Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Tarea Moral 3

García Ponce José Camilo - 319210536

1. Texto descifrado (y con espacios correctos)
   generalmente la mejor politica en la guerra es tomar un estado intacto arruinarlo es inferior capturar el ejercito enemigo entero es mejor que destruirlo tomar intacto un regimiento una compania o un escuadron es mejor que destruirlo conseguir cien victorias en cien batallas no es la medida de la habilidad someter al enemigo sin luchar es la suprema excelencia de este modo lo que es de maxima importancia en la guerra es atacar la estrategia del enemigo lo segundo mejor es romper sus alianzas mediante la diplomacia en tercer lugar viene atacar a su ejercito y la peor de todas las estrategias es atacar ciudades atacar ciudades es algo que solo ha de hacerse cuando no hay ninguna otra alternativa ya que la preparacion de escudos y su transporte y tener preparadas las armas y el equipo necesario requiere al menos tres meses y montar las maquinas de asedio y las escalas para asaltar las murallas requiere otros tres meses adicional es el general incapaz de controlar su impaciencia ordenara a las tropas cargar contra las murallas con el resultado de que un tercio de ellas perecera sin haber tomado la ciudad asi de calamitoso es atacar ciudades asi pues los verdaderamente habiles en la guerra someten al ejercito enemigo sin batallar capturan las ciudades enemigas sin asaltarlas y se apoderan del estado enemigo sin campanas prolongadas su meta es tomar intacto todo cuanto hay bajo el cielo mediante consideraciones estrategicas como resultado sus tropas no se desgastaran y las ganancias seran completas este es el arte de la estrategia ofensiva en consecuencia el arte de usar tropas es este si se es diez veces superior al enemigo rodeadle si se es cinco veces mas fuerte atacadle si se tiene el doble de fuerzas dididle si se esta a la par superadle mediante un buen plan si se esta en inferioridad numerica sed capaces de mantener abierta una via de retirada y si se esta en desventaja en todos los aspectos sed capaces de eludirle pues una fuerza pequena no es nada excepto botin para una mas poderosa si se enfrenta a ella temerariamente el general es el asistente del soberano del estado si esta asistencia es estrecha el estado sera fuerte sin duda si es debil el estado sera ciertamente debil

2. Clave usada
   SUNTZARTEG

3. Código usado
   El código usado para resolver este ejercicio se encuentra en el archivo version1.py, los otros archivos importantes son criptograma_2.txt (ahí está el texto cifrado), criptograma_2_b.txt (ahí está el texto descifrado), criptograma_2_bonita.txt (ahí está el texto descifrado con espacios entre las palabras), criptograma_2_d.txt (ahí está el texto cifrado divido en fragmentos de longitud 10), criptograma_2_s.txt (ahí está el texto cifrado sin espacios y saltos de linea) y pasos.txt (los pasos seguidos para descifrar el texto).
   En version1.py esta todo el código usado, se uso el módulo collections (para usar Counter). Los métodos usados fueron: método para limpiar un texto de espacios y saltos de linea, método para calcular el índice de coincidencia de un texto dado un alfabeto, método para leer un archivo, método para encontrar cadenas repetidas (de cierta longitud mínima) y las posiciones de donde aparecen, método para calcular la distancia entre las cadenas repetidas, método para calcular factores primos de un numero, método para obtener factores primos de las distancias entre cadenas repetidas, método para dividir un texto en fragmentos de una longitud dada, método para obtener la frecuencia de las letras de un texto, método para obtener la frecuencia de las letras en una posición de los fragmentos de texto, método para volver letras a números, método para volver números en letras y método para descifrar un texto usando una clave, una tabla de Vigenere y un alfabeto.

4. Anotaciones y proceso de resolver
   Para resolver el ejercicio primero quitamos los espacios y saltos de linea del texto cifrado. Luego sacamos el índice de coincidencia del texto cifrado (que es 0.04176713979567001) y con este índice de coincidencia usamos la tablita vista en clase para notar que la clave debe usar 8 o 9 letras distintas (8 o 9 alfabetos). Después empezamos a buscar secuencias de caracteres que se repitan varias veces en el texto (usamos secuencias de al menos 7 en

longitud, esto debido a que si usamos longitud 6 mínima al calcular los factores de las distancias nos salían cosas raras). Posteriormente calculamos las distancias entre las secuencias encontradas y con esas distancias les sacamos sus factores primos encontrando que los números 2 y 5 aparecían en todos, por lo tanto pensamos que la longitud de la cadena es 10. Luego dividimos el texto cifrado en fragmentos de longitud 10. Después revisamos la frecuencia de cada letra en la posición 0 de los fragmentes, obteniendo que las letras que más aparecían son W y S, por lo tanto usando la tablita de Vigenere buscamos una letra tal que al usarla como llave y codificar a las letras a o e (ya que son las que más aparecen en el Español) nos den las letras W y S, obteniendo a la clave S, por lo tanto el primer carácter de la clave sera S, este proceso lo repetimos con las otras 9 posiciones de la clave. Obtuvimos algo así para cada posición:

- S en la posición 0, ya que las letras que aparecen más son W y S, en la tabla de Vigenere tenemos que [S][a]= S y [S][e]= W
- U en la posición 1, ya que las letras que aparecen más fueron Y y U, en la tabla de Vigenere tenemos que [U][a]= U y [U][e]= Y
- N en la posición 2, ya que las letras que aparecen más fueron N, F y R, en la tabla de Vigenere tenemos que [N][a]= N y [N][e]= R, en este caso no logramos que las letras N y F coincidieran en una clave, por lo cual usamos la tercer letra que aparece más
- T en la posición 3, ya que las letras que aparecen más fueron T y X, en la tabla de Vigenere tenemos que [T][a]= T y [T][e]= X
- Z en la posición 4, ya que las letras que aparecen más fueron Z, Q y D, en la tabla de Vigenere tenemos que [Z][a]= Z y [Z][e]= D, en este caso no logramos que las letras Z y Q coincidieran en una clave, por lo cual usamos la tercer letra que aparece más
- A en la posición 5, ya que las letras que aparecen más fueron A y E, en la tabla de Vigenere tenemos que [A][a]= A y [A][e]= E
- R en la posición 6, ya que las letras que aparecen más fueron V y R, en la tabla de Vigenere tenemos que [R][a]= R y [R][e]= V
- T en la posición 7, ya que las letras que aparecen más fueron X, L y T, en la tabla de Vigenere tenemos que [T][a]= T y [T][e]= X, en este caso no logramos que las letras X y L coincidieran en una clave, por lo cual usamos la tercer letra que aparece más
- E en la posición 8, ya que las letras que aparecen más fueron V y R, en la tabla de Vigenere tenemos que [E][a]= E y [E][e]= I
- G en la posición 9, ya que las letras que aparecen más fueron K y G, en la tabla de Vigenere tenemos que [G][a]= G y [G][e]= K

Por lo tanto la clave es SUNTZARTEG, notamos que la clave tiene 10 caracteres de longitud y 9 letras distintas por lo tanto nuestro análisis fue útil y correcto. Y para finalizar usamos la clave encontrada para descifrar el texto.
Solo queda notar que encontramos las siguientes palabras(?): rodeadle, atacadle, divididle, superadle y sed, las cuales no estamos muy seguros de ¿por qué aparecen?, tal vez el texto es de Español de España o algo salio extraño debido a que el resto del texto tiene mucho sentido luego de descifrarlo.