Universidad del Rosario

Matemáticas Aplicadas y Ciencias de la Computación

Introducción a la criptografía

Profesor: Mateo Sanabria Ardila

Examen 1

Fecha de entrega:31/Ago | 2022-20 | Nota máxima: 50

1. (**25pts**) Dados $x, y, a, b \in \mathbb{Z}_{26}$ tal que $gcd(a, 26) = 1$, se propone la siguiente función para cifrar x con la llave $k = (a, b)$:

$$e_k(x) = y \equiv ax + b \textbf{ mod } 26$$

   (a) (**10pts**) Proponga una función $d_k(y)$ tal que

$$d_k(e_k(x)) = x$$

   Es decir la función para descifrar $e_k(x)$, **demuestre** que la función que propone cumple dicha propiedad.

   (b) (**5pts**) Basado en un conteo numérico, explique que tan seguro es este algoritmo.

   (c) (**10pts**) Suponga que tiene n claves de la forma (a_i, b_i) con $i \in [0 : n)$ y se realiza el ciframiento de x aplicando la composición de $e_{k_i}(x)$ un total de n veces,es decir:

$$y = e_{k_n}(e_{k_n-1}(e_{k_n-2}(e_{k_n-3}(\cdots e_{k_0}(x)\cdots))))$$

   Proponga y **demuestre** una generalización para y en términos de una única aplicación de $e_K(x)$ y una única llave $K = (A, B)$, es decir:

$$Ax + B \textbf{ mod } 26 = e_{k_n}(e_{k_n-1}(e_{k_n-2}(e_{k_n-3}(\cdots e_{k_0}(x)\cdots))))$$

2. (**5pts**) Demuestre que para $a, b \in \mathbb{Z}_2$

$$a \oplus b \equiv a + b \textbf{ mod } 2$$

3. (**20pts**) **Demuestre** que cada ronda de DES es su propia inversa, para esto puede pensar cada ronda de DES como una red Feistel, es decir sin entrar en detalles de la implementación interna de cada tabla al interior de la ronda.