Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad

Práctica 3

Licón Colón Francisco Arturo
314222095

Molina Bis Victor Hugo
314311212

18 Mar 2020

Descifrados[1]

One.txt

Llave: INFANTE

Mensaje:
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

Procedimiento: El texto se cifró con Vigenere.
El texto se logró descifrar con la prueba de Kasiski.
Hay patrones como AUR(70,91), PM(76,97), YN(8,64,135), HX(74,95,222), EE(80,101,158), MZ(28,260). La mayoría tienen como factor al 7, por lo que se intuye que la longitud de la llave es 7.
Lo siguiente es separar el texto en renglones de longitud 7.

XNXAFNI
IYNLNWS
KBRGETQ
PZIIRXV
MZHINNY
ABÑOFGM
AUVUUXV
IITLGXE
ZBRHNVM
…

Después tomamos columna por columna y se contaron las ocurrencias de las letras.
Por ejemplo, las de la columna uno son
X: 2, I: 10, K: 2, P: 2, M: 7, A: 4, Z: 1, B: 1, G: 1, Ó: 1, H: 1, Y: 2, E: 1, V: 1, S: 1, W: 1, T: 1 .
Se supone que la I=E, por lo que la primera letra de la clave sería E, pero después de hacer varias combinaciones, se llegó a la conclusión de que la primer letra en realidad era la I.
Esto se realizó en cada columna hasta llegar a la palabra clave, INFANTE.

Herramienta: Vigenere.py

[1] Todos los archivos txt fueron probados con cada programa hecho, con el fin de determinar el cifrado al que pertenecía cada uno.

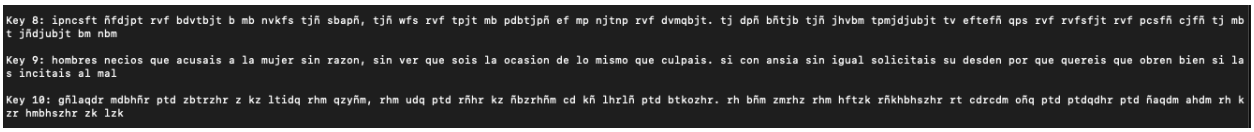
Two.txt

Llave: 9

Mensaje:

hombres necios que acusais a la mujer sin razon, sin ver que sois la ocasion de lo mismo que culpais. si con ansia sin igual solicitais su desden por que quereis que obren bien si las incitais al mal

Procedimiento: El texto se cifró con César.
El descifrado se logró por medio de un ataque por fuerza bruta, porque era el método más sencillo para lograr descifrar este texto. Al ya tener programado el descifrado, sólo era necesario iterar sobre cada elemento del alfabeto y así, poder conocer el texto correspondiente a cada llave, al final, restaba analizar cada texto y elegir el adecuado.



Herramienta: Caesar.py

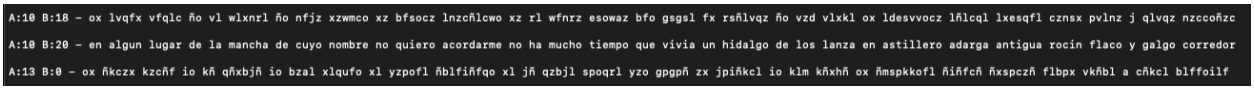
Three.txt

Llave: A:10 B:20

Mensaje:

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

Procedimiento: El texto se cifró con Affín.
El descifrado se logró por medio de un ataque por fuerza bruta. Analizando la forma en que se descifra el Affine, notamos que el valor de A es menor a 27 y el valor de B no es muy grande, por lo que analizar cada combinación no iba a resultar un gran problema; es por esto que se decidió descifrarlo por fuerza bruta.
Al ya tener programado el descifrado, sólo era necesario iterar sobre cada posible llave y así conocer el texto correspondiente a ella, al final, restaba analizar cada texto y elegir el adecuado. Como este trabajo iba a ser pesado, con ayuda de una biblioteca, la cual no acierta en muchas ocasiones, que analiza texto y devuelve el idioma en el que se encuentra, pudimos reducir el número de casos los cuales íbamos a analizar nosotros, lo que agilizó el proceso.



Herramienta: Affine.py

Four.txt

Llave: $\begin{bmatrix} 5 & 25 \\ 7 & 2 \end{bmatrix}$(FZHC)

Mensaje:
lahipotesisatomicaelconceptodelatomoenlafomaquefueraaceptadoporloscientificosdesdemilseiscientoshastamilnovecientossebasoenlasideasdefilosofosgriegosdelsiglovacfueronleucippodemiletoysudiscipulodemocritodeabderaquienesoriginaronlafilosofiaatomicaintroduciendolanociondeunconstituyenteultimodelamateriaquedenominaronatomoesdecirindivisibleenlalenguagriegademocritocreiaqulosatomoseranuniformessolidosdurosincompresibleseindestructiblesyquesemovianennumeroinfinitoporelespaciovaciosegunsusideaslasdiferenciasdeformaytamanodelosatomosdeterminabanlaspropiedadesdelamateriaestasespeculacionesfueronluegocontinuadasporepicurodesamossibienlateoriaatomicagriegaessignificativadelpuntodevistahistoricoyfilosoficocarecedevalorcientificopuesnosefundaenobservacionesdelanaturalezanienmedicionespruebasyexperimentosparalosgriegoslacienciaconstituiatansolounaspectodesusistemafilosoficomedianteelcualbuscabanunateoriageneralqueexplicaraeluniversoconestefinellosusabancasiexclusivamentelamatematicayelrazonamientocuandohablandelafisicafueasiqueplatonyaristotelesatacaronlateoriaatomicasobrebasesfilosoficasynocientificasenefectomientraademocritocreiaquelamaterianosepodiamoverenelespaciosinelvacioyquelaluzconsistiadelrapidomovimientodeparticulasatravesdelvasioplatonrechazabalaideaqueatributoscomobondadobellezafueransimplementemanifestacionesmecanicasdeatomosmaterialesdelmismomodoaristotelesnoaceptabalaexistenciadelvaciopuesnopodiaconcebirqueloscuerposcayeranconigualrapidezenunvacioelpuntodevistaaristotelicoprevalecioenlaeuropamedievalylacienciadelosteologoscristianossebasoenlarevelacionylarazonmotivoporelcuallasideasdedemocritofueronrepudiadasporconsiderarselasmaterialistasyateas

Procedimiento: El texto fue cifrado con Hill.
El descifrado se logró gracias al texto claro el cual fue brindado, ya que con los datos se pudo crear una ecuación, la cual con ayuda de una matriz y al aplicar el método de Gauss-Jordan permitía obtener la llave, en forma de matriz, que fue utilizada.[2]
Por las pistas dadas, las cuales estaba divididas en dos palabras, se dedujo que la matriz era de 2x2. Su matriz correspondiente es la siguiente[3]

[2] Ejemplo obtenido de http://mikelgarcialarragan.blogspot.com/2016/07/criptografia-xxiv-cifrado-de-hill-y.html

[3] La sección izquierda pertenece al texto claro y la derecha al cifrado.

$$\left[\begin{array}{cc|cc} 13 & 0 & 13 & 13 \\ 19 & 20 & 23 & 17 \\ 17 & 0 & 7 & 15 \\ 11 & 4 & 25 & 7 \\ 25 & 0 & 21 & 19 \\ 0 & 19 & 7 & 12 \\ 14 & 12 & 6 & 18 \\ 8 & 2 & 12 & 8 \\ 0 & 3 & 23 & 6 \\ 4 & 11 & 9 & 24 \\ 0 & 12 & 14 & 24 \\ 0 & 19 & 7 & 12 \\ 4 & 17 & 3 & 10 \\ 8 & 0 & 14 & 4 \end{array}\right]$$

Primero se intercambiaron la 1° fila con la 5° y la 2° con la 6°.

$$\left[\begin{array}{cc|cc} 25 & 0 & 21 & 19 \\ 0 & 19 & 7 & 12 \\ 17 & 0 & 7 & 15 \\ 11 & 4 & 25 & 7 \\ 13 & 0 & 13 & 13 \\ 19 & 20 & 23 & 17 \\ 14 & 12 & 6 & 18 \\ 8 & 2 & 12 & 8 \\ 0 & 3 & 23 & 6 \\ 4 & 11 & 9 & 24 \\ 0 & 12 & 14 & 24 \\ 0 & 19 & 7 & 12 \\ 4 & 17 & 3 & 10 \\ 8 & 0 & 14 & 4 \end{array}\right]$$

Se multiplico a la primer fila por el inverso multiplicativo modular de la primer columna (25) y la segunda por el inverso multiplicativo de la segunda columna (11), con esto se lograba obtener la matriz identidad.

$$\left[\begin{array}{cc|cc} 1 & 0 & 5 & 7 \\ 0 & 1 & 25 & 2 \\ 17 & 0 & 7 & 15 \\ 11 & 4 & 25 & 7 \\ 13 & 0 & 13 & 13 \\ 19 & 20 & 23 & 17 \\ 14 & 12 & 6 & 18 \\ 8 & 2 & 12 & 8 \\ 0 & 3 & 23 & 6 \\ 4 & 11 & 9 & 24 \\ 0 & 12 & 14 & 24 \\ 0 & 19 & 7 & 12 \\ 4 & 17 & 3 & 10 \\ 8 & 0 & 14 & 4 \end{array}\right]$$

Podemos notar que convertir las filas restantes en 0s no es problema, porque las que tengan inverso modular van a ayudarnos a eliminar el resto de las filas. Por lo tanto, nuestra solución es

$$\left[\begin{array}{cc|cc} 1 & 0 & 5 & 7 \\ 0 & 1 & 25 & 2 \end{array}\right]$$

Por lo que

$$K^T = \begin{bmatrix} 5 & 7 \\ 25 & 2 \end{bmatrix}$$

$$K = \begin{bmatrix} 5 & 25 \\ 7 & 2 \end{bmatrix}$$

Entonces la llave era FZHC.
Lo que restaba era ejecutar el programa escrito con los datos obtenidos.

Herramienta: hill.py y utils.py