Laboratorio **17/2/14**

Segundo parcial

Apellidos _____ Nombre _____

Consideramos el siguiente sistema criptográfico (la clave de encriptado es k):

- El código del primer carácter de la cadena encriptada se obtiene sumando k (módulo la longitud del alfabeto) al código del primer carácter de la cadena original.
- El carácter i-ésimo ($i > 1$) de la cadena encriptada es aquel cuyo código es la suma (módulo la longitud del alfabeto) de los códigos de los caracteres i-ésimo e $(i-1)$-ésimo de la cadena original.

1. Escribir una función Sage, `cifrado1SegundoParcial(texto,clave,alfabeto)`, que espere un `texto`, una `clave` y un `alfabeto`, y devuelva el resultado de encriptar `texto` por medio del esquema que acabamos de describir con clave $k =$ `clave` usando el alfabeto `alfabeto`. La función usará por defecto el alfabeto

```
alfabeto=u' ABCDEFGHIJKLMNÑOPQRSTUVWXYZabcdefghijklmnñopqrstuvwxyz'
```

que tiene un espacio en blanco como primer caracter.

2. Escribir una función Sage, `descifrado1SegundoParcial(texto,clave,alfabeto)`, que espere un `texto` resultado de encriptar un mensaje por medio del esquema descrito con una `clave` y un `alfabeto`, y que devuelva el mensaje desencriptado. Por defecto usará el alfabeto mencionado anteriormente.

3. Consideramos la siguiente variante del esquema descrito, con clave de encriptado k:

- El código del primer carácter de la cadena encriptada se obtiene sumando k (módulo la longitud del alfabeto) al código del primer carácter de la cadena original.
- Los caracteres de la cadena encriptada que ocupan una posición j entre 2 y la clave k son aquellos cuyo código es la suma (módulo la longitud del alfabeto) de los códigos de los caracteres de la cadena original que ocupan posiciones menores o iguales que j.
- Los caracteres de la cadena encriptada que ocupan una posición j mayor que la clave k son aquellos cuyo código es la suma (módulo la longitud del alfabeto) de los códigos de los caracteres de la cadena original que ocupan posiciones entre $j-(k-1)$ y j (en total se toman en cuenta k posiciones).

Escribir dos funciones de Sage, de nombres `cifrado2SegundoParcial(texto,clave,alfabeto)` y `descifrado2SegundoParcial(texto,clave,alfabeto)`, que, respectivamente, cifren y descifren textos de acuerdo con este esquema.