INFORME DE TALLER 3

Criptoanálisis de métodos de cifrado clásicos

García Grimaldos, Alberto Manuel; Álvarez Caballero, Hernán David
alberto.garcia.2016@upb.edu.co; hernan.alvarez.2014@upb.edu.co
Universidad Pontificia Bolivariana
Seccional Bucaramanga
Octubre 6 de 2019

I. *OBJETIVOS DE DESARROLLO*

Objetivo General

– *Identificar y comprender los procedimientos de criptoanálisis a métodos criptográficos por sustitución y transposición, mediante la práctica de ejercicios manuales y algorítmicos, con el fin de sentar una base teórico-práctica para los protocolos de criptoanálisis del cifrado moderno..*

II. INTRODUCCIÓN

El criptoanálisis (del griego kryptós, "escondido" y analýein, "desatar") es la rama de la criptología que se dedica al estudio de sistemas criptográficos, para los fines de este laboratorio serán los métodos de cifrado clásicos como el cifrado Afín y el cifrado de Vigenere, con el fin de encontrar debilidades en los sistemas y romper su seguridad sin el conocimiento de información secreta.

El cifrado Afín es un tipo de cifrado de sustitución monoalfabética-monográfica, en el que cada letra del alfabeto se asigna a su equivalente numérico, se cifra mediante una función matemática simple y se convierte de nuevo en una letra, por lo tanto, tiene las debilidades de los cifrados de sustitución, y es que cada letra se cifra con la función $(ax+b)mod(n)$, donde b es la magnitud del cambio y a una constante de decimación, la cual debe ser impar y no estar dentro del conjunto de divisores de n, es decir, a debe ser coprimo con n: $mcd(a,n) = 1$.

El cifrado Vigenère es un tipo de cifrado de polialfabética periódica, utiliza el mismo método que el cifrado de César, agregando una clave de cifrado y descifrado, que se escribe cíclicamente sobre el mensaje en texto claro. La principal debilidad del cifrado de Vigenère es la naturaleza repetitiva de su clave, si un analista encuentra correctamente la longitud de la clave, entonces el texto cifrado puede ser tratado como un cifrado de Caesar entretejido, el cual puede ser descifrado.

III. *PROCEDIMIENTO*

Para el primer y segundo numeral, se realiza la rotación de César con todas las posibles claves ***b*** (cantidad de rotaciones en los caracteres) para así lograr inferir la respuesta mediante el conocimiento del lenguaje obtenido en el posible mensaje descifrado, esto gracias a que se conocía que el cifrado era de desplazamiento puro, se aplicó a los mensajes cifrados:

C_1 =
LEUZRCRRSLVCRUVTRGVILTZKRHLVMZ
MZRVEVCSFJHLVVEWVIDFPCRDRUIVU
VTRGVILTZKRCVGZUZFHLVCVCCVMRIR
LERTVJKRTFELERKFIKRPLEKRIIFUVDR
EKVHLZCCRTRGVILTZKRRTVGKFVETRE
KRUR

C_2 =
GKUHYTQXYBTUDEIQRUISKQDJECUQF
UJUSULEBLUHQSQIQUDBYBBUIQDTSQ
BSKBEGKUQJUHHYPQHUUDAZULYAJU
CFHQDEBQDESXUTUIQDZKQDCUXKRY
UHQWKIJQTELEBLUHFQHQJKSKCFBU
QEIFUHEUIJEORQZEEHTUDUICYBYJQH
UIQSQCRYEFKUTEFHECUJUHJUGKUUI
JEOFEDYUDTEJETECYUCFUEUDKDWH
QDHUWQBEGKUHUSYRYHQIUBTYQTUJ

KSKCFBUQEIKDSQHYEIEIQBKTETUQB
WKYUDGKUIYUCFHUFYUDIQUDUBVKJ
KHETUIKXYZQUDLYEKDQSEFYQTUUIJ
QFEIJQBQQBWKYUDGKUBEITEISEDESU
CEIOQBESECFHUDTUHQIXYBTUSYJQFE
HQXEHQUIJEOIYUDTECKOCYIJUHYEIE
FUHEOQBEUDJUDTUHQIIEVYQSEWYEB
QIYWKYUDJUFEIJQBGKUHYTQXYBTUQ
GKYQRQZEIULYLUIEBEUBCECUDJEIYT
UQBWECUQSEHTQHUTUUIJEICUIUIUD
UBBYRQDEIUHQTUUIJQUJUHDQUIFUH
QFUHEXQWEBEGKUFKUTEFQHQGKUJ
UDWQIUBCUZEHHUWQBEFEIYRBUUDJ
KTUSYCEGKYDJESKCFBUQEIDEFKUTE
TUSYHCQIFEHQXEHQCUYCFEDWEQCY
CYICEKDQIULUHQSUDIKHQQRHQPEIF
QFQ

Para descifrar las dos comunicaciones en castellano cifradas mediante Afín con desplazamiento puro se utilizó el script affineDecrypt.py con con unas leves modificaciones, se definió por defecto que a = 1 y para hacer una validación a fuerza bruta de b el script se corrió en un ciclo for de 0 hasta 25.

```
import re, os
from operator import itemgetter
import pickle

original_text = input('Enter the text to be decrypted: ')
replaced_text = original_text
len_text = len(replaced_text)

a = 1
for b in range(26):
    replaced_text = original_text
    for i in range(0,len_text):
        if replaced_text[i] is not " ":
            replaced_text = replaced_text[:i] + chr(int(a*((ord(replaced_text[i])-65) - b)%26 + 65)) + replaced_text[i+1:]
    print('Resultado iteracion ' + str(b) + ': ' + replaced_text)
```

Codigo 1. AffineDecrypt modificado. Autor: Julian Miranda. Modificado: Autores.

En el tercer punto se obtienen los divisores de la distancia entre los n-gramas dados, para así poder determinar la posible longitud de la clave utilizada para el cifrado. Cabe destacar que dentro de las longitudes obtenidas, las más probables son las longitudes primas. Las posibles claves se seleccionaron según su longitud de la tabla 1 brindada por el enunciado.

society	marry	property	ceiling
behavior	rare	book	guide
hesitant	council	hand	provide
plaster	stew	correct	beautiful
network	tacit	box	crevice

Tabla 1. Tabla de posibles clases usada para cifrar. Fuente: Documento guia.

Para el cuarto numeral se realizó la descomposición por divisores de las distancias entre los n-gramas repetidos presentados en la tabla 2, y de esta forma, poder hallar los divisores más frecuentes entre las distancias, los cuales serían la posible longitud de la clave.

n-grama	Distancias
PQMI	28, 329
QAWA	42
ASJU	98
BLVE	112
QOSO	154

Tabla 2. n-gramas y su distancias. Fuente: Documento guia.

En el quinto punto se operan las distancias entre cada una de las repeticiones del n-grama "**CGDRTHGH**" dado, para poder así hallar los divisores en común y saber la posible longitud de la clave que se seleccionará con respecto a si es o no un número primo con longitud menor o igual a la del n-grama.

Para el sexto numeral se deben hallar los n-gramas de 3 o más caracteres y sus distancias, para identificar los divisores más frecuentes entre ellas. Se ordenan los caracteres según su frecuencia, para identificar las coincidencias con el idioma español, y así poder hallar la longitud de la clave con respecto a la tabla de coincidencias y el IC.

L	IC	σ	[IC − σ, IC + σ]
...	...	...	...
2	0.0575	0.0047	[0.0529,0.0622]
3	0.0512	0.0037	[0.0457,0.0550]
4	0.0480	0.0030	[0.0450,0.0510]
5	0.0459	0.0025	[0.0435,0.0484]
6	0.0450	0.0022	[0.0428,0.0472]
7	0.0439	0.0019	[0.0420,0.0458]
...	...	...	...

Tabla 2. longitud de clave e índices de coincidencias. Fuente: Documento guia.

Se divide en subcriptogramas con respecto a la longitud de la clave, tomando un caracter cada L (longitud de la clave) caracteres, para su posterior análisis del IF de cada caracter, para al final resultar con un conjunto de caracteres de la posible clave, escogidos con respecto al mayor índice de frecuencia de cada subcriptograma.

Se utiliza fuerza bruta para descifrar con todas las claves halladas, combinando los conjuntos de caracteres posibles.

El criptograma utilizado en el procedimiento anterior fue:

C_3 =

GBCTWCPRGEFSSHKQHRAEDWRNRXS
ETHQOMXRCRFNRFWRXPXSETHQOM
XRCRFJYKNFBVUSUXPCQZNHCRTHQ
QSITXCBROIPOUHINJVGEFCVKECZVK
KKQFTPCOMXRCRVOIPOUHCGBSHKQ
HRLSNCGHHKOMXVNOCNDFSCWMCQ
FFSCJVGEFSMXRCRFXPCJVGEFCMXR
CRF

En el último número se pide descifrar un mensaje intervenido, y como se dijo que el cifrado utilizado fue Vigenere, se utilizó el método de Kasiski para romper el cifrado. Se realizó la búsqueda de cadenas repetidas en el texto cifrado y calculamos sus distancias, gracias al índice de coincidencia se determina la longitud de la clave del cifrado para poder dividir el criptograma en subcritogramas y finalmente aplicar el rompimiento del cifrado de sustitución monoalfabética en cada uno; el criptograma utilizado fue:

C_4 =

YWTXZEYPVBXIAALLPWPNZEMOIDODB
CFGFMPCXPVWAGZZFRMIPYTPQRSCLX
JHFQFPXVIUAYLTBEIMLOIQEIABFMQY
VDLYTJFVRLCVPWUEPDBBTIIDTWOIEL
LBCFRFSETMOIECLFBJZFSWLKMEMEO
PMOXIAOLIMEJEOPLFPJUWEIOEKOPD
MMWZGFTMOXVCZYRVRKOOPVPZVNEL
GESJLPEZBWTIQCIEEJCZYMMGZFCLLP
HVCPDISHVLBFMOSJENZVPGVLLNTBZV
OMZBYICNPXBHAOFEVSOBMHWIMGXB
KSUVCXVTFESUPEGSQCLBZHVUVYBVL
YPUUKKWSWFLXCNTVPJFOMEVJIMYK
WMFGMBXPDXFVRMZDXVIUAYCMTGRT
LCVPWGRZYBPECEYEZBVRLNLAUMCLZ
NWKEEEWACOXFDPLKDIJOLWIEIIENSI
FWFLZDTMIMACLIMETAGPZOEFPFPAU
ERDZYLFLRYFYOSYGOOPOVEIDTLADYR
NOZMTXVNPYTBGRVPCVBKVNPCMOYE
AOTAUVRCNTWOIJOSLZBULEWZAHYRR
OTITZRYLYPBGZAFDBFHVSXTMOXIADD
MEMIIRPVIETILPTDYRREZLFPCAGPADS
AAYWITPCAGPACEAEYOWTTZSZDXPVVL
NLTMIAOYOMMEDAYNPBVFJLJDFVRNW
LADICDLDLFTIIDTWOIIODPAUEDODLX
SIJAOZAFRCAOPKJQRCPWLBQLCSLAVII
TP

IV. *ANÁLISIS DE RESULTADOS*

De las dos comunicaciones de cifrado afín se encontró los siguientes mensajes:

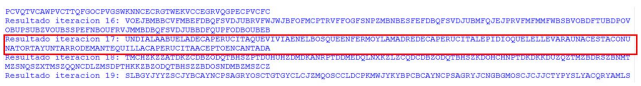

Imagen . Output script mensaje cifrado 1. Fuente: Autores.

M_1 = UN DIA LA ABUELA DE CAPERUCITA QUE VIVIA EN EL BOSQUE ENFERMO Y LA MADRE DE CAPERUCITA LE PIDIO QUE LE LLEVARA UNA CESTA CON UNA TORTA Y UN TARRO DE MANTEQUILLA CAPERUCITA ACEPTO ENCANTADA.

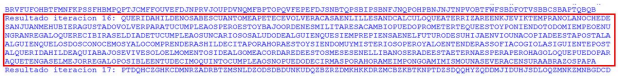

Imagen . Output script mensaje cifrado 2. Fuente: Autores.

M_2 = QUERIDA HILDE NO SABES CUANTO ME APETECE VOLVER A CASA EN LILLESAND CALCULO QUE ATERRIZARE EN KJEVIK TEMPRANO LA NOCHE DE SAN JUAN ME HUBIERA GUSTADO VOLVER PARA TU CUMPLEAOS PERO ESTOY BAJO ORDENES MILITARES ACAMBIO PUEDO PROMETERTE QUE ESTOY PONIENDO TODO MI EMPEO EN UN GRAN REGALO QUE RECIBIRAS EL DIA DE TU CUMPLEAOS UN CARIOSO SALUDO DE ALGUIEN QUE SIEMPRE PIENSA EN EL FUTURO DE SU HIJA ENVIO UNA COPIA DE ESTA POSTAL A ALGUIEN QUE LOS DOS CONOCEMOS YA LO COMPRENDERAS HILDECITA POR AHORA ESTOY SIENDO MUY MISTERIOSO PERO YA LO ENTENDERAS SOFIA COGIO LA SIGUIENTE POSTAL QUERIDA HILDEA QUIABAJO SE VIVE SOLO EL MOMENTO SI DE ALGO ME ACORDARE DE ESTOS MESES EN EL LIBANO SERA DE ESTA ETERNA ESPERA PERO HAGO LO QUE PUEDO PARA QUE TENGAS EL MEJOR REGALO POSIBLE EN TU DECIMOQUINTO CUMPLEAOS NO PUEDO DECIR MAS POR AHORA ME IMPONGO A MI MISMO UNA SEVERA CENSURA ABRAZOS PAPA

Para el numeral tres del cual se conoce que la cadena “TVAIVCXIERAA” se repite en las posiciones 4 y 235, se encuentran los divisores de 231 (*235 -4*) los cuales son = 1, 3, 7, 11, 21, 33, 77 y 231, ya que de la tabla 1 la clave las larga tiene 9 dígitos se utilizaron los números 3 y 7 como posibles longitudes, con estas longitudes las posibles claves a elegir para tres son:

- box

y siete:

- crevice
- provide
- ceiling
- correct
- council
- netowrk
- plaster

En el numeral cuatro en el cual se brindan unos n-grama expuestos en la tabla 2 con sus respectivas distancias se encontraron los siguientes divisores:

- 28: 1, 2, 4, 7, 14 y 28
- 329: 1, 7, 47 y 329
- 42: 1, 2, 3, 6, 7, 14, 21 y 42
- 98: 1, 2, 7, 14, 49 y 98
- 112: 1, 2, 4, 7, 8, 14, 16, 28, 56 y 112
- 154: 1, 2, 7, 11, 14, 22, 77 y 154

Los números que coinciden son 1,2,7,4,14; de estos números se puede concluir la longitud de la clave es 7, dado que es un número primo.

Al igual que el anterior punto, en el numeral cinco, se tiene un texto cifrado con Vigenere y contiene tres apariciones de las letras CGDRTHGH con distancias 1283 - 37 = 1246, 2291 - 1283 = 1008 y 2291 - 37 = 2254. De las distancias se obtienen los siguientes divisores:

- 1246: 1, 2, 7, 14, 89, 178, 623 y 1246
- 2254: 1, 2, 7, 14, 23, 46, 49, 98, 161, 322, 1127 y 2254
- 1008: 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 18, 21, 24, 28, 36, 42, 48, 56, 63, 72,

84, 112, 126, 144, 168, 252, 336, 504 y 1008

De los cuales se repiten los números: 1,2,7,14. Se toma como posible longitud de la clave de nuevo el 7 como número primo y multiplo de 14.

En el sexto numeral contamos con el mensaje cifrado C_3 del cual se rescataron las siguientes secuencias repetidas:

n-gram	Distance
GEF	[90, 70, 15]
EFS	[160]
SHK	[120]
HKQ	[120]
KQH	[120]
QHR	[120]
XSE	[20]
SET	[20]
ETH	[20]
THQ	[20, 29]
HQO	[20]
QOM	[20]
OMX	[20, 65, 30]
MXR	[20, 65, 55, 15]
XRC	[20, 65, 55, 15]
RCR	[20, 65, 55, 15]
CRF	[20, 120, 15]
XPC	[110]
OIP	[35]
IPO	[35]
POU	[35]
OUH	[35]
JVG	[70, 15]
VGE	[70, 15]
EFC	[85]
FSC	[8]
CJV	[15]
GEFS	[160]
SHKQ	[120]
HKQH	[120]
KQHR	[120]
XSET	[20]
SETH	[20]
ETHQ	[20]
THQO	[20]
HQOM	[20]
QOMX	[20]
OMXR	[20, 65]
MXRC	[20, 65, 55, 15]
XRCR	[20, 65, 55, 15]
RCRF	[20, 120, 15]
OIPO	[35]
IPOU	[35]
POUH	[35]
JVGE	[70, 15]
VGEF	[70, 15]
GEFC	[85]
CJVG	[15]
SHKQH	[120]
HKQHR	[120]
XSETH	[20]
SETHQ	[20]
ETHQO	[20]
THQOM	[20]
HQOMX	[20]
QOMXR	[20]
OMXRC	[20, 65]
MXRCR	[20, 65, 55, 15]
XRCRF	[20, 120, 15]
OIPOU	[35]
IPOUH	[35]
JVGEF	[70, 15]
VGEFC	[85]
CJVGE	[15]
SHKQHR	[120]
XSETHQ	[20]
SETHQO	[20]
ETHQOM	[20]
THQOMX	[20]
HQOMXR	[20]
QOMXRC	[20]
OMXRCR	[20, 65]
MXRCRF	[20, 120, 15]
OIPOUH	[35]
JVGEFC	[85]
CJVGEF	[15]
XSETHQO	[20]
SETHQOM	[20]
ETHQOMX	[20]
THQOMXR	[20]

HQOMXRC [20]
QOMXRCR [20]
OMXRCRF [20]
XSETHQOM [20]
SETHQOMX [20]
ETHQOMXR [20]
THQOMXRC [20]
HQOMXRCR [20]
QOMXRCRF [20]
XSETHQOMX [20]
SETHQOMXR [20]
ETHQOMXRC [20]
THQOMXRCR [20]
HQOMXRCRF [20]

Se obtienen los conteos de coinicidencias de cada caracter en los subcriptogramas anteriores, que serán usados para hallar el índice de coincidencia del criptograma y los conjuntos de caracteres a combinar para hallar la posible clave:

Char Ocurrences
C 21
R 19
F 14
H 12
X 12
S 11
Q 9
O 9
E 8
K 8
N 8
V 8
G 7
P 7
M 7
T 6
B 4
W 4
J 4
U 4
I 4
D 2
Z 2
A 1
Y 1
L 1

Los divisores de las longitudes que más aparecen es 2, 5 y 10 con 8,12 y 7 respectivamente, dado que se afirma que la llave tiene una longitud mayor a 2 caracteres y que el IC tiene un valor de 0.048235 se elige la longitud 5 al ser múltiplo de 10 y un número primo.

Teniendo el IC = 0.048235, se puede inferir la longitud de la clave 5, con respecto a la tabla de IC e IF.

Seleccionando los caracteres más recurrentes según cada subcriptograma:

char	s1	s2	s3	s4	s5
A	1	3	1	1	2
B	1	3	1	1	1
C	2	1	1	2	1
D	1	2	2	1	2
E	0	2	2	0	2
F	1	1	1	2	0
G	1	0	0	3	1
H	0	0	1	1	1
I	0	0	2	0	0
J	1	1	0	2	0
K	2	2	1	1	1
L	1	0	1	0	1
M	1	1	1	0	1
N	2	2	2	1	2
O	2	3	2	1	0
P	1	0	1	3	2
Q	1	1	0	1	2
R	1	1	3	0	2
S	2	1	1	1	1
T	1	0	0	4	2
U	0	0	1	1	1
V	1	0	2	1	0
W	2	1	0	1	1
X	1	2	0	1	2
Y	2	1	2	0	1
Z	2	2	2	1	1

Las posible combinaciones de clave son: 'CARTA', 'CARTD', 'CARTE', 'CARTN', 'CARTP', 'CARTQ', 'CARTR', 'CARTT', 'CARTX', 'CBRTA', 'CBRTD', 'CBRTE', 'CBRTN', 'CBRTP', 'CBRTQ', 'CBRTR', 'CBRTT', 'CBRTX', 'CORTA', 'CORTD', 'CORTE', 'CORTN', 'CORTP', 'CORTQ', 'CORTR', 'CORTT', 'CORTX', 'KARTA', 'KARTD', 'KARTE', 'KARTN', 'KARTP',

'KARTQ', 'KARTR', 'KARTT', 'KARTX', 'KBRTA', 'KBRTD', 'KBRTE', 'KBRTN', 'KBRTP', 'KBRTQ', 'KBRTR', 'KBRTT', 'KBRTX', 'KORTA', 'KORTD', 'KORTE', 'KORTN', 'KORTP', 'KORTQ', 'KORTR', 'KORTT', 'KORTX', 'NARTA', 'NARTD', 'NARTE', 'NARTN', 'NARTP', 'NARTQ', 'NARTR', 'NARTT', 'NARTX', 'NBRTA', 'NBRTD', 'NBRTE', 'NBRTN', 'NBRTP', 'NBRTQ', 'NBRTR', 'NBRTT', 'NBRTX', 'NORTA', 'NORTD', 'NORTE', 'NORTN', 'NORTP', 'NORTQ', 'NORTR', 'NORTT', 'NORTX', 'OARTA', 'OARTD', 'OARTE', 'OARTN', 'OARTP', 'OARTQ', 'OARTR', 'OARTT', 'OARTX', 'OBRTA', 'OBRTD', 'OBRTE', 'OBRTN', 'OBRTP', 'OBRTQ', 'OBRTR', 'OBRTT', 'OBRTX', 'OORTA', 'OORTD', 'OORTE', 'OORTN', 'OORTP', 'OORTQ', 'OORTR', 'OORTT', 'OORTX', 'SARTA', 'SARTD', 'SARTE', 'SARTN', 'SARTP', 'SARTQ', 'SARTR', 'SARTT', 'SARTX', 'SBRTA', 'SBRTD', 'SBRTE', 'SBRTN', 'SBRTP', 'SBRTQ', 'SBRTR', 'SBRTT', 'SBRTX', 'SORTA', 'SORTD', 'SORTE', 'SORTN', 'SORTP', 'SORTQ', 'SORTR', 'SORTT', 'SORTX', 'WARTA', 'WARTD', 'WARTE', 'WARTN', 'WARTP', 'WARTQ', 'WARTR', 'WARTT', 'WARTX', 'WBRTA', 'WBRTD', 'WBRTE', 'WBRTN', 'WBRTP', 'WBRTQ', 'WBRTR', 'WBRTT', 'WBRTX', 'WORTA', 'WORTD', 'WORTE', 'WORTN', 'WORTP', 'WORTQ', 'WORTR', 'WORTT', 'WORTX', 'YARTA', 'YARTD', 'YARTE', 'YARTN', 'YARTP', 'YARTQ', 'YARTR', 'YARTT', 'YARTX', 'YBRTA', 'YBRTD', 'YBRTE', 'YBRTN', 'YBRTP', 'YBRTQ', 'YBRTR', 'YBRTT', 'YBRTX', 'YORTA', 'YORTD', 'YORTE', 'YORTN', 'YORTP', 'YORTQ', 'YORTR', 'YORTT', 'YORTX', 'ZARTA', 'ZARTD', 'ZARTE', 'ZARTN', 'ZARTP', 'ZARTQ', 'ZARTR', 'ZARTT', 'ZARTX', 'ZBRTA', 'ZBRTD', 'ZBRTE', 'ZBRTN', 'ZBRTP', 'ZBRTQ', 'ZBRTR', 'ZBRTT', 'ZBRTX', 'ZORTA', 'ZORTD', 'ZORTE', 'ZORTN', 'ZORTP', 'ZORTQ', 'ZORTR', 'ZORTT', 'ZORTX'

Obteniendo el siguiente mensaje: EN LA SABANA DE BOGOTA HABIA UN VENADO AVENADO UN DIA EL VENADO AVENADO QUIZO IRSE DE LA CIUDAD COMO ERA TAN AVENADO EL VENADO ERA ALERGICO A LA AVENA DE VENADO Y EN BOGOTA SOLO PODIA VER LA LUZ DEL DIA COMO AVENA DE VENADO EL AVENADO VENADO.

De la misma forma que en el punto anterior, el criptoanálisis de vigenere se realiza de la siguiente manera, utilizando el método Kasiski:

Se obtienen los n-gramas repetidos.

n-gram	Distance
XVIU	[301]
VIUA	[301]
IUAY	[301]
LCVP	[280]
CVPW	[280]
TIID	[574]
IIDT	[574]
IDTW	[574]
DTWO	[574]
TWOI	[420, 154]
MOXI	[427]
OXIA	[427]
LIME	[294]
TMOX	[392]
PAUE	[231]
PCAG	[14]
CAGP	[14]
AGPA	[14]
XVIUA	[301]
VIUAY	[301]
LCVPW	[280]
TIIDT	[574]
IIDTW	[574]
IDTWO	[574]
DTWOI	[574]
MOXIA	[427]
PCAGP	[14]
CAGPA	[14]
XVIUAY	[301]
TIIDTW	[574]
IIDTWO	[574]
IDTWOI	[574]
PCAGPA	[14]
TIIDTWO	[574]
IIDTWOI	[574]
TIIDTWOI	[574]

Se hallan los divisores comunes entre las distancias de cada par de n-gramas.

Divisor	Ocurrences
7	10
2	7
14	6

Se ordenan los caracteres por coincidencias.

Char	Ocurrences
L	49
P	48
I	46
E	45
O	41
V	40
M	37
F	35
A	34
T	33
Z	31
C	31
Y	30
D	30
B	27
W	25
R	24
X	20
S	19
G	17
N	16
J	16
U	14
K	11
Q	8
H	8

Se halla el IC, así también seleccionando la longitud de la clave.

IC value: 0.04108256316150438 - Most probable length key: 7

De los subcriptogramas, se analizan los conjuntos de los caracteres par las posibles claves.

char	s1	s2	s3	s4	s5	s6	s7
A	0	1	1	1	1	4	1
B	2	1	4	0	1	1	2
C	2	1	1	0	0	0	1
D	1	1	0	1	2	0	0
E	0	2	0	4	3	1	0
F	1	1	1	2	2	0	0
G	2	1	0	1	0	0	1
H	2	1	0	1	1	1	3
I	0	4	1	3	2	1	1
J	0	1	1	2	1	2	0
K	1	0	2	1	0	1	2
L	4	0	1	0	0	1	4
M	1	2	1	1	0	2	1
N	0	1	2	1	2	3	0
O	0	0	3	0	1	1	1
P	3	1	1	0	0	0	1
Q	1	1	0	2	1	1	0
R	0	2	1	3	5	1	0
S	0	0	1	1	2	0	0
T	2	1	0	1	0	1	1
U	2	2	1	1	1	1	2
V	0	3	1	2	3	1	1
W	0	1	1	1	1	3	1
X	2	0	3	1	0	2	3
Y	3	1	2	0	0	1	3
Z	1	1	1	0	1	1	1

La única posible clave arrojada fue: LIBERAL

Lo que nos devuelve el mensaje en claro:

NOS TIENEN ATRAPADOS Y NO TENEMOS QUE COMER POR FAVOR ENVIEN LO MAS RAPIDO QUE PUEDAN A LA ARMADA PARA QUE PUEDAN LIBERARNOS DE ESTA PRISION EN LA QUE NOS TIENEN CAUTIVOS LA CLAVE DE ENTRADA A LA SEDE DEL SULTANATO ES EL SIGUIENTE CONJUNTO DE NOVENTA Y DOS LETRAS CIFRADAS CON EL CIFRADO DE CESAR DEL QUE NO SE CONOCE LA CLAVE
OBOTXELNEMTGWXFTKKNXVHLXEFT
KKHJNBTETUTKTLNGHFUKXIHKJNXX
ELNEMTGTWHLXKTLNIKHIBXMTKBHI
HKLBXFIKX ESPERAMOS PUEDAN RESCATARNOS PRONTO AL ENTRAR AL CASTILLO COJAN EL PUNTO DE ACCESO A LA DERECHA ESO LOS LLEVARA A LA CAVERNA OPUESTA ADONDE HAY UN GRUPO DE GUARDIAS CUANDO ESTEN EN LA CAVERNA GENEREN UNA DISTRACCION ESO HARA QUE LOS GUARDIAS VAYAN HACIA USTEDES

MIENTRAS SE DIRIGEN HACIA EL CUARTO DE LLAVES COJAN LAS LLAVES BAJEN DOS PISOS POR EL CALLEJON DE LA MANCHA ROJA Y VERAN LAS CELDAS DE PRISIONEROS ESTAMOS APRESADOS EN LA DECIMA CELDA MUCHA SUERTE

V. *CONCLUSIONES*

Los cifrados clásicos son las formas más simples de cifrar; han existido por miles de años y han sido ampliamente estudiados, gracias al método de Kasiski la complejidad necesaria para vulnerarlos no es tan alta computacionalmente hablando, este algoritmo de análisis de frecuencia es seguramente el enfoque rápido para descifrar texto. Sin embargo, requiere el conocimiento de las estadísticas de frecuencia del idioma utilizado para escribir el texto original.

Los principios de cifrado por sustitución monoalfabética y polialfabética son básicos en sus bases y son fáciles de entender. Sin embargo, los principios de sustitución y transposición forman la base de muchos de los estándares de cifrado actuales. Al combinar la sustitución y la transposición de manera creativa, es posible producir sistemas criptográficos extremadamente seguros.

Si se desea garantizar un nivel de seguridad incondicional en un mensaje cifrado, se debe utilizar el cifrado de Vernam.

VI. *REFERENCIAS BIBLIOGRÁFICAS*

[1] Kozdron, Michael. "Affine Ciphers - Affine Ciphers, Decimation Ciphers, and Modular Arithmetic " (2006). Disponible en: http://pi.math.cornell.edu/~kozdron/Teaching/Cornell/135Summer06/Handouts/affine.pdf

[2] Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. Disponible: https://books.google.com.co/books?id=fd2LtVgFzoMC&pg=PA21&redir_esc=y#v=onepage&q&f=false