Tarea 2 criptografía

José Lara Hinojosa

Mayo 2021

Pregunta 1

1.a key-schedule

El key-schedule es el algoritmo que genera las subllaves de DES basadas en una llave inicial secreta.
Inicialmente la llave tiene 64 bits y es pasada por el PC 1 (Permuted Choice 1) que selecciona 56 de estos bits y los 8 restantes son descartados o usados como bits de paridad. Estos 56 bits se dividen en dos segmentos de 28 bits cada uno, donde por separado, son pasados por una serie de pasos. En rondas sucesivas, estos dos segmentos permutados de la llave original son rotados a la izquierda (en uno o en dos bits dependiendo de la ronda), luego, en cada ronda, 48 bits formados por estos segmentos son tomados por el PC 2 (Permuted Choice 2), creando la primera subkey de 48 bits.
Las siguientes n rondas definen las n subkeys siguientes de 48 bits, donde también se ocupa la PC 2 pero los segmentos han sido rotados más veces por lo que se generan llaves diferentes también .
El proceso de key schedule para decriptar es similar, solo que las subkeys están en orden reverso en comparación a la forma de encriptación.
Lo anterior fue basado desde wikipedia:
`https://en.wikipedia.org/wiki/Data_Encryption_Standard`
Por lo tanto, la llave que se ocupa en cada f de la red de feistel esta dada por este key-schedule, que genera estas llaves desde la llave principal, donde se ocupa una diferente por cada ronda de la red de feistel.

1.b