Criptografía y Seguridad
Práctica 3

Ángela Janín Ángeles Martínez Ailyn Rebollar Pérez

Desarrollo

Para resolver la práctica acudimos a diferentes medios los cuales se especifican en cada ejercicio:

1. **One.txt**

   El criptotexto en éste archivo fue cifrado con el método de Vigenère donde la llave es la palabra **infante** y el texto claro es:

   "Pasaste a mi lado con gran indiferencia tus ojos ni siquiera voltearon hacia mi te vi sin que me vieras te hable sin que me oyeras y toda mi amargura se ahogó dentro de mi me duele hasta la vida saber que me olvidaste pensar que ni desprecios merezca yo de ti y sin embargo sigues unida a mi existencia y si vivo cien años cien años pienso en ti"

   Que es un fragmento de la canción 100 años de Pedro Infante. Nos apoyamos en la siguiente página para decifrar el texto:

   https://www.boxentriq.com/code-breaking/vigenere-cipher

   Sin embargo, sucedió algo raro, lo decifró por partes ya que nos decía que había dos palabras clave que eran infante y einfant, pero notamos que esto sucedió por la ó en la palabra ahogó, porque la página no supo cómo decifrarla y buscó alguna otra palabra para decifrar por lo que trató de decifrarlo con einfant que era lo que seguía para decifrar lo que faltaba del texto.

2. **Two.txt**:

   Este criptotexto estaba cifrado con Caesar, donde la llave es **9** y el mensaje en claro es un extracto de la obra de Sor Juana Inés de la Cruz "Hombres necios que acusáis":

   Hombres necios que acusáis a la mujer sin razón sin ver que sois la ocasión de lo mismo que culpáis si con ansia sin igual solicitáis su desdén por qué queréis que obren bien si las incitáis al mal

   Logramos decifrar el criptotexto apoyándonos de la siguiente página en internet:

   http://ccat.sas.upenn.edu/romance/spanish/219/07colonial/sorjuanahombresnecios.html

3. **Three.txt**:

   Éste criptotexto estaba cifrado con Afín, donde la llave es **(10,20)** y el mensaje en claro es:

   "En algún lugar de la mancha de cuyo nombre no quiero acordarme no ha mucho tiempo que vivía un hidalgo de los lanza en astillero adarga antigua rocin flaco y galgo corredor"

Que es un fragmento del primer capítulo de Don Quijote de La Mancha. Logramos decifrar el criptotexto apoyándonos de la siguiente página en internet:

https://www.boxentriq.com/code-breaking/affine-cipher

Y para comprobar utilizamos el archivo de nuestra práctica 2 affine_cipher.py, donde nos dio el mismo texto.

4. **Four.txt**

Éste archivo estaba cifrado con el método de Hill donde la llave es la matriz:

$$\begin{pmatrix} 5 & 25 \\ 7 & 2 \end{pmatrix} = \begin{pmatrix} f & z \\ h & c \end{pmatrix}$$

Y el mensaje en claro es

"LA HIPOTESIS ATOMICA EL CONCEPTO DEL ATOMO EN LA FOMA QUE FUERA ACEPTADO POR LOS CIENTIFICOS DESDE MIL SEISCIENTOS HASTA MIL NOVECIENTOS SE BASO EN LAS IDEAS DE FILOSOFOS GRIEGOS DEL SIGLO V AC FUERON LEUCIPPO DEMILETO Y SU DISCIPULO DEMOCRITO DE ABDERA QUIENES ORIGINARON LA FILOSOFIA ATOMICA INTRODUCIENDO LA NOCION DE UN CONSTITUYENTE ULTIMO DE LA MATERIA QUE DE NOMINARON ATOMO ES DECIR INDIVISIBLE EN LA LENGUA GRIEGA DEMOCRITO CREIA QU LOS ATOMOS ERAN UNIFORMES SOLIDOS DUROS INCOMPRESIBLES E INDESTRUCTIBLES Y QUE SE MOVIAN EN NUMERO INFINITO POR EL ESPACIO VACIO SEGUN SUS IDEAS LAS DIFERENCIAS DE FORMA Y TAMANO DE LOS ATOMOS DETERMINABAN LAS PROPIEDADES DE LA MATERIA ESTAS ESPECULACIONES FUERON LUEGO CONTINUADAS POR EPICURODESAMOS SI BIEN LA TEORIA ATOMICA GRIEGA ES SIGNIFICATIVA DEL PUNTO DE VISTA HISTORICO Y FILOSOFICO CARECE DE VALOR CIENTIFICO PUES NO SE FUNDA EN OBSERVACIONES DE LA NATURALEZA NI EN MEDICIONES PRUEBAS Y EXPERIMENTOS PARA LOS GRIEGOS LA CIENCIA CONSTITUIA TAN SOLO UN ASPECTO DE SU SISTEMA FILOSOFICO MEDIANTE EL CUAL BUSCABAN UNA TEORIA GENERAL QUE EXPLICARA EL UNIVERSO CON ESTE FIN ELLOS USABAN CASI EXCLUSIVAMENTE LA MATEMATICA Y EL RAZONAMIENTO CUANDO HABLAN DE LA FISICA FUE ASI QUE PLATON Y ARISTOTELES ATACARON LA TEORIA ATOMICAS OBREBAS ES FILOSOFICAS Y NO CIENTIFICAS EN EFECTO MI ENTRA A DEMOCRITO CREIA QUE LA MATERIA NO SE PODIA MOVER EN EL ESPACIO SIN EL VACIO Y QUE LA LUZ CONSISTIA DEL RAPIDO MOVIMIENTO DE PARTICULAS ATRAVES DEL VASIO PLATON RECHAZABA LA IDEA QUE ATRIBUTOS COMO BONDADO BELLEZA FUERAN SIMPLEMENTE MANIFESTACIONES MECANICAS DE ATOMOS MATERIALES DEL MISMO MODO ARISTOTELES NO ACEPTABA LA EXISTENCIA DEL VACIO PUES NO PODIA CONCEBIR QUE LOS CUERPOS CAYERAN CON IGUAL RAPIDEZ EN UN VACIO EL PUNTO DE VISTA ARISTOTELICO PREVALECIO EN LA EUROPA MEDIEVAL Y LA CIENCIA DE LOS TEOLOGOS CRISTIANOS SE BASO EN LA REVELACION Y LA RAZON MOTIVO POR EL CUAL LAS IDEAS DE DEMOCRITO FUERON REPUDIADAS POR CONSIDERARSE LAS MATERIALISTAS YATEAS"

Y logramos decifrarlo planteando un sistema de ecuaciones a partir de las pistas o hints que venían al final del archivo que nos decía parte del texto en claro y parte del texto cifrado.

NN XR HP ZH VT HM GS MI XG JY OY HM DK OE
NA TU RA LE ZA AT OM IC AD EL AM AT ER IA

Y para que el sistema de ecuaciones fuera más sencillo nos tomamos diptongos donde la letra A apareciera al inicio y al final porque sabemos que su índice corresponde al 0, de esa forma se elimina una de las variables en cada ecuación. Los diptongos que nos tomamos fueron:

- ZA - VT que nos da :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 25 \\ 0 \end{pmatrix} (\text{mód } 26) = \begin{pmatrix} 21 \\ 19 \end{pmatrix}$$

(25a + 0b) mód 26 = 21
(25c + 0d) mód 26 = 19
donde a = 5 y c = 7

- AM - OY que nos da:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix} (\text{mód } 26) = \begin{pmatrix} 14 \\ 24 \end{pmatrix}$$

(0a + 12b) mód 26 = 14
(0c + 12d) mód 26 = 24
donde b = 25 y d = 2

Finalmente lo que hicimos fue ocupar el archivo hill.py que se entregó en la práctica 2 para decifrar el criptotexto.

5. **Five.txt**
Éste criptotexto fue cifrado con código Morse, donde cada A es un punto, B es un - y cada punto es un espacio o separación de una palabra. Así que primero hicimos esa sustitución y luego nos apoyamos de una página de internet para decifrar el mensaje que es:

"NECESITAMOS UN MENSAJE QUE CONTENGA TODAS LAS LETRAS DEL ALFABETO COMO LA X EN XILOFONO LA K DE KOALA Y LA Z DE ZOOLOGICO Y LA"

La página que usamos fue:

https://www.boxentriq.com/code-breaking/morse-code