Práctica 07. Clave Privada: Cifrado por Bloques

19 de abril de 2023

Apellidos: ..... Nombre: .....

Apellidos: ..... Nombre: .....

Grupo G3. Ordenador: .....

En esta práctica vamos a cifrar y descifrar mensajes usando el cifrado de Hill y el cifrado afín. En ambos casos son cifrados que trabajan con bloques. En los dos problemas a resolver la información está escrita en el alfabeto *alf* formado por los 85 símbolos:

"aáàbcdeéfghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFG
HIÍJKLMNÑOÓPQRSTUÚVWXYZ0123456789 ,.:;-()¿?"

(alfabeto disponible en la variable alf del fichero entrada_datos_07.txt, dentro de la carpeta práctica 07 de la moodle)

Los procesos de cifrado siguen los siguientes pasos:

1. 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 ($0 \leq n(\alpha) \leq 84$). El mensaje numérico será una lista con las codificaciones numéricas de sus símbolos.

2. Relleno del mensaje numérico (**padding**). Si k es la longitud del bloque que usa el cifrado, se completa el mensaje numérico realizando os siguientes pasos:

   - Se rellena el último bloque del mensaje numérico con números aleatorios en $\mathbb{Z}_{85}$.
   - Se añade un último bloque con la expresión (en base 85) de la longitud del mensaje numérico (completada con ceros a la izquierda hasta obtener longitud k).

3. Cifrado por bloques. Para cada bloque $\underline{z} \in (\mathbb{Z}_{85})^k$ del mensaje numérico, se le aplica la función de cifrado.

Cifrado de Hill. En el caso del cifrado de Hill, la función de cifrado es:

$$\begin{array}{rccc} f: & (\mathbb{Z}_{85})^k & \to & (\mathbb{Z}_{85})^k \\ & \underline{z} & \mapsto & \underline{z} \cdot C \end{array}$$

siendo C una matriz en $\mathbb{Z}_{85}$, cuadrada de orden k y con inversa. La matriz C es la clave del cifrado de Hill.

Cifrado afin. En el caso del cifrado de afín, la función de cifrado es:

$$\begin{array}{rccc} f: & (\mathbb{Z}_{85})^k & \to & (\mathbb{Z}_{85})^k \\ & \underline{z} & \mapsto & \underline{z} \cdot C + \underline{x} \end{array}$$

siendo C una matriz en $\mathbb{Z}_{85}$, cuadrada de orden k, invertible y siendo $\underline{x}$ un vector (ó matriz fila) de $(\mathbb{Z}_{85})^k$. El par $(C, \underline{x})$ es la clave del cifrado afín.

El mensaje numérico cifrado es la concatenación del cifrado de los bloques.

4. Decodificación numérica: Una vez obtenida la lista del mensaje numérico cifrado, se realiza el proceso inverso al descrito para la codificación numérica.

PROBLEMA 1

Supongamos que un mensaje M escrito en el alfabeto *alf* lo ciframos con el cifrado de **Hill** de clave *clave_cif_1* (ver *entrada_datos_07.txt*). Sabiendo que el mensaje cifrado es el indicado en *texto_cifrado_1* (ver fichero de datos), obtener el mensaje M.

10 últimos simbolos de M

PROBLEMA 2

Supongamos que un mensaje M escrito en el alfabeto *alf* lo ciframos con el cifrado de **afín** de clave *clave_cif_2* (ver *entrada_datos_07.txt*). Sabiendo que el mensaje cifrado es el indicado en *texto_cifrado_2* (ver fichero de datos), obtener el mensaje M.

10 últimos simbolos de M