Practico 2 de Criptografia-2007

1): Las cuatro claves debiles de DES (miradas como claves de 56 bits, i..e, eliminando cada octavo bit) tienen la propiedad de que si una clave es débil, su complemento tambien lo es. Suponga que ahora Ud. define DES-mejorado en donde DES-mejorado es igual que DES, solo que ahora tiene una clave de, digamos, 128 bits, y la expansión de clave esta dada por: (K denota la clave, k_i la clave de ronda i)

$$
\begin{aligned}
&for\ i = 1\ to\ 16\\
&\qquad k_i = seleccionar_i(K);\\
&\qquad K := T_i(K);\\
&next\ i
\end{aligned}
$$

donde $seleccionar_i$ es una función que selecciona 48 bits de los 128, dada por ua tabla de selección que cambia de ronda a ronda, y $T_i : \boldsymbol{Z}_2^{128} \mapsto \boldsymbol{Z}_2^{128}$ son transformaciónes lineales biyectivas, tambien dependientes de las rondas, pero con la propiedad de que todas ellas cumplen que $T_i(1...1) = (1...1)$. (no se pierde ningun 1)

Sin conocer las tablas de selección o las transformaciones lineales es imposible saber si DES-mejorado tiene o no claves debiles, y teniendo en cuenta que todas dependen de las rondas, debe ser casi imposible que tenga. De todos modos, probar que, si tuviera claves débiles, entonces si una clave es débil su complemento también.

2): La tabla de selección de los bits de las claves de ronda en DES es: (i.e., el primer bit es 14, el segundo 17, etc)

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Recordemos que antes de la ronda i se rotan las mitades (de 28 bit c/u) de la clave maestra por 1 bit a la izquierda si $i = 1, 2, 9, 16$, y por 2 bits en las otras rondas.

Determinar cuantas veces se usa cada bit de la clave.

3): Probar que una ronda de la estructura de Lai-Massey puede verse como tres rondas de Feistel, con dos de esas rondas "triviales" (es decir, con funcion de ronda igual a la identidad)

4): Si en vez de usar la operacion $\oplus$ en la estructura de Lai-Massey quisiera usar otra operacion de grupo $+$, ¿como debiera ser la estructura? (describir la estructura de encripcion y la de descripcion) (hay (al menos) dos respuestas posibles).

5): Supongamos que definimos IDEA-128 con la misma estructura de IDEA, solo que ahora en vez de tener 4 subloques de 16 bits, tenemos 4 subbloques de 32 bits, cambiando las operaciones a los grupos adecuados. ¿Cual es el problema obvio con esta definicion? ¿Se le ocurre alguna solución?