NOMBRE: Javier Tramon

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

a) Key-scedule es el manejo de planificación de las claves dentro del proceso de generación de claves para el algoritmo de encriptación DES. Este consiste en un procedimiento de permutación y transformación de la clave original de 64 bits, donde es transformada para generar 16 subllaves de 48 bits que serán utilizadas dentro del algoritmo por las funciones F.

La primera parte del algoritmo consta del procedimiento PC 1, donde primero se eliminan los 8 bits de paridad continuando con una permutación de la clave según la tabla a de la imagen 2 y una posterior división de la clave de 56 bits en dos partes de 28 bits, quedando C_0 y D_0. Posteriormente, para cada ronda, su subclave rota 1 o 2 bits a la izquierda según la tabla de la imagen 1 . Esto genera 32 subclaves por las 16 rondas y ambas mitades C_i y D_i.

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

Figure 1: Tabla de rotaciones PC1

PC_1						
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
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

(a)

PC_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

(b)

Figure 2: Tablas de permutaciones PC1 y PC2

Con el resultado de esta permutación se aplica el algoritmo PC2, esta permutación se conoce como la permutación por compresión, dado que las operaciones de concatenar y permutar ambas mitades de la subclave de la ronda, lo que genera la clave K de la ronda de 48 bits que será utilizada en la función F.

Para el proceso se aplica la permutación realizada en base a la tabla b de la imagen 2 y posteriormente la concatenación, se concatena C_i y después D_i. La versión algorítmica de esta permutación se encuentra

en la imagen 3 para cada lado de la sub clave. Cada * indica una autoclave generada por la caja S, mientras que las X son bits excluidos de las subclaves. Esta permutación permite generar ambas subclaves de 24 bits cuando originalmente eran de 28. Con estas permutaciones se concatenan ambas sub llaves y obtenemos la clave para la ronda correpondiente.
Podemos ver aca un resumen de lo que sería el algoritmo de key schedule para cada llave de la ronda i:

Table 2 - Current DES Permutation PC2
C: 1 4* 2* 3 1* 2 4 3* X 2* 1 3 4 1* 2 4* 1 X 3 4 2 X 3* 1 X 3 4 2
D: 8 6* 5 8* 6 7 X 8 5 X 7 6 5* 8 X 7* 6 8* 5 6* 7 8 6 5 7* X 5* 7

Figure 3: Algoritmo de permutaciones de PC2

$K(i) = PC2(KS(U, i)),$ donde $U = PC1(K)$ y $KS(U, i)$ es las rotaciones declaradas en la tabla 1.

b) Para el ataque pienso que la mejor manera es usando el método de fuerza bruta, donde poseo dos mensajes con sus respectivas encriptaciones. Con esto, genero 2^{28} llaves donde la primera mitad tiene 2^{28} combinaciones de bits, mientras que la segunda solo 0s. Sabiendo que el comportamiento de las mitades de las funciones F es afectado por cada mitad de la llave original de la misma manera, entonces podré enfocarme en el comportamiento de la encriptación del algoritmo. Con el resultado de la encriptación de los mensaje originales usando estas keys, les aplico XOR con la encriptación del mensaje original, y busco que se logre un resultado de más del 50% de coincidencia, lo cual consideraría la llave como una llave posiblemente correcta.

Este procedimiento lo ejecuto para ambos lados de la llave, que al concatenar las posibles mitades correctas, tendría un conjunto de llaves posibles. Esto lo repito para un segundo mensaje con su encriptación, generando un segundo conjunto de posibles llaves posibles, donde la intersección de las llaves posiblemente correctas será muy probablemente la llave de encriptación. Esto tomaría, considerando los 2^{28} pasos para generar las llaves, que son dos mitades, y que son 2 pares de mensajes, un total 2^{30} pasos.