NOMBRE: Felipe Carlos Jiménez Ortega SECCIÓN: 1

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

IIC3253 — Criptografía y Seguridad Computacional — 1' 2021

Tarea 2 – Respuesta Pregunta 1

1. El key-schedule para DES consiste en recibir la llave de 64-bits y lo primero que se hace es eliminar los bits múltiples de 8 que se utilizan para verificar la paridad del mensaje. En la siguiente tabla, aquellos números en negrita son los bits que serán eliminados, quedando una llave de 56-bits.

Table 1: **Parity Drop Table**

1	2	3	4	5	6	7	**8**
9	10	11	12	13	14	15	**16**
17	18	19	20	21	22	23	**24**
25	26	27	28	29	30	31	**32**
33	34	35	36	37	38	39	**40**
41	42	43	44	45	46	47	**48**
49	50	51	52	53	54	55	**56**
57	58	59	60	61	62	63	**64**

Luego, se utiliza Permuted Choice 1, que toma los 56-bits y los parte por la mitad, y para cada una de las mitades se utiliza una tabla de permutación, ya sea la izquierda o derecha de acuerdo a la siguiente tabla. Una vez que la llave está dividida en 2 partes de 28-bits, se procede a ejecutar un left shift

Table 2: Left

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

Table 3: Right

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

circular de uno o dos bits de acuerdo a la ronda que se esté ejecutando; si la ronda es la 1,2,9 o 16, se ejecuta un left shift circular de 1 bit, en cualquier otro caso, es de 2 bits. Por último, se ejecuta Permuted Choice 2 a los 56-bits (se juntan ambas partes) y que retornará la llave k_i de la ronda i de 48-bits. A continuación la tabla de permutación que se ocupa. De esta manera, para cada ronda i se obtiene una k_i haciendo todo el proceso anteriormente descrito a partir de la llave k, se obtendrán las sub-llaves $k_1, ..., k_{16}$ para DES.

Table 4: **Permuted Choice 2**

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