

Universidad del Valle de Guatemala
Cifrado de Información - CC 3078 - Sección 10
Julio Herrera 19402
Bryann Alfaro 19372
Diego Arredondo 19422

Algoritmos Básicos y Fuerza Bruta Laboratorio 1

INTRODUCCIÓN

En este laboratorio se exploraron algunos de los cifrados históricos como una forma de adentrarse en el concepto de cifrado de la información. En primer lugar se utilizaron los cifrados de Caesar, Vigenere y Afín para la encriptación y la decriptación de textos de ejemplo.

Seguidamente, se hizo un análisis de frecuencias y la definición de una función de métrica para poder realizar un ataque de fuerza bruta y descifrar ciertos textos que fueron encriptados con los 3 algoritmos anteriormente mencionados.

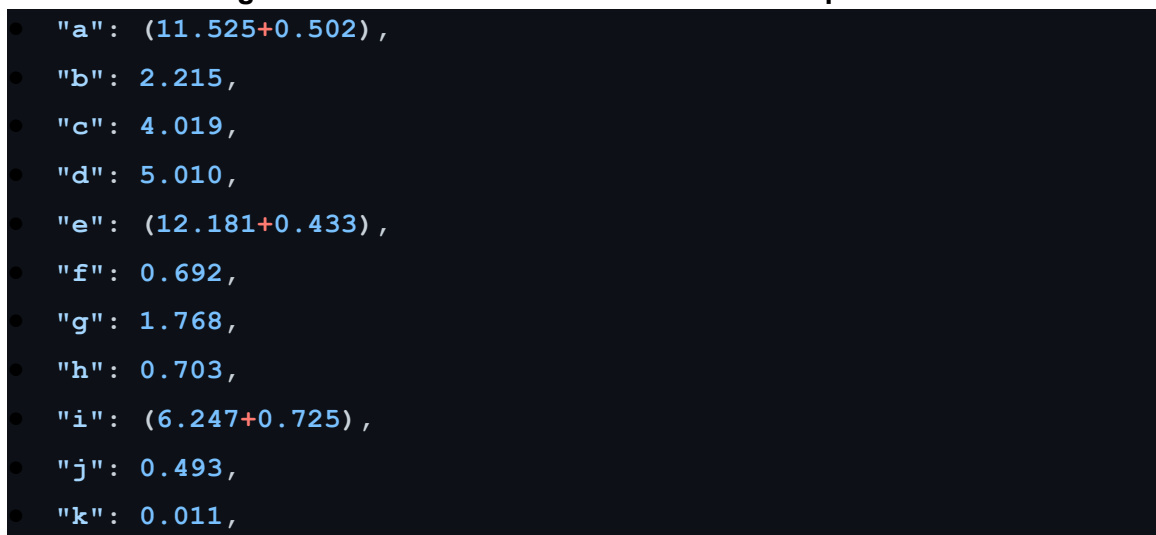
Esto se realizó con el fin de poder observar lo vulnerable que sería la utilización de este tipo de algoritmos en sistemas actuales y la necesidad que existe de utilizar algoritmos más complejos.

METODOLOGÍA

Datos

- El alfabeto que se utilizó durante este laboratorio es el alfabeto castellano de 27 letras, incluyendo la "ñ" y excluyendo las vocales tildadas. Por lo tanto la variable M utilizada durante este laboratorio toma este valor ($M = 27$).
- Se utilizó la tabla de frecuencias mostrada en la **Figura 1** la cual une las frecuencias de las vocales en el caso que tengan o no un carácter especial como tilde o diéresis.

Figura 1: Tabla de frecuencias del idioma español.



"a":	(11.525+0.502) ,
"b":	2.215 ,
"c":	4.019 ,
"d":	5.010 ,
"e":	(12.181+0.433) ,
"f":	0.692 ,
"g":	1.768 ,
"h":	0.703 ,
"i":	(6.247+0.725) ,
"j":	0.493 ,
"k":	0.011 ,

```

"l": 4.967,
"m": 3.157,
"n": 6.712,
"ñ": 0.311,
"o": (8.683+0.827),
"p": 2.510,
"q": 0.877,
"r": 6.871,
"s": 7.977,
"t": 4.632,
"u": (2.927+0.168+0.012),
"v": 1.138,
"w": 0.017,
"x": 0.215,
"y": 1.008,
"z": 0.467

```

Cifrados

- **Caesar**

Para encriptar en este cifrado se utilizó la fórmula $E(x) = x + k \pmod{M}$ donde x es la posición de la letra a la que se aplica el desplazamiento y k es la llave que indica el tamaño del desplazamiento. Para desencriptar en este cifrado se utilizó la fórmula $D(x) = x - k \pmod{M}$ teniendo como parámetros los mismos valores que en el encriptado.

- **Afín**

Para el encriptado del cifrado afín se utilizó la fórmula $E(a, b, x) = (a \cdot x + b) \pmod{M}$ donde a y b son las llaves donde a es un entero que no posee factor común con M , es decir a es coprimo de M para que pueda tener inverso y el desencriptado sea funcional. Para el desencriptado de este cifrado se utilizó la fórmula $D(a, b, x) = a^{-1}(x - b) \pmod{M}$ teniendo en cuenta lo mencionado en el cifrado, donde a es coprimo con M .

- **Vigenere**

Para el cifrado Vigenere se utilizó la fórmula $E(x) = (x_i + k_{i \pmod{N}}) \pmod{M}$ en donde M es el tamaño del alfabeto a utilizar y N es el tamaño de la clave k . Para la descripción del mensaje se debe acudir a la fórmula $E(x) = (x_i - k_{i \pmod{N}}) \pmod{M}$.

Métrica y fuerza bruta

- Probabilidades

Estas son las frecuencias o probabilidad de aparición de una letra respecto a un texto. Primero se obtiene la cantidad de veces que aparece cada letra en el texto utilizando la función “FreqDist” de la librería “nltk”, luego se obtiene el total de resultados y se obtiene la probabilidad de cada letra por medio de su ocurrencia dividido la cantidad de letras en el texto.

- Métrica

La métrica calcula el error entre las frecuencias de todas las letras obtenidas de un descifrado con un posible valor del espacio de claves contra las frecuencias verdaderas del idioma español. El error total se obtiene del error de cada letra utilizando la fórmula $error_1 = (valor\ teórico - valor\ experimental)^2$. Luego se

obtiene finalmente $error_{total} = \sqrt{\frac{\sum_{i=1}^M error_1}{M \cdot (M-1)}}$ que será el error de cada posible valor de la clave en el espacio de claves para cada cifrado, donde un menor error representa una frecuencia de letras más parecida al del idioma español.

- Fuerza bruta Caesar

- Se ejecutó el descifrado para cada posible valor del campo de claves (27) y se calculó el error comparando la frecuencia de letras del idioma español con la obtenida a partir del descifrado.

- Fuerza bruta Afín

- Se ejecutó el descifrado para cada posible valor del campo de claves (286) y se calculó el error comparando la frecuencia de letras del idioma español con la obtenida a partir del descifrado.

- Fuerza bruta Vigenere

- Primero se obtuvo todas las combinaciones sobre el abecedario de 1 a 4 letras de longitud (dando menos error las combinaciones de 4 letras de longitud), para luego meter cada combinación al método de descifrado. Seguidamente, se calculó el error comparando la frecuencia de letras del idioma español con la obtenida a partir del descifrado.

RESULTADOS

- **Cifrado Caesar**

- Tiempo: 0.073 milisegundos.
- Primer puesto
 - Llave 19
 - error 0.0016103904146207765%
 - Decriptado caesar:
el analisis por frecuencias para descifrar criptogramas se basa en estudiar la frecuencia con la que aparecen los distintos simbolos en un lenguaje determinado y luego estudiar la frecuencia con la que aparecen en los criptogramas y de esta manera establecer una relacion y obtener el texto plano la idea es fundamental es que no todas las letras aparecen con la misma frecuencia en los textos sino que algunas aparecen mas a menudo que otras contando los signos del texto cifrado y ordenandolos de mayor a menor frecuencia podemos establecer

ecerconjeturasacercadequeletracorrespondeacadasignoel analisisseco mpletaconlabusquedadepalabrasfrecuentescomoarticulosy preposicion essi ademasconocemososospechamosdealgunapalabraquedebaapare cerenelmensajemejorquemejorelrestoescuestionedeintuicionsegununes tudiosobretextosdeldiarioelpaisdeenriquefontanillolamuestratomadads onlosejemplaresdedichodiariopublicadosduranteunasemanacincuenta ydosmilseiscientosdiecinueveletrasentotallafrecuenciadelasletrasenca stellanoesaproximadamentelaquesigue

○ Segundo

- Llave 8
- error 0.008879057471202647%
- Decriptado caesar:
ovlxlvdsdzcpconfoxnsldalclñodnspclncsaezqclwlddomldloxodeñslc
vlpconfoxnslnzxvlbfolalconoxvzdñsdesxezddswmvzdoxfvovxqfltoñoe
ocwsxlñzjvfoqzodeñslc vlpconfoxnslnzxvlbfolalconoxoxvzdncaezqclw
ldjñoodelwloclo delmvonocfxcovlnsxjzmeoxocoveoiezavlxzvlñolpfx
ñlwoxelvodbfvxezñldvldvoecl dalconoxnzxvlsdwl pconfoxnsloxvzdeo
iezddsxbfolvqfxldalconoxwldlwofñzbfzecldnzxelñzvlddsqxzdñove
oieznspclñzjzcnñoxlxñzvdñowljzclwoxzc pconfoxnslazñowzdodelmvon
ocnzxtoefcl dlnoclnñobfoveclnzccodazñolnñldsqxzovlxlvdsddonzw
avoelnzxvlmfdbfoñlñaalvmlcl d pconfoxeodnzwzlc esnfvdjacoazdsnszx
oddsñowldnxznwzd d dzaonrlwzdñolvqfxlalvmlcl bfoñomllalconocox
ovwoxdlto wotzcbfowotz covcodezodnfodeszxñosxefsnszxdofxfoxdefñ
szdzmcoeoiezdñovñslcszovalsdñooxc sbfopzxelxsvvzvlwfodeclezwlñlñ
dzxvzdotowavlcodñonñsnrñslcszafmvsnlñzdñfclxeofxldowlxlnsxnfoxelj
ñzdwsvdosdnsoxezdñonsxfogovoecl d oxezelvlpconfoxnslñovldvoecl
doxnld eovvlxzodlacziswlñlwoxeovlbfodsqfo

○ Tercero

- Llave 4
- error 0.008959692332862508%
- Decriptado caesar:
szobozwhwhedgtgsqjsbqwoheogorshqwtgogqgweidugoaohhspohosbs
hijrwogzotgsqjsbqwoqdbzofjsoeogsqsbzdhwhiwbidhhwapdzdhbjbz
bujoxsrsgawbordnzsudshijrwogzotgsqjsbqwoqdbzofjsoeogsqsbzbd
hggweidugoaohnrsshioaobsgoshiopzsqsgjbogszoqwbndpisbsgszismi
dezobdzowrsotjbroasbiozshfjsb didrohzhzsigohoeogsqsbqdbzoawhao
tgsqjsbqwosbzdhis midhhw bdfjsozujbohoeogsqsbao hoasbjrd fjsdigohq
dbiobrdzohhwubdhrsizmidqwtgordndgrsbobrdzdhrsaondgoasbdgtgsq
jsbqwoedrsadhshiopzsqsgqdbxsijgohogsgqorsfjszsigoqdggsbedbrsoq
orohwubdszobozwhwhhsqdaezsioqdbzopjh fjsrorseozopgohtgsqjsbish
qdadogi wqjzdhnegsedhwqwdbshhworsaohqdbdq sadhdhdhesqvoadhr
sozujboeozopgofjrs p ooeogsqsgsbzsbzasbhoxsasxdgfsasxdgsgzgidsh
qjshiwdbrswbijwqwdbhsujbjshijrwdhdpgsismidhrs zrwogwdszeowhrss
bgwfjstdbiobwzzdzoajshigoidaororhdbzdhsxaezogs hrswqvd rwogwd
ejpzwqordhrjgobisjbohsaoboqwbqjsbionrdhawzhshwqwsbidhrwsqwbjs
kszsigohsbidiozzotgsqjsbqworszohzsigohsbqohiszzobdshoegdmwaor
oasbiszofjshwujs

● Cifrado Afin

- Tiempo: 1.6 segundos
- Primero
 - Llaves: 23 y 12
 - error 0.0014964708505096108%
 - Decriptado afin:
 lamadrugadadeestejuevesquincedejulioaterrizoenelaeropuertointernac
 ionallaauroradeguatemalaelavionquetrajounlotedetrescientasdiezmild
 osisdevacunasputnikvqueserviranparacontinuarconelplannacionaldev
 acunacioncontraelcoronavirusoriginalmenteelavionibaaaterrizarenguat
 emalaelmiercolesalasveintiunahorasperoluegoseinformoqueelvuelose
 habiaretrasadoyporesollegoalpaisesodelascuatrohorasdeestejueves
 elministeriodesaludinformoqueelaviontrajotrescientasdiezmildosisdelbi
 ologicorusodelascualesseentamilsonegundasdosisydoscientoscincu
 entamilprimerasdosisadiferenciadeotrasvacunaselbiologicoderusiatien
 edoscomponentesunoqueseutilizaparalaprimerdosisyotroparaelfue
 rzoyestecargamentodesesentamilsignificariaelprimeroquerecibeelpais
 desegundasdosisconestasdosissecontinuaraconelplannacionaldevacu
 nacionyseiniciaraconlaadministraciondelassegundasdosiscuandolasp
 imeraspersonasinmunizadasconsputnikvcumplansusnoventadiasdeha
 berrecibidolaprimerdosisitalainformaciondelministeriodesalud
- Segundo
 - Llaves: 4 y 9
 - error 0.006443292511110896%
 - Decriptado afin:
 ishspbynspspooazokyoxoacylgqopokyileszobblteogoisobedyobzelgzo
 bgsqlegsiissybebsponyszohsisoisxlegcyozbskeygiezopozboaqlgzsap
 lothlipealapoxsqygsadyzgljxcyoabxlbgsdsbsqegzlgysbqegoidisggsqle
 gsipoxsqygsqlegqegzbsoiqebegsxlbyaebnlgsihogzooisxleglrssszobblt
 sbognyszohsisoihlobqeioasisaxlolgzlygsmebsadobeiyoneaolgñebhec
 ooixyoieaomsrlsbozbsaspeudeboaeiionesidslasoapoisaqyszbemeb
 apooazokyoxoaoihlglaoblepoasiyplgñebhecyoisxlegzbskezboaqlgzsap
 lothlipealapoirleienlqebyapoisaqysioaaoagzshliaegaonygpsapea
 laupeaqllogzeaqlgqyogzshlidblhobsapealasplñobogqlspoezbsaxsqygs
 aoirleienlqepobyalszlogopeaqehdegogzoaygecyaooyzliitsdsbsisdblh
 bspealauezbedsboiboñyobteuoazoqsbnsbhogzepoaoagzshliainglñlqs
 blsoidblhobecyoboblrooidslapoanygpsapealaqegoazsapealaoqegz
 gysbsqegoidisggsqlegsipoxsqygsqleguaolglqlsbsqegissphlglaqzbsqleg
 poisaaonygpsapealaqysgpeisadblhobsadobaegsalghygltspsaqegadyz
 gljxqyhdisgayagexogzspisapomsrobboqlrpeisdblhobspealaqlzsislgñeb
 hsqlegpoi hlglaoblepoasiyp
- Tercero
 - Llaves: 4 y 15
 - error 0.007044540113742563%
 - Decriptado afin:
 tesebnkyebabaamlavkajamñkwrcabavktwpelannwfparateanpokanlpwrl
 anrecwpretteeknpnebaykelaseteatejwprñkalnevpkrtplabalnmcwarlem
 bwafswtbpmbwmbajeckremoklrwujñkamanjwneroenecprlwrkencpratote
 rrecwpretbajeckrecwprcprlneatcpnprejwnkmpnwywretsarlaatejwprwde

eelannwfenarykelaseteatswancptametemjwawrlwkrexpnemoanptkayp
 mawrzpnspñkaatkpmaxedwenalnemebpgopnampttaypetoewmeam
 pbatemckelnpxpnembaamlavkajamatswrwmlanwpbametkbwrzpnspñk
 aatejwprlnevplnamcwarlembwafswtbpmwmbatdwptpywcpnkmpbatem
 cketammamarleswtmprmaykrbembpmwmgbpmcwarlpmcwrckarleswto
 nwsanembpmwmebwzanarcwebaplnemjeckrematdwptpywcpbankmw
 elwarabpmcpsoprarlamkrpñkamaklwtwfeoeneteonwsanebpmwmgplnp
 oeneatnazkanfpgamlacenyesarlpbamamarleswtmwywzwcenweatonw
 sanpñkanacwdaatoewmbamaykrbembpmwmcpramlembpmwmmacprl
 wrkenecpratoterrecwpretbajeckrecwprgmawwrcwenecprteebswrwmln
 ecwprbatemmaykrbembpmwmckerbptemonwsanemoanmpremwrskrw
 febemcprmoklrwujcksotermkmrpjarlebwembaxedannacwdwbpteonws
 anebpmwmcwletewrzpnsecwprbatswrwmlanwpbametkb

- **Cifrado Vigenere**

- Tiempo: 21.13 minutos

- Primero

- Llave: bees

- error 0.0010466438768528194%

- Decriptado Vigenere:

cuandofraybartolomearrazolasesintioperdidoaceptoqueyanadapodrias
 alvarlolaselvapoderosadeguatemalalohabiaapresadoimplacableydefini
 tivaantesuignoranciatopograficasesentocontranquilidadaesperarlamue
 rtequisomorirallisinningunaesperanzaaisladoconelpensamientofijoenla
 españoladistante particularmente en el convento de los abrojos donde carlos
 quinto condescendiera unavezabajar desu eminencia para decirle que con
 fiaba en el celo religioso de su labor redentora al despertar se encon tro ro de ad
 o por un grupo de indigenas de ro sto im pasible que se disponian a sacrificarl
 o ante un altar un altar que abartolome le parecio como el lecho en que descan
 saria al fin de su temores de su destino de su miseria años en el pais le habi
 an conferido un medianodominio de las lenguas nativas intento al godijo al gu
 na palabras que fueron comprendidas entonces florecio en el una idea que t
 uvopordignadesu talento y de su cultura universal y de su arduo conocimiento
 o de aristo teles recordo que para es de iase esperaba un eclipse total de sol y d
 ispuso en lo mas intimo alersede a quel conocimiento para enganar a sus op
 resores y salvar la vida a si mismo a tales diosjopuedo hacer que el sol se oscurezc
 a en su altur a los indigenas lo miraron fijamente y bartolome sorprendiolo in cr
 edulidad en sus ojos vio que se produjounpequeño consejo yespero confiad
 onosinciertodesdendoshoras despues el corazon de fray bartolome arrazol
 achorreabasusangrevehementessobrelapiedradelossacrificiosbrillante b
 ajola opacaluz de un soleclipse adomientras unodelos indigenas recitaba sin
 ningunainflexion de voz sin pris aunaporunalas infinitas fechas en que se pro
 ducirianeclipse solares y lunares que los astrónomos de la comunidad may
 a habian previsto y anotado en sus codices sin lavaliosa ayuda de aristo teles

- Segundo

- Llave: bess

- error 0.0019572561518825396%

- Decriptado Vigenere:

cumndoqraynartalomparrmzlmsestntiaperoidomcepfoqupyandapad

rimsalharlalasplvabodedosaoegumtemmlalahabtaapdesaoimblacmbi
ekdefnittvaaytesgignaranñiatapogdafiñaseeentaconfrancuiltadmesp
prarwamuprtecuisamortralwisiyninrunapspedanzmaiswadoñonewpene
amipntoqijopnlapspazadietanfepadticglarxentpenewconhentadelasab
ojoedonoecadloscuinfocoydesñendteragnavpzabmjaroessupminpncimp
armdectrlecuecanfimbaeyelcplorpligtosooesuwabodredpntodaaloespp
rtadseeeyconforadeaopodungdupooeinoigeyasdprosfoixpastblecues
pdisbonimnasmcriqicadloayteuyaltmrunmltadquembarfoloxelebareñioc
amoewlecsoencuedpscaysartaalqindpsusfemodesdpsudpstiyodeeimie
motdesazoseyelpmisphabtancanfedidognmeoianadomtnioelaenru
asyatihasyitenfoalrodiuolrunaepalmbraequerancoxpreydidmsenfo
ncpsflarectoenplunmidemquefuvobordtгнаoesufaleytoyoesuñultgrauyi
vedsalkdesgardgocoyocixienfodemrisfotewesrporooqupparmeseoias
pespprbrmuneñlipeetofaldpsolkdisbusopnloxasiytimavalprseoeaqgcl
anoctmiejtopmraeygañmrasgsopdesodesyealvmrlahidaeimexatatslee
dijapueoohañerqgeeleolspocgrezñaeneualfurawosiydigpnaswomidar
oyfijmmenfeybmrtoowomeeorpdendtolatncrpdultdadpnsueojoeviocuesp
prooujognpecueñaconeeyjokespprocanfimdonasinñierfodeedenoochar
asoespgesewcormzonoefrmybadtolameadrazalacsorrpabaeusaygrehe
hexentpsobdelabieddadewossmcriqiciasbrtllaytebmjmlmopañaluldeuys
olpclibsadamieytraeunooeloeindtngenmsreñitanasiyninrunatnflpxioydev
azsiyprieaunmporgnalmsinqinifasfpchaeenqgesebrodgcirtaneñlipeess
alarpsylgnarpsqulplosmstranomasdewacoxunioadmmayahmbiayprehist
ayanatadaensgscooicesinwavawiosmayuoademrisfotewes

○ Tercero

- Llave: beeh
- error 0.001997799144696237%
- Decriptado Vigenere:

cuaydofdaybmrtoowomemrralolaeesiytiobertdoañeptaquekanaoapoori
aealvmrlowasewvapaderasadpguafemawalosabimaprpsadaimpwacan
leyoefiyitihaanfesutgnodancatobogrmfcmssespntoñontdanqgilioadaps
pedarlmmuedteqgisoxoridalltsinyinggnaeepermnzamislm docanelbens
mmieytoftjoeylaeepañmdisfantpparficuwarmptepnelñonvpntooeloeab
rajoosondpcarwosqgintaconoescpndiprauyavelabauardpsuexineyciab
araoecidleqgecoyfianaenplceworewigiasodpsulmbordede yformaldpsp
edtareeenñontdorooeadaporgngrgpodpindtngenmsdedostdoimbasinleq
geseoispaniayasañriftcarwoanfeunmltadunawtarcueanartalomplepmre
ctocoxoelwechaenqgedeecanearimalftndeeustpmorpsdeeudeetinades
tmisxotrpsañasenplpatslesabimncoyfertdouymedtanoomiyiodplaswe
nggasnmtivmsinfentaalgadijaalggnasbalanrascuefgeroycombrenoidae
entanceeflodeciaenewunatdeacuetgvopardirnadpsutmlenfoydpsucgltu
dauntverealyoesumrduaonacimtentadeadistatelpseñordaquebaraps
edtasepspedabagnecwipsptotmldeeolyoispgsoeylommsinfimohaledse
dpaquplcoyocixienfopadaenrañadasueoprpsorpsysmlvadlavtdastmem
mtaielesoijobuedahacprqupelsalseascudezcmensgaltgralasinoigeyasl
amirmronqijaxentpybadtolamesarprndialaiycreouliaoadeysusajoshioqg
esebrodggjouypeqgeñofñonspjoypspedocoyfiaoonoeinctertadesoendas
hodasdpupselñoralondpfrakbarfoloxeardazowacharrembasgsanrev

phempnteeobrplaptedrmde la sañ riftcioe briwlanfebauolaapacmluzoeu
neoleñlipeadoxienfrasgnodplostndirenaerecttabmsinyinggnaiyflejionoe
volsinbrismunaboruyalaeinfntitmsfeñhaspnqupsepdoduñirimnecwipsp
ssowareeyluyareequewosaetroyomoedel mcomgnidmdmakahanianbre
vtstokanofadopnsuecodtcese inlmvaltosamyudmdeadistatelps

CONCLUSIONES

- Es posible obtener la llave de estos cifrados por el método de fuerza bruta debido a que estos tienen un espacio de claves relativamente pequeños al poder computacional utilizado actualmente.
- Mientras mayor sea el espacio de clave, mayor será el tiempo que tome computar todos los posibles valores de clave que descifren el texto.
- Para los tres cifrados se encontró la llave correcta a partir de un error menor al 0.00161. Por lo que, se puede concluir que en estos cifrados, al analizar sus frecuencias, existe cierta correlación con el alfabeto que se utilizó y esto es lo que los hace vulnerables.
- Para el cifrado Caesar y Afín, desde la segunda opción con un error a partir a 0.00644 (Afín) y 0.0089 (Caesar) dió como resultado un texto ilegible, mientras que para el cifrado Vigenere, tanto la segunda opción como la tercera, con un error de 0.001957 y 0.001997 respectivamente, dieron como resultado un texto donde se pueden llegar a entender palabras con solo algunas letras incorrectas.