Cifrados clásicos - I

Problemas de Criptología - Hoja 3

Curso 07-08

1 **Composición de claves**. Estudia la composición consecutiva de cifrados con distintas claves en los cifrados de desplazamiento, afín y de sustitución desde el punto de vista del criptoanálisis.

2 **Cifrado de desplazamiento.** Mediante un cifrado de desplazamiento de 13 posiciones cifra la frase *Siempre que enseñes, enseña a la vez a dudar de lo que enseñas*.

3 **Criptoanálisis de un cifrado de desplazamiento**. Descifra, sin recurrir a la exploración exhaustiva del espacio de claves, el siguiente mensaje usando un análisis de frecuencias. Se sabe que el mensaje está cifrado con un cifrado de desplazamiento y que el texto está escrito en español.

```
CRZDRXZERTZGETGEKMVCRRCGKYGDSJVKUVCGIMV
EGHMVUVEKVJVCYMDGJCGKTGEKMVCRUVCGIMVKGE
```

Se proporciona la siguiente tabla de frecuencias de las letras del criptograma:

G, V	C	E, K	R, M	T, U, Z, D, J	Y, I	S, X, H
11	8	7	6	3	2	1

El número total de letras es 78.

4 **Criptoanálisis de un cifrado afín**. Descifra, sin usar fuerza bruta, el siguiente mensaje usando un análisis de frecuencias. Se sabe que el mensaje está cifrado con un cifrado afín y que el texto está escrito en español.

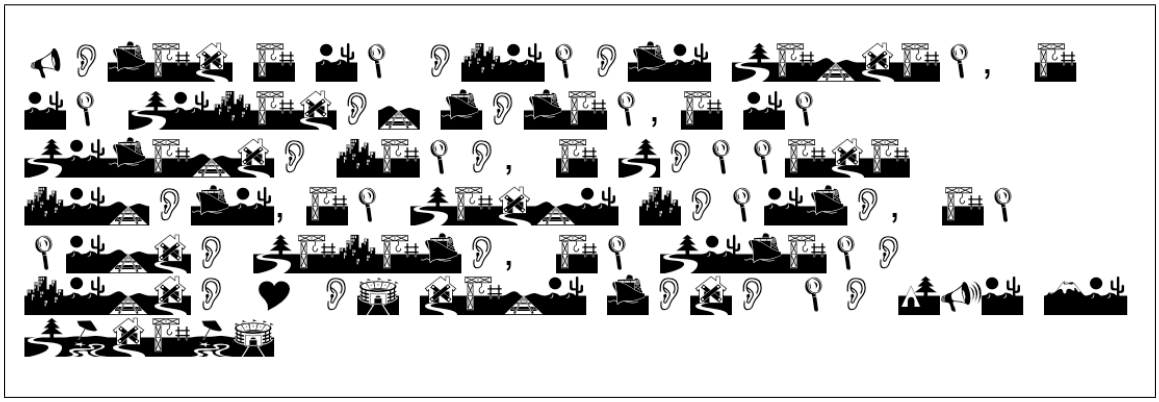
```
FVÑXOXAAKOCHUHCXANXPXOVOCÑHPHTHTÑRXPLHNXAXOCÑHTH
CHERÑKNXVOHUXFVXZHAXSVPÑNHNLPHOAÑLKPÑHOKAKOEXPXCXNKPXA
OÑNXTHTÑRXPLHNOÑNXTHAXSVPÑNHN
```

Se da la siguiente tabla de frecuencias de las letras del criptograma:

El número total de letras es 131.

X	H	Ñ	O, N	P	A	C, T, K, V	L	R	S, U, F, E	Z
20	18	12	11	10	9	6	4	3	2	1

5 **Cifrados de sustitución y de permutación.** El señor Pato, director de la Escuela de Estudios Informáticos Avanzados de La Granja (Segovia), convoca elecciones. Se vuelve a presentar y la oposición, que critica su gestión por corrupta, sospecha que ha comprado a la delegación de alumnos para ganar las elecciones. El señor Pato, de extraño e ilustre apellido Lerda Celo, manda un mensaje cifrado a la señorita Cordera, una ídem de rizo platero a la sazón delegada de la escuela, pero este mensaje es interceptado por el siempre vigilante señor Salva Dore (un fino gallo italiano), el líder de la oposición. El criptograma está más abajo. ¿Podrá probar la oposición que el señor Pato ha comprado a delegación de alumnos? ¿Y tú?



Por ironías de la vida, la señorita Cordera, que no sabe de quién procede el mensaje exactamente, fue capaz de descifrarlo, pero no acierta a comprender su significado. Finalmente, siguiendo órdenes de la señorita Cordera, los alumnos se abstienen en la votación y se va a una segunda vuelta. El señor Pato está furioso. ¿Puedes precisar qué no supo desentrañar la señorita Cordera en el mensaje?

6 **Permutaciones.** Consideremos la siguiente permutación π.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 9 & 10 & 1 & 8 & 7 & 6 & 3 & 4 \end{pmatrix}$$

(a) Calcula $\pi(5), \pi(9), \pi^{-1}(8)$ y $\pi^{-1}(9)$.

(b) Descompón π en ciclos.

(c) Calcula $\pi \circ \pi$ y $\pi^{-1} \circ \pi^{-1}$.

7 **Cifrados de permutación.** Descifra los siguientes criptogramas sabiendo que el primer fue cifrado por permutación sin clave y el segundo, con clave:

ANCNIYEOELDITSANEYLEOEOLQSEAFNLRGUTADUAEHUEADONUVAINLO

NYEANOCIETANLDEISYELQLESOOELGUAFTNRAEUEDUAAHDVINONLUAO

8 **Cifrados de sustitución polialfabéticos.** El siguiente criptograma ha sido cifrado con un cifrado polialfabético con clave. Se sabe que la primera palabra del texto claro es *muchos*. Descifra el criptograma mediante un ataque de texto claro conocido.

AMFLBHYDFEWRPEGGMPDCÑISOJDONHREMPJJLEFWERWQ
VMEMQGRPGESZGSNOKXJUQZHQGSDHQGSKDFUDK

9 **Cifrados sobre el código ASCII.** Describe cómo se definirían los cifrados de este tema si el alfabeto base es el código ASCII.