Criptografía - Tarea 2.

Matías Correa

Pregunta 1

a) Describa el key-schedule de DES.

El key schedule es un algoritmo que, a partir de una llave k, genera 16 sub-llaves $\{k_1, \dots, k_{16}\}$.

El input del algoritmo es:
- k: llave de 64 bits
- PC1: Permuted choice 1 — $PC1: \{1,0\}^{64} \to \{1,0\}^{56}$
- PC2: Permuted choice 2. — $PC2: \{1,0\}^{56} \to \{1,0\}^{48}$
- $\{s_1, \dots, s_{16}\}$: left shifts. — $s_i: \{1,0\}^{28} \to \{1,0\}^{28}$

El output es:
- $\{k_1, \dots, k_{16}\}$: sub-llaves de 48 bits

Las elecciones permutadas PC1 y PC2 son permutaciones que además descartan el último bit de cada byte. Este bit es utilizado como bit de paridad de los 7 bits anteriores: corresponde al XOR de éstos.

El conjunto de left shifts $\{s_1, \dots, s_{16}\}$ está definido por:

$$s_i(l) := \begin{cases} \text{left\_circular\_shift}(l,1) & \text{si } i \in \{1,2,9,16\} \\ \text{left\_circular\_shift}(l,2) & \text{e.o.c.} \end{cases}$$

Con $l \in \{0,1\}^{28}$ y left_circular_shift(l, n) definido como la función que realiza un shift circular a la izquierda de n bits sobre la cadena de bits l.

El algoritmo es como sigue:

1) Procesar, excluyendo los bits de paridad, k por PC1. Se obtiene $K_0 := PC1(k)$

Para todo $i \in \{0, \dots, 15\}$:

2) K_i se separe en sus mitades L_i y R_i

3) Aplicando S_i sobre cada mitad, se obtienen $L_{i+1} := S_i(L_i)$ y $R_{i+1} := S_i(R_i)$.

4) Concatenando las mitades, se procesan por PC2 para obtener $K_{i+1} := PC2(L_{i+1} \| R_{i+1})$

4) Entregar las 16 sub-llaves de 48 bits, $\{k_1, \dots, k_{16}\}$