Universidad Nacional Autónoma de México
Facultad de Ciencias

Criptografía y Seguridad

Tarea Moral 1

García Ponce José Camilo - 319210536

1. Texto descifrado (y con espacios correctos)
   la historia de todas las sociedades hasta nuestros dias es la historia de las luchas de clases hombres libres y esclavos patricios y plebeyos senores y siervos maestros y oficiales en una palabra opresores y oprimidos se enfrentaron siempre mantuvieron una lucha constante velada unas veces y otras franca y abierta lucha que termino siempre con la transformacion revolucionaria de toda la sociedad o el hundimiento de las clases en pugna en las anteriores epocas historicas encontramos casi por todas partes una completa diferenciacion de la sociedad en diversos estamentos una multiple escala gradual de condiciones sociales en la antigua roma hallamos patricios plebeyos y esclavos en la edad media senores feudales vasallos maestros oficiales y siervos y ademas en casi todas estas clases todavia encontramos gradaciones especiales

2. Alfabeto usado

   Alfabeto del texto cifrado

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
b	q	l	-	-	h	o	m	i	r	a	d	e	n	s	t	u	c	p	v	-	-	y	f	g	-

   Alfabeto del texto descifrado

3. Código usado
   El código usado para resolver este ejercicio se encuentra en el archivo version2.py, los otros archivos importantes son criptograma_1.txt (donde venia el texto cifrado) y spanish_words_limpio.txt (texto con varias palabras del Español).
   En version2.py esta todo el código usado, se usaron los módulos random (para generar números aleatorios) y collections (para usar Counter). Los métodos usados fueron: método para calcular las frecuencias de letras en el texto cifrado, método para crear un mapeo (alfabeto?) aleatorio usando las frecuencias del texto cifrado y las frecuencias de palabras del Español, método para sustituir letras en el texto cifrado usando un mapeo, método para verificar si el texto sustituido contiene palabras de cierta longitud usando un diccionario de palabras y método para generar el diccionario usando un archivo.
   En criptografia.py hay funciones útiles (las que vimos en clase) como mdc, obtener un inverso y Euclides, son de gran ayuda para obtener funciones de alfabetos.

4. Anotaciones y proceso de resolver
   Para resolver el ejercicio se empezó primero generando diferentes mapeos e intentando encontrar una palabra de longitud 8, como la lista de palabras en Español son de Español de España, entonces algunas palabras que encontramos no se tomaron en cuenta. Así se siguió hasta encontrar la palabra “constante“, luego se modifico el mapeo inicial usando la palabra encontrada como guía (R:c, G:o, N:n, O:s, P:t, K:a, M:e). Después se buscaron dos palabras de longitud 8 (que tuvieran algo de sentido), encontrando la palabra “anterior“, se volvió a modificar el mapeo inicial para tomar en cuenta esta palabra. Luego se pudo notar la palabra “historia“ al inicio del texto debido a que se tenia “`_istoria`“ y también la palabra “la“, debido a que al inicio se tenia “`_a`“, por lo tanto se modifico el mapeo inicial otra vez. Después se buscaron cuatro o más palabras de longitud 8, hasta encontrar la palabra “patricio“ (lo cual fue algo sorprendente y cómico), se volvió a modificar el mapeo inicial. Luego se buscaron palabras de longitud 9 y se encontró “oficiales“. Más tarde, se pudieron deducir las palabras “de“ (al ver “`_e`“), “nuestros“ (al ver “`n_estros`“), “hombres libres“ (al ver “`ho__res li_res`“), “y“ (al ver “`patricios_plebe_os`“) y “esclavos“ (al ver “`escla__os`“), todos estos descubrimientos fueron posibles por revisar el texto sustituido hasta el momento y por algo del contexto de las palabras encontradas antes, se volvió

a modificar el mapeo inicial para tomar en cuenta las nueva palabras encontradas. Después se ordeno el mapeo obtenido hasta el momento y se noto que las únicas letras en el texto cifrado que faltaban por descifrar eran B, D, E, U, V, Y y Z. Las letras D, E, U, V y Z se ignoraron, ya que no aparecen en el texto cifrado. Para B se observo que era q por "`lucha_uetermino`" y para Y se observo que era g por "`anti_ua roma`". Se modifico el mapeo por ultima vez, se sustituyo el texto cifrado y se obtuvo el texto descifrado, revisándolo para que todo estuviera en orden y por ultimo se realizo el alfabeto en una tablita.
Posiblemente lo que se pudo hacer mejor es que la primera palabra usada para modificar el mapeo inicial fuera una que apareciera dos veces en el texto, pero no se hizo esto en el proceso, posiblemente fue algo de suerte encontrar una palabra que si apareciera en el texto descifrado.