=aa$, $m=aaa$, etc.

Al recibir de parte del oráculo un $c=c_0c_1\ldots c_n$ con $c_0=c_n$, el adversario deduce que ***n*** es la longitud de la clave.

Luego, el adversario emite $m_0=a^{2n}$ y $m_1=a^n b^n$.

Con probabilidades iguales puede recibir $Enc(m_0)$ si b = 0, o $Enc(m_1)$ si b = 1.

En un caso, $c=c_0c_1\ldots c_n c_0 c_1\ldots c_n$ y en el otro, $c=c_0c_1\ldots c_n c_1 c_2\ldots c_0$

El adversario decide emitir $b'=0$ cuando ve que el cifrado tiene la forma $c=\alpha\alpha$ y $b'=1$ en caso contrario.

Pero entonces el experimento tiene éxito siempre, ya que la encripción de $m_0=a^{2n}$ puede dar como resultado $c=\alpha\alpha$ si la clave es n.

Es decir:

$\Pr\left[\text{PrivK}_{A,\pi}^{CPA}(n)=1\right]=\left[\Pr(b'=0 \wedge b=0)\right]+\left[\Pr(b'=1 \wedge b=1)\right]$

$\Rightarrow = \Pr(b=0)\cdot[\Pr(b'=0 \mid b=0)] + \Pr(b=1)\cdot[\Pr(b'=1 \mid b=1)]$

$\Rightarrow = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1$

$\Rightarrow = 1$

Como el experimento tiene éxito siempre, el esquema **no** es seguro ante Ataques de Texto Plano Elegido.

Ejercicio 6:

a) En CBC un error en un bit se propaga hasta el final

b) En CBC un error en un bit en C1 se propaga a P1 y P2

c)

[Menezes, Cap. 7]

Propiedades del Modo CFB:

Propagación de errores: uno o más bit con errores en un bloque de texto cifrado c_j, afecta el descifrado de ese y de los $\left\lceil \frac{n}{r} \right\rceil$ bloques de texto cifrado siguientes. El bloque de texto plano recuperado x'_j va a diferir del verdadero x_j en la posición en donde está el error en c_j.

Ejercicio 7:

a) 5 bits, para poder encriptar del 0 al 31. El espacio efectivo de la clave es $\varphi(32)=\varphi(2^5)=16$. Se calcula la cantidad de números coprimos con 32, ya que si K no es coprimo con 32, se corre el riesgo de que al encriptar se obtenga todo cero. Ejemplo: si K = 2 y M = 16, E(2,M) = M*2 = 32 = 0 módulo 32.

b) Encriptar el mensaje 24 17 26 25 12 usando modo CBC con vector de inicialización IV = 19 y K = 7.

Mensaje cifrado = $13-4-18-13-7$

Se va resolviendo:

$(IV \oplus P1) = (19 \oplus 24) = 11$

$E(K,11) = E(7,11) = 13 \rightarrow C1$

$(C1 \oplus P2) = (13 \oplus 17) = 28$

$E(K,28) = E(7,28) = 4 \rightarrow C2$

$(C2 \oplus P3) = (4 \oplus 26) = 30$

$E(K,30) = E(7,30) = 18 \rightarrow C3$

$(C3 \oplus P4) = (18 \oplus 25) = 11$

$E(K,11) = E(7,11) = 13 \rightarrow C4$

$(C4 \oplus P5) = (13 \oplus 12) = 1$

$E(K,1) = E(7,1) = 7 \rightarrow C5$

c) Desencriptar en modo CBC.

Al desencriptar, deberíamos aplicar el algoritmo inverso con la clave 7. (Dividir por 7). Pero “Dividir” por 7 módulo 32, es lo mismo que multiplicar por 23 y reducir módulo 32.

Es decir, hay que usar $K^{-1} = 23$, porque $K.K^{-1} \equiv 1(32)$

$E(K^{-1},13) = E(23,13) = 11$

$(11 \oplus IV) = (11 \oplus 19) = 24 \rightarrow P1$

$E(K^{-1},4) = E(23,4) = 28$

$(28 \oplus C1) = (28 \oplus 13) = 17 \rightarrow P2$

$E(K^{-1},18) = E(23,18) = 30$

$(30 \oplus C2) = (30 \oplus 4) = 26 \rightarrow P3$

...

Ejercicio 8:

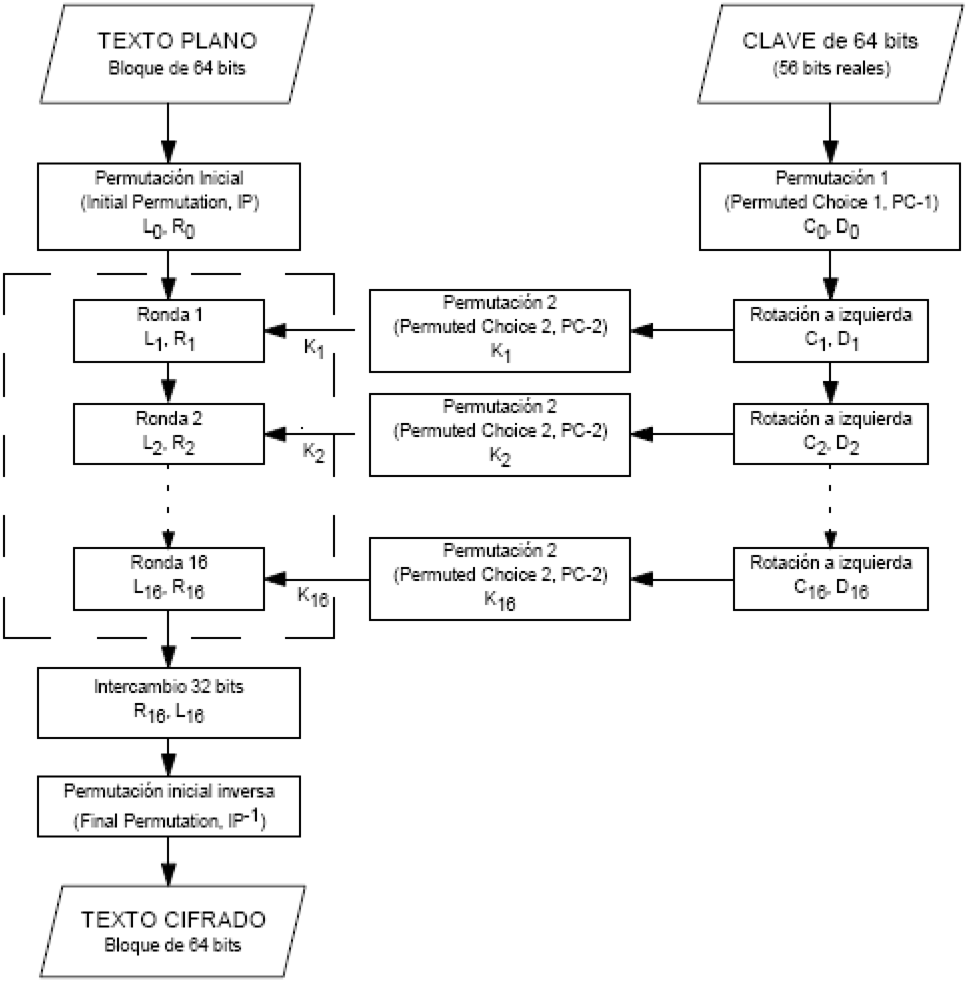
a) Hay que tener en cuenta cómo funciona una caja feistel: **[Menezes Chap. 7]**

Un cifrado Feistel es un cifrado iterativo que mapea un texto plano de $2t - bits$ (L_0, R_0) *en un texto cifrado* (R_r, L_r) *, a través de un proceso de* r *rondas, con* $r \geq 1$ *. Cada ronda* $1 \leq i \leq r$ *transforma* $(L_{i-1}, R_{i-1}) \rightarrow_{Ki} (L_i, R_i)$ *de la siguiente manera:*

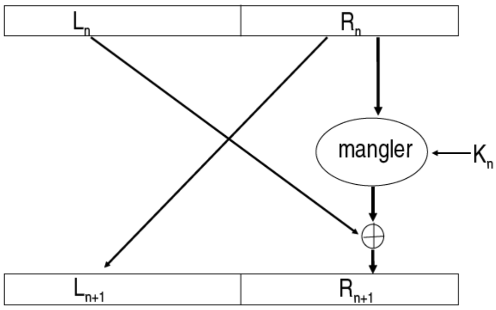
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

donde cada subclave K_i *se deriva de la clave original* K

En DES, el proceso para transformar un texto plano x de 64 bits con una clave K de 64 bits es:



Donde en cada ronda se usa una caja feistel, donde las transformaciones se llevan a cabo mediante una función que expande R_{i-1} , hace un $\oplus$ con la nueva subclave K_i y elige un valor de SBox y permuta la parte izquierda de la clave.



La clave K se tranforma en cada ronda mediante rotaciones y permutaciones:

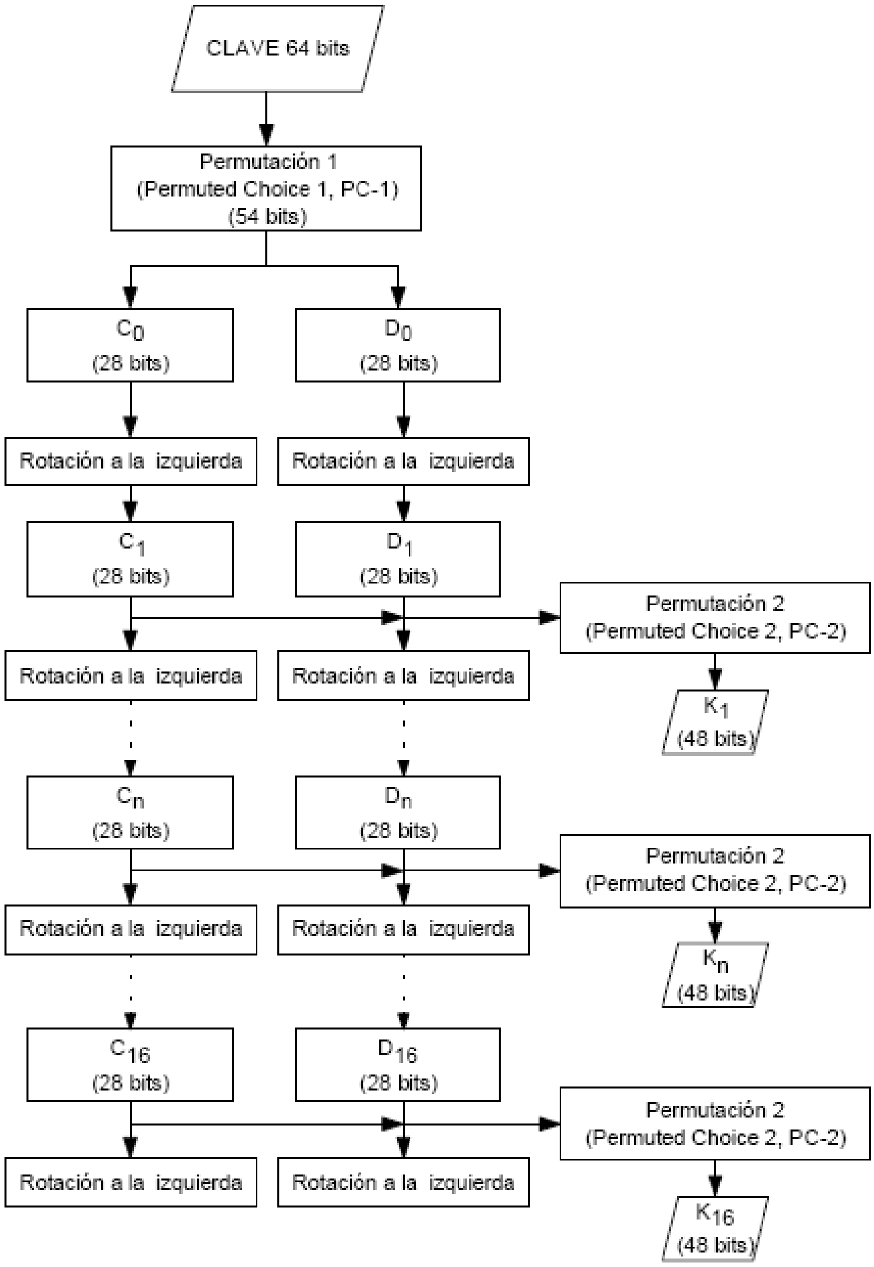


Figura 2: Cálculo de las subclaves, K_i

Todos 0: Si la clave está formada sólo por ceros, al cabo de cierto número de rounds termino teniendo el mensaje original:

Al comienzo:

$m=L_0R_0$ y $K=C_0D_0$ donde tanto C_0 como D_0 tienen todos sus bits en 0.

después de la primera ronda:

$L_1=R_0$ y $R_1 = L_0 \oplus f(R_0, K_0)$

Como la función f hace $R_0 \oplus K_0=00\ldots0$, resulta R_0 sin cambios

$R_1 = L_0 \oplus R_0$

Así, después de la primera ronda:

$L_1R_1 = R_0(L_0 \oplus R_0)$

Después de la segunda:

$L_2R_2 = R_1(L_1 \oplus R_1) = (L_0 \oplus R_0)(R_0 \oplus (L_0 \oplus R_0))$

y como $(R_0 \oplus (L_0 \oplus R_0)) = L_0$ queda:

$L_2R_2 = (L_0 \oplus R_0)L_0$

En la siguiente:

$L_3R_3 = R_2(L_2 \oplus R_2) = L_0((L_0 \oplus R_0) \oplus L_0)$

y como $((L_0 \oplus R_0) \oplus L_0) = R_0$ queda:

$L_3R_3=L_0R_0$

Como se ve, las rondas impares terminan obteniendo nuevamente el mensaje original.

Todos 1: Si la clave está formada sólo por unos, el análisis es similar.

Por otra parte, hay que tener en cuenta que como el cifrado es simétrico, debe utilizarse la misma clave en sentido inverso. Si la clave utilizada no se modifica en las sucesivas rondas, (en las rondas de modificación de las claves), se aplicará 16 veces la misma clave al encriptar que al desencriptar. Es decir, los 16 rounds inversos son iguales a los 16 rounds originales. Por eso, otras claves débiles son: $\{0\}^{28}\{1\}^{28}$ y $\{1\}^{28}\{0\}^{28}$.

Importante: estamos considerando las claves de 56 bits correspondientes a las rondas.

[Menezes Chap. 7]:

(ii) Weak keys, semi-weak keys, and fixed points

If subkeys K_1 to K_{16} are equal, then the reversed and original schedules create identical subkeys: $K_1 = K_{16}$, $K_2 = K_{15}$, and so on. Consequently, the encryption and decryption functions coincide. These are called weak keys (and also: *palindromic keys*).

The four DES weak keys are listed in Table 7.5, along with corresponding 28-bit variables C_0 and D_0 of Algorithm 7.83; here $\{0\}^j$ represents j repetitions of bit 0. Since C_0 and D_0 are all-zero or all-one bit vectors, and rotation of these has no effect, it follows that all subkeys K_i are equal and an involution results as noted above.

	C_0	D_0
	$\{0\}^{28}$	$\{0\}^{28}$
	$\{1\}^{28}$	$\{1\}^{28}$
	$\{0\}^{28}$	$\{1\}^{28}$
	$\{1\}^{28}$	$\{0\}^{28}$