Informática. Práctica 2

Facultad de Matemáticas
Universidad Complutense de Madrid
Curso 2017-2018

Sistemas de cifrado

Un sistema de cifrado es aquel sistema que permite que un emisor y un receptor intercambien información confidencialmente. El emisor proporciona el mensaje original (o mensaje en claro) para que el algoritmo de cifrado lo transforme en un mensaje cifrado (o criptograma), mediante el uso de una clave. El criptograma se envía a través de un canal público y entonces el receptor, que conoce la clave, lo transforma en el mensaje original con la ayuda del algoritmo de descifrado.

A continuación, se describen dos sistemas clásicos de cifrado, cuyos algoritmos de cifrado y descifrado debes implementar en Python.

Cifrado de Atbash

El cifrado de Atbash o encriptación hebrea fue un sistema utilizado por los hebreos del año 600 a.C. y se usó en el Libro de Jeremías[1] para ocultar la palabra `Babilonia`, cuyo criptograma era `Sesac`. Este es un cifrado por sustitución monoalfabética, es decir, cada carácter del mensaje original es sustituido por otro del mismo alfabeto.

El método de cifrado consiste en sustituir la primera letra del alfabeto por la última, la segunda letra por la penúltima, la tercera letra por la antepenúltima y así sucesivamente con todo el alfabeto. El método de descrifrado consiste en cifrar de nuevo el criptograma.

Ejemplo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Mensaje en claro: `LAS EDADES DEL HOMBRE.`
Criptograma: `OZH VWZWVH WVO SLNYIV.`

Cifrado por transposición simple

La transposición simple realiza un cifrado por transposición, que modifica la posición de los caracteres del mensaje original de forma que el criptograma contiene los mismos caracteres, pero resulta incomprensible a simple vista ya que estos están desordenados.

El método de cifrado consiste en reescribir el mensaje original en dos líneas, de forma que los caracteres impares aparecen en la primera línea y los caracteres pares aparecen en la segunda línea. El criptograma se obtiene concatenando ambas líneas.

El método de descifrado consiste en dividir el criptograma en dos fragmentos de la misma longitud (si la longitud total del criptograma es impar, el primer fragmento tendrá un carácter más que el segundo). Cada fragmento se escribe en una línea. El mensaje en claro se obtiene tomando los caracteres de ambas líneas de manera alterna.

Ejemplo:

Mensaje en claro: `LAS EDADES DEL HOMBRE`

Línea 1:

L	S	E	A	E	_	E	_	O	B	E

Línea 2:

A	_	D	D	S	D	L	H	M	R

Criptograma: `LSEAE E OBEA DDSDLHMR.`

¿Qué debes hacer?

Debes diseñar y escribir en Python las cuatro funciones siguientes:

1. `coder_atbash(message)`: El parámetro `message` es una cadena de caracteres que contiene un mensaje en claro. Devuelve otra cadena de caracteres que contiene el criptograma correspondiente obtenido mediante el cifrado de Atbash.
2. `decoder_atbash(cryptogram)`: El parámetro `cryptogram` es una cadena de caracteres que contiene un criptograma. Devuelve otra cadena de caracteres que contiene el mensaje original correspondiente obtenido mediante el descifrado de Atbash.

[1] El Libro de Jeremías es uno de los libros del Antiguo Testamento. Fue escrito por el Profeta Jeremías entre los años 630 y 580 a.C. y registra las últimas profecías al pueblo de Judá.

3. `coder_transposition(message)`: El parámetro `message` es una cadena de caracteres que contiene un mensaje en claro. Devuelve otra cadena de caracteres que contiene el criptograma correspondiente obtenido mediante el cifrado por transposición simple.
4. `decoder_transposition(cryptogram)`: El parámetro `cryptogram` es una cadena de caracteres que contiene un criptograma. Devuelve otra cadena de caracteres que contiene el mensaje original correspondiente obtenido mediante el descifrado por transposición simple.

Observación: En el cifrado de Atbash, el alfabeto considerado es el compuesto por los caracteres `c` tales que `(ord('a')`$\leq$`ord(c)`$\leq$`ord('z'))` $\vee$ `(ord('A')`$\leq$`ord(c)`$\leq$`ord('Z'))`.