Práctica 2
Cifrado afín

Índice

Para entregar

- Carpeta "afin" con
  - El código de las funciones $cifafin()$, $decafin()$ completado.
  - Problemas de la sección 4 resueltos.

1. Introducción

En esta práctica programaremos funciones de cifrado y descifrado empleando transformaciones afines. Para ello necesitaremos utilizar algunos de los algoritmos programados anteriormente.

2. Cifrado afín

La función de cifrado afín es

$$C = f(M) \equiv aM + b \mod N^k,$$

donde N es la longitud del alfabeto, k es el número de letras de cada bloque en que queda dividido el mensaje, M es el equivalente numérico del mensaje en claro y C el del mensaje cifrado.

La clave de cifrado es (a, b). Debe ser $\text{mcd}(a, N) = 1$.

- Programar una función ($cifafin()$) que admita como entradas un alfabeto, un mensaje en claro y números enteros k, a, b, y devuelva como salida un mensaje cifrado con una transformación afín sobre k-gramas con clave (a, b).

  Los pasos que habrá que seguir son:

  - Convertir el mensaje en números con la función $men2num()$.
  - Cifrar.
  - Convertir los números resultantes en mensaje con la función $num2men()$.

EJERCICIO. Dado un alfabeto de 27 caracteres (con " "=26) usar una transformación afín sobre trigramas ($k = 3$) con clave $a = 13$, $b = 9$ para cifrar el mensaje: "ENVIAME LA CLAVE".
Solución: "ERMXGDKTRMPIIKMK X"

3. Descifrado afín

La función de descifrado afín es la inversa de la función anterior:

$$M = f^{-1}(C) = a'C + b' \mod N^k,$$

donde N es la longitud del alfabeto, k es el número de letras de cada bloque en que queda dividido el mensaje, M es el equivalente numérico del mensaje en claro y C el del mensaje cifrado.

Si la clave de cifrado es (a, b) con $\mathrm{mcd}(a, N) = 1$, la clave de descifrado es

$$a' = a^{-1} \mod N^k, \quad b' = -a^{-1}b \mod N^k.$$

- Programar una función ($decafin()$) que admita como entradas un alfabeto, un criptograma y números enteros k, a, b, y devuelva como salida un mensaje en claro sabiendo que ha sido cifrado con una transformación afín sobre k-gramas con clave (a, b).

  Pasos a seguir:

  - Obtener la clave de descifrado.
  - Cifrar el criptograma con la función $cifafin()$ utilizando la clave de descifrado.

EJERCICIO. Dado un alfabeto de 27 caracteres (con " "=26) descifrar los criptogramas "ERMXGDKTRMPIIKMK X" y "GKXIMXERMZKXLRHR X" sabiendo que han sido cifrados con una transformación afín sobre trigramas ($k = 3$) con clave $a = 13$, $b = 9$.
Solución: "ENVIAME LA CLAVE "; "TE LA ENVIE AYER "

4. Problemas

Como de costumbre, hay que escribir la solución en el fichero "problemasafin.R", comentando los pasos necesarios para la resolución del problema. A modo de ejemplo, el primer problema está resuelto.

1. En un texto largo, que ha sido cifrado con una transformación afín usando el alfabeto de 26 letras y partiendo los mensajes en bloques de una letra, observamos que las letras más frecuentes son "D" y "L", en ese orden. Suponiendo que estas dos letras corresponden al cifrado de "E" y "A", respectivamente, descifrar el mensaje "CJKDHJYBDZXVSJ".

2. Interceptamos el mensaje "ELIX", que sabemos que ha sido cifrado con una transformación translación (transformación afín con clave $a = 1$, b) usando el alfabeto de 26 letras y partiendo el mensaje en bloques de una letra. Obtener la clave y descifrar el mensaje probando todas las claves posibles.

3. Estamos intentando criptoanalizar una transformación afín sobre un alfabeto de 37 caracteres. El alfabeto comprende los dígitos 0 a 9, las 26 letras "A"-"Z" y el espacio " ". Los números están etiquetados con ellos mismos (es decir, con los enteros 0 a 9), las letras con los enteros 10 a 35 y el espacio con 36. Los mensajes se dividen en bloques de una letra. Interceptamos el mensaje "D0PV4DS1DP22CPIVP DOVJVADMW 5P22Q" y sabemos que termina con la firma "007". Descifrar el mensaje.

4. En un texto largo, que ha sido cifrado con una transformación afín sobre digramas ($k = 2$) usando el alfabeto de 26 letras, observamos que los digramas más frecuentes son "AL" y "BQ", en ese orden. Supongamos que estos dos digramas corresponden al cifrado de "EN" y "DE", respectivamente (digramas más frecuentes en español),

   a) obtener las claves de cifrado y descifrado,

   b) descifrar: "ALIWVZHYTWRPKQWDAZHN",

   c) cifrar: "BUENTRABAJO".