Profesor: Alejandro Hevia
Auxiliar: Bryan Ortiz
Ayudante: David Contreras

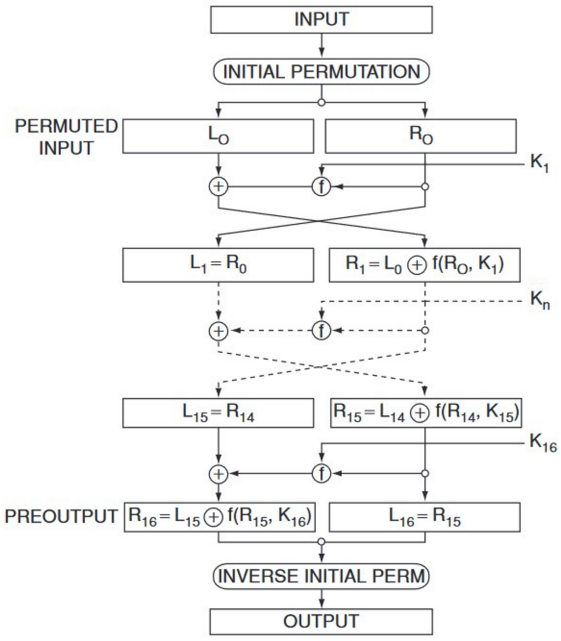
CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE CHILE

Tarea 1

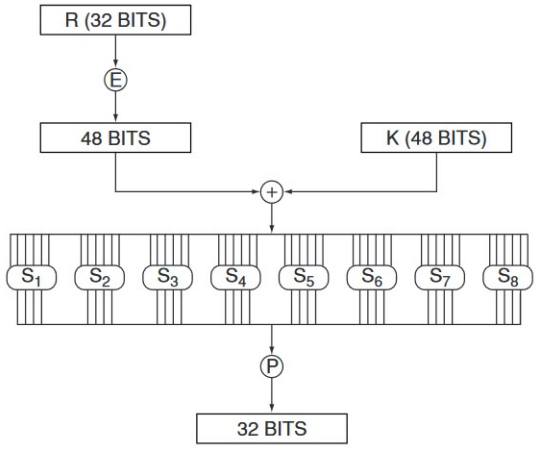
CP, Cifradores de Bloque y PRF

Fecha de Entrega: 10 de Septiembre, 2024

P1. El cifrador de bloque DES se compone por 16 rondas de Feistel, tal como se ilustra en la Figura 1a. En cada ronda i, el proceso de cifrado aplica una función conocida $f(K_i, R_i)$ (ver Figura 1b), y el resultado es luego operado con L_i mediante un XOR.



(a) Diagrama del algoritmo de cifrado DES.



(b) Diagrama de función f.

Figura 1: Representación gráfica del cifrador DES.

Considere una versión simplificada de DES llamada 2-SDES, la cual consiste en aplicar sólo dos rondas de la red de Feistel. Demuestre que 2-SDES no es un PRF. Indique el número de consultas realizadas al oráculo y un tiempo estimado de ejecución para la rutina del adversario, explicite supuestos.

P2. Sea $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ una función pseudoaleatoria (es decir, un PRF seguro). Considere la familia de funciones $E' : \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ definida para todo $x, x' \in \{0,1\}^n$ como:

$$E'_K(x\|x') := E_K(x \oplus x')\|E_K(x \oplus \overline{x'})$$

donde $\|$ denota la concatenación de strings binarios, y para todo $x \in \{0,1\}^n$, y $\overline{x} = 1^n \oplus x$ denota el complemento de x. Demuestre o refute que E' es una función pseudoaleatoria.