Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

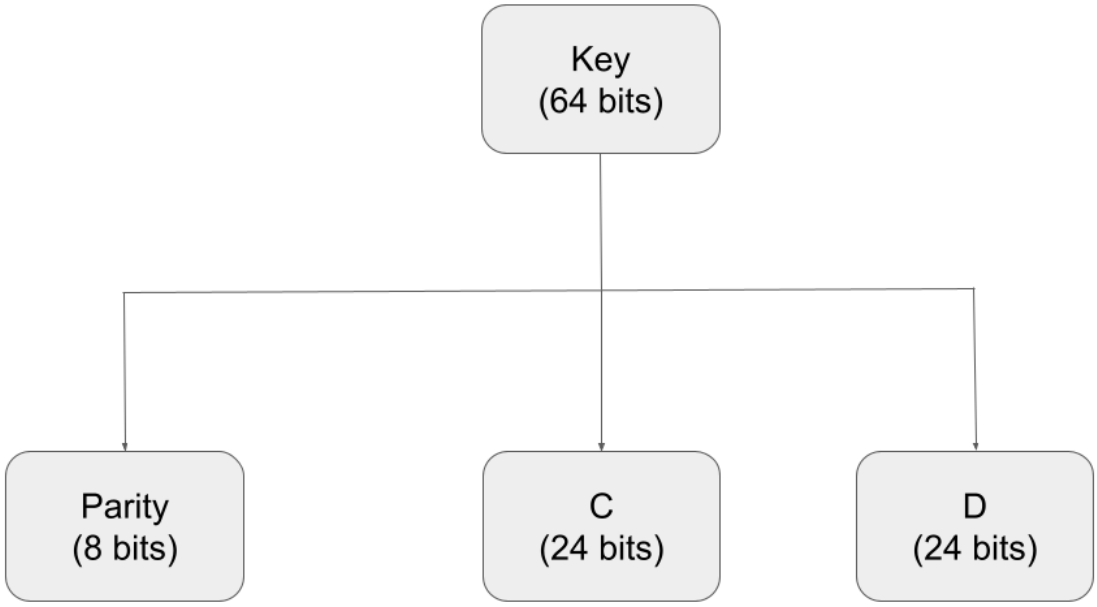
IIC3253 - Criptografía y Seguridad Computacional

Sebasthian von Bergen (15635635)

Tarea 2 – Respuesta Pregunta 1

- a) Investigue y describa en detalle el key-schedule, es decir, explique cómo se deriva la llave correspondiente a cada ronda en base a la llave original.

  Utilizando una seria de permutaciones, se pueden generar 16 subclaves de 48 bits a partir de una clave inicial de 64 bits. Para comenzar, la clave original se separa en 3 partes.



  A partir de estas 2 partes C y D se construyen todas las siguientes subclaves. En cada ronda se toma C y D y se aplica un *left-rotate* de 1 o 2 bits (la cantidad se muestra en la tabla de abajo).

Table 1 - Key Schedule for DES																
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Shift	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
Total	1	2	4	6	8	10	12	14	15	17	19	21	23	25	27	28

En cada ronda despues de haber rotado C y D, se juntan los resultados y se entrega una clave k_i. Todo este proceso es reversible para el caso de desencriptacion aplicando la funcion *right-rotate* en vez de *left-rotate* en cada ronda. Una vez completadas las 16 rondas, se llega de vuelta a los valores originales de C y D.

- b)