Cifrado Payfair

Andoni Latorre Galarraga y Mariana Zaballa Bernabé

Cifrado

Utlizamos un bucle While Wend para recorrer el mensaje. La variable k es la posición del mensaje que vamos a leer. Dependiendo de si tenemos que introducir un caracter sin sentido ($\odot$) avanzamos k por 1 o por 2.

a_1	a_2	
letra	letra	$k \leftarrow k+2$
letra	$\odot$	$k \leftarrow k+1$

En la última posición nos aseguramos de aumentar el valor de k para que no se cumpla la condición $k \leq l$. Cuando ambas letras están en la misma fila/columna queremos sumar 1 módulo 5. Pero en vez de tener el resultado en $\{0,1,2,3,4\}$ lo queremos en $\{1,2,3,4,5\}$. Hemos logrado esto de la siguiente manera

$$(x \text{ Mod } 5)+1$$

Para cuando no comparten ni fila ni columna hemos hecho una observación,

	j_1	j_2
i_1	a_1	
i_2		a_2

, | | j_2 | j_1 |
|---|---|---|
| i_2 | a_2 | |
| i_1 | | a_1 |

$\Rightarrow sig(j_1-j_2)=sig(i_1-1_2) \Rightarrow (j_1-j_2)(i_1-i_2)>0$

	j_1	j_2
i_1		a_1
i_2	a_2	

, | | j_1 | j_2 |
|---|---|---|
| i_2 | | a_2 |
| i_1 | a_1 | |

$\Rightarrow sig(j_1-j_2)\neq sig(i_1-1_2) \Rightarrow (j_1-j_2)(i_1-i_2)<0$

Por eso utlizamos $(j_1-j_2)(i_1-i_2)>0$ como condición en el If. Calculamos b_1, b_2 como corresponde en cada caso

	j_1	j_2
i_1	a_1	b_1
i_2	b_2	a_2

, | | j_2 | j_1 |
|---|---|---|
| i_2 | a_2 | b_2 |
| i_1 | b_1 | a_1 |

$\Rightarrow b_1$ en (i_1, j_2) $\quad b_2$ en (i_2, j_1)

	j_1	j_2
i_1	b_2	a_1
i_2	a_2	b_1

, b_1 | | j_1 | j_2 |
|---|---|---|
| i_2 | b_1 | a_2 |
| i_1 | a_1 | b_2 |

$\Rightarrow b_1$ en (i_2, j_1) $\quad b_2$ en (i_1, j_2)

Descifrado

El código es basicamente el mismo con el cambio de restar 1 módulo 5 en vez de sumarlo y el cambio correspondiente al caso de fila y columna diferentes.

x	$((x+3) \text{ Mod } 5)+1$
1	5
2	1
3	2
4	3
5	4

La idea para esta fórmula ha venido de $-1 \equiv_5 4 = 3+1$.