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.
Patrones:
AUR (2) [70,91]
Distancias: 21

PM (2) [76,97]
Distancias: 21

YN (3) [8,64,134]
Distancias: 56,70

HX (3) [74,95,221]
Distancias: 21, 126

IU (4) [174,181,237,251]
Distancias: 7,56,14

En todos los casos las distancias tienen como factor común a 7, por lo que se tomará que el tamaño de la palabra clave es 7, obteniendo así lo siguiente:

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

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

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

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

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

Haciendo el conteo por columnas obtenemos las siguientes frecuencias.

{('X', 1), ('I', 6), ('K', 1), ('P', 3), ('M', 8), ('A', 5), ('Z', 2), ('B', 1), ('G', 1), ('L', 3), ('U', 5), ('W', 1), ('C', 1), ('D', 1)}
Esto sugiere que 'I' = E, 'M' = E.
Desplazamientos: E, I.

{('N', 4), ('Y', 5), ('B', 4), ('Z', 4), ('U', 5), ('I', 2), ('Q', 7),('G', 1), ('F', 3), ('X', 2), ('O', 2)}
Esto sugiere que 'Q' = E, 'U' = E, 'Y' = E.
Desplazamientos: N, Q, U.

{('X', 2), ('N', 8), ('R', 6), ('I', 2), ('H', 1), ('Ñ', 1), ('V', 1), ('T', 2), ('M', 1), ('D', 1), ('F', 4), ('J', 3), ('G', 1), ('E', 1), ('Y', 1), ('Q', 1), ('C', 1), ('A', 1), ('S', 1)}
Esto sugiere que 'N' = E, 'R' = E, 'F' = E, 'J' = E.
Desplazamientos: J, Ñ, B, F.

{('A', 4), ('L', 2), ('G', 2), ('I', 4), ('O', 5), ('U', 1), ('H', 2), ('T', 3), ('Q', 2), ('E', 4), ('D', 2), ('R', 2), ('M', 1), ('V', 1), ('C', 1), ('B', 1), ('Ñ', 1), ('S', 1)}
Esto sugiere que 'O' = E, 'I' = E, 'A' = E, 'E' = E.
Desplazamientos: L, E, W, A.

Las opciones que tienen cierto sentido son:
ENBL, ENBA, INBL, INBE, INBA, INFL, INFE, INFA.

{('F', 6), ('N', 8), ('E', 5), ('R', 1), ('U', 2), ('G', 1), ('Q', 3), ('H', 3), ('Ñ', 1), ('S', 1), ('T', 1), ('X', 1), ('D', 1), ('L', 2), ('O', 1), ('B', 2)}
Esto sugiere que 'N' = E, 'F' = E, 'E' = E, 'Q' = E, 'H' = E.
Desplazamientos: J, B, A, N, D.

Las opciones que tiene cierto sentido son:
ENBLA, INBAN, INFLA, INFAN.

{('N', 3), ('W', 3), ('T', 4), ('X', 7), ('G', 1), ('V', 2), ('O', 2), ('E', 1), ('F', 2), ('Ñ', 2), ('I', 2), ('M', 4), ('K', 1), ('J', 2), ('R', 1), ('L', 1), ('B', 1)}

Esto sugiere que 'X' = E, 'T' = E, 'M' = E.
Desplazamientos: T, P, I.

Las opciones que tienen cierto sentido son:
INFLAT, INFANT.

{('I', 7), ('S', 2), ('Q', 2), ('V', 4), ('Y', 3), ('M', 8), ('E', 2), ('P', 3), ('W', 3), ('K', 2), ('H', 1), ('X', 1), ('T', 1)}
Esto sugiere que 'M' = E, 'I' = E, 'V' = E.
Desplazamientos: I, E, R.

Las opciones que tienen cierto sentido son:
INFLATE, INFANTE.

Al probar las llaves, se llegó a la conclusión que la llave es INFANTE.

Herramienta: Vigenere.py

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.

```
Key 8: ipncsft ñfdjpt rvf bdvtbjt b mb nvkfs tjñ sbapñ, tjñ wfs rvf tpjt mb pdbtjpñ ef mp njtnp rvf dvmqbjt. tj dpñ bñtjb tjñ jhvbm tpmjdjubjt tv eftefñ qps rvf rvfsfjt rvf pcsfñ cjfñ tj mb t jñdjubjt bm nbm

Key 9: 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

Key 10: gñlaqdr mdbhñr ptd zbtrzhr z kz ltidq rhm qzyñm, rhm udq ptd rñhr kz ñbzrhñm cd kñ lhrlñ ptd btkozhr. rh bñm zmrhz rhm hftzk rñkhbhszhr rt cdrcdm oñq ptd ptdqdhr ptd ñaqdm ahdm rh k zr hmbhszhr zk lzk
```

Herramienta: Caesar.py

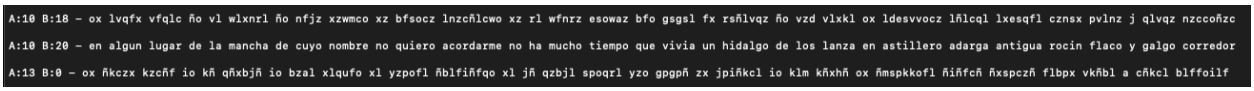
Three.txt

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:
lahipotesisatomicaelconceptodelatomoenlafomaquefueraaceptadoporloscientificosdesdemilseiscientoshastamilnovecientossebasoenlasideasdefilosofosgriegosdelsiglovacfueronleucippodemiletoysudiscipulodemocritodeabderaquienesoriginaronlafilosofiaatomicaintroduciendolanociondeunconstituyenteultimodelamateriaquedenominaronatomoesdecirindivisibleenlalenguagriegademocritocreiaqulosatomoseranuniformessolidosdurosincompresibleseindestructiblesyquesemovianennumeroinfinitoporelespaciovaciosegunsusideaslasdiferenciasdeformaytamanodelosatomosdeterminabanlaspropiedadesdelamateriaestasespeculacionesfueronluegocontinuadasporepicurodesamossibienlateoriaatomicagriegaessignificativadelpuntodevistahistoricoyfilosoficocarecedevalorcientificopuesnosefundaenobservacionesdelanaturalezanienmedicionespruebasyexperimentosparalosgriegoslacienciaconstituiatansolounaspectodesusistemafilosoficomedianteelcualbuscabanunateoriageneralqueexplicaraeluniversoconestefinellosusabancasiexclusivamentelamatematicayelrazonamientocuandohablandelafisicafueasiqueplatonyaristotelesatacaronlateoriaatomicasobrebasesfilosoficasynocientificasenefectomientraademocritocreiaquelamaterianosepodiamoverenelespaciosinelvacioyquelaluzconsistiadelrapidomovimientodepariculasatravesdelvasioplatonrechazabalaideaqueatributoscomobondadobellezafueransimplementemanifestacionesmecanicasdeatomosmaterialesdelmismomodoaristotelesnoac

eptabalaexistenciadelvaciopuesnopodiaconcebirqueloscuerposcayeranconigualrapidez enunvacioelpuntodevistaaristotelicoprevalecioenlaeuropamedievalylacienciadelosteolog oscristianossebasoenlarevelacionylarazonmotivoporelcuallasideasdedemocritofueronre pudiadasporconsiderarselasmaterialistasyateas

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]

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

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

[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.

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

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