Práctica 5: Simulación de un sistema criptográfico de clave privada: Sustitución Monoalfabética

6 de abril - 7 de abril - 12 de abril

SOLUCIÓN

El esta práctica vamos a simular un sistema criptográfico de clave privada basado en la técnica criptográfica de sustitución monoalfabética. A continuación se describe cómo se puede trabajar algebraicamente con este sistema criptográfico, sin más que usar aritmética modular.

Para encriptar la información escrita en el alfabeto $\mathcal{A}$

> $\mathcal{A}$ = "aáàbcdeéfghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFGHIÍJKLMNÑOÓPQR STUÚVWXYZ0123456789 ,.:-()"

alfabeto con 81 caracteres, ciframos cada símbolo del mensaje utilizando el siguiente proceso:

- Codificación numérica: A cada símbolo α del alfabeto se le asigna el número $n(\alpha) = p(\alpha) - 1$, donde $p(\alpha)$ es la posición que ocupa α dentro del alfabeto ($0 \leq n(\alpha) \leq 80$).
- Cifrado por sustitución monoalfabética con **clave de cifrado** $(a, b) \in (\mathbb{Z}_{81})^2$, descrito en la siguiente función

$$\begin{array}{rccc} f: & \mathbb{Z}_{81} & \to & \mathbb{Z}_{81} \\ & n & \mapsto & an+b \end{array}$$

  Nota: a debe ser un elemento de $\mathbb{Z}_{81}$ con inverso, es decir, $\text{mcd}(a, 81) = 1$.
- Decodificación numérica: Proceso inverso al descrito para la codificación numérica.

(el mensaje cifrado es la concatenación del cifrado de los símbolos)

Una vez fijada la clave de cifrado, la función sustitución monoalfabética establece una biyección del alfabeto $\mathcal{A}$ de forma que a cada letra en claro se le asocia de forma única otra letra del alfabeto $\mathcal{A}$, letra cifrada. De esta forma, para realizar la operación de descifrado, podríamos optar por almacenar, de forma exhaustiva, dicha biyección. Sin embargo, también podemos optar por describir el proceso de descifrado vía la operación aritmética que permite construir la función inversa f^{-1}. Es fácil de demostrar que f^{-1} es una sustitución monoalfabética con clave

$$(a^{-1}, -a^{-1}b)$$

denominada **clave de descifrado**.

Si trabajamos con las claves de cifrado y de descifrado, la implementación los procesos de cifrado y de descifrado no requiere el almacenamiento de la biyección que determina el cambio de alfabeto.

PROBLEMA PARA RESOLVER

Supongamos que un mensaje en claro lo ciframos con sustitución monoalfabética de forma que para cada línea del mensaje en claro usamos la **clave de cifrado**

$$(64^i, i \cdot 5) \in (\mathbb{Z}_{81})^2$$

siendo i el lugar que ocupa la línea dentro del mensaje (como hemos hecho en las prácticas anteriores, los cambios de línea de los mensajes en claro los codificamos como dos espacios). Si el mensaje cifrado es el dado en el archivo datos_5.txt, obtener el mensaje en claro.

mensaje en claro

Las matemáticas son como una CORRIENTE de agua.
Existen diversas teorías complicadas, es cierto, pero
la LÓGICA básica es muy sencilla. De igual modo
que el AGUA fluye desde un lugar elevado hacia
otro más bajo tomando la distancia más CORTA,
sólo hay una corriente matemática.
(1Q84, Haruki Murakami, Kioto 1949)