

**Realizado por: Victor Amador Muñoz**  
**Boleta: 2014630538**

### **Cifrado Cesar**

Nombre programa: cifradoCesar.c

nombre ejecutable: cifrado

Uso:

1. escribir la palabra a cifrar despues de que aparezca el mensaje “Escribe la palabra a anlizar” en minusculas
2. escriba el número de letras a correr (pueden ser entre -25 y +25)
3. lea el resultado

### **Descifrado Cesar**

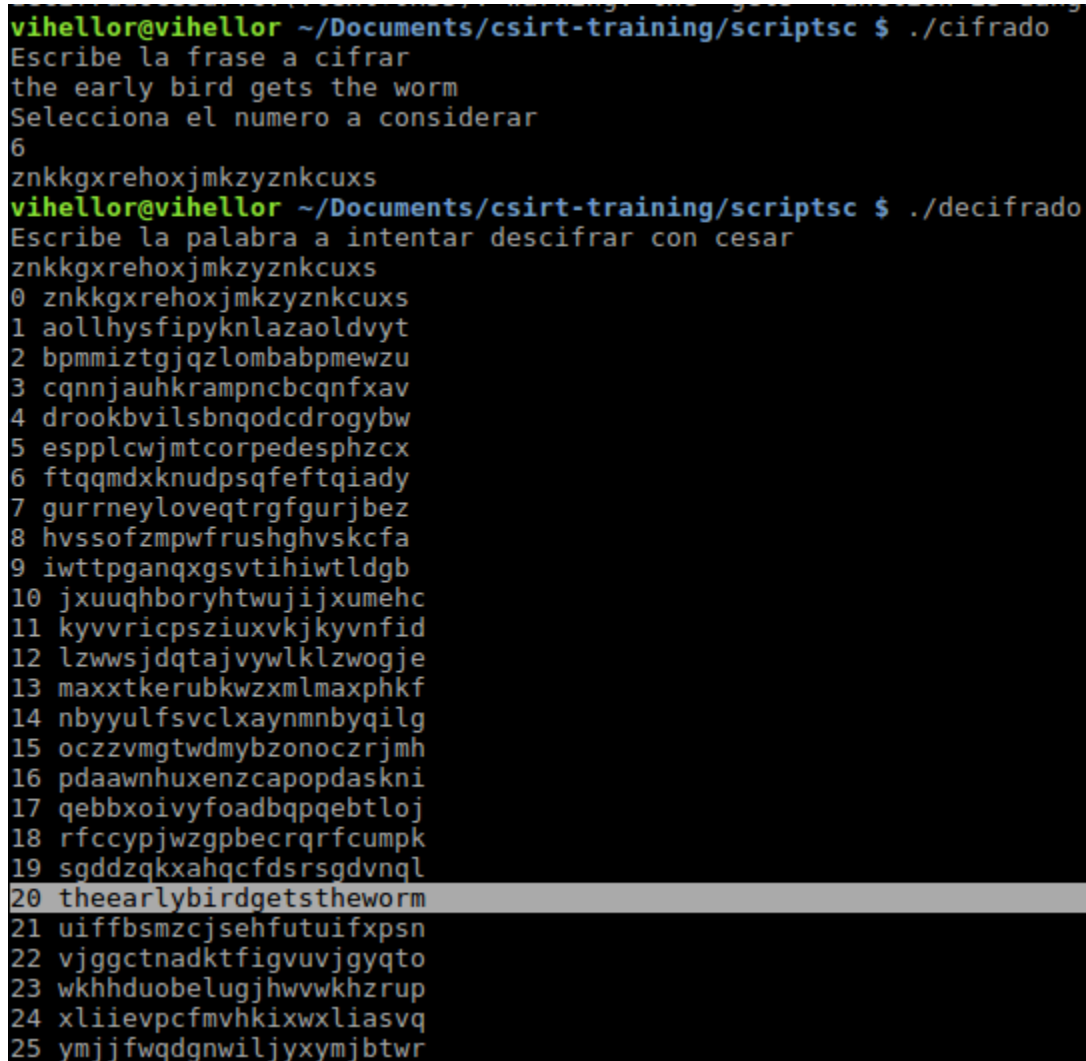
Nombre programa: cifradoCesar.c

nombre ejecutable: cifrado

Uso:

1. escribir la frase a descifrar despues de que aparezca el mensaje “Escribe la palabra a intentar descifrar con cesar”
2. Busque una linea que tenga sentido

screenshots:



```
vihellor@vihellor ~/Documents/csirt-training/scriptsc $ ./cifrado
Escribe la frase a cifrar
the early bird gets the worm
Selecciona el numero a considerar
6
znkkgxrehoxjmkzyznkcuxs
vihellor@vihellor ~/Documents/csirt-training/scriptsc $ ./descifrado
Escribe la palabra a intentar descifrar con cesar
znkkgxrehoxjmkzyznkcuxs
0 znkkgxrehoxjmkzyznkcuxs
1 aollhysfipyknlazaoldvyt
2 bpmmitzgjqlombabpmewzu
3 cqnnjauhkrampncbcqnfav
4 drookbvilbnqodcdrogybw
5 espplcwjmtcorpedesphzcx
6 ftqqmdxknudpsqfeftqiady
7 gurrneyloveqtrgfgurjbez
8 hvssofzmpwfrushghvskcfa
9 iwttpganqxgsvtihiwtldgb
10 jxuuqhboryhtwujijxumehc
11 kyvvricpsziuxvkjkyvnfid
12 lzwvsjdqtajvywlklzwogje
13 maxxtkerubkwzxmlmaxphkf
14 nbyyulfsvclxaynmnbyqilg
15 oczzvmgtwdmybzocrzjmh
16 pdaawnhuxenzcapopdaskni
17 qebbxoivyfoadbqpqebtloj
18 rfccypjwzgpbecrqrfcumpk
19 sqddzqkxahqcfdsrsgdvnql
20 theearlybirdgetstheworm
21 uiffbsmzcjsehfutuifxpsn
22 vjggctnadktfigvuvjgyqto
23 wkhhduobelugjhvwkhzrup
24 xliievpcfmvhkixwxliasvq
25 ymjffwqdgwniljyxymjbtwr
```



## Cifrado Vigenere

Nombre programa: vinegere.c

nombre ejecutable: vinegere

Uso:

1. escribir la primer palabra a cifrar después del mensaje: “Escribe la primer palabra”
2. escribir la segunda palabra a cifrar (llave) después del mensaje: “Escribe la segunda palabra”
3. lea el resultado

## Descifrado vinegere

Nombre programa: desvinegere.c

nombre ejecutable: decvinegere

Uso:

1. escribir la palabra a decifrar después del mensaje: “Escribe la primer palabra”
2. escribir la llave para decifrar después del mensaje: “Escribe la segunda palabra”
3. lea el resultado

screenshots:

```
vihellor scriptsc # ./vinegere
Escribe la primer palabra
politecnico
Escribe la segunda palabra
ipnipnipnip
xdyqirkcvkd
vihellor scriptsc # ./decvinegere
Escribe la primer palabra
xdyqirkcvkd
Escribe la segunda palabra
ipnipnipnip
politecnico
vihellor scriptsc # █
```

## Cifrado por bloques

Nombre programa: bloques.c

nombre ejecutable: bloques

Uso:

4. escribir la palabra(s) a cifrar después del mensaje: "Escribe la palabra a modificar"
5. escribir el tamaño del bloque a modificar (el tamaño de la palabra debe ser divisible entre el tamaño del bloque)
6. escribir a donde se deben hacer los cambios de las letras

## Descifrado por bloques

Nombre programa: bloques.c

nombre ejecutable: bloques

Uso:

Es igual al anterior, sólo debe de darsele los números invertidos de la tabla

screenshots:

```
vihellor scriptsc # ./bloques
Escribe la palabra a modificar
PIRATEATTACK
Selecciona el numero a considerar
4
Selecciona los numeros para el intercambio
3
1
4
2
IAPRETTAAKTC
vihellor scriptsc # ./bloques
Escribe la palabra a modificar
IAPRETTAAKTC
Selecciona el numero a considerar
4
Selecciona los numeros para el intercambio
2
4
1
3
PIRATEATTACK
vihellor scriptsc # █
```

## Tarea1:

### Ejercicio 1:

Mensaje original:

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr  
jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko  
bj yt wkbrusurbmbwj k lmird jk xjbt trmui jx ibndt wb wi kjb mk rmit bmq bj rashmwk rmvp  
yjeryrk mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjysrbr  
rashmkmbwj k jkr cjhnd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd  
urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrri i jnkd mkd ipmsrhrii ipmsr  
w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnln bpmb bpr  
xjhjcwko wi bpr sujsru msshwvmbwj k mkd wkbrusurbmbwj k w jxxru yt bprjuwri wk bpr pjsr bpmb  
bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvp

Mensaje decifrado:

because the practice of the basic movements of kata is the focus and mastery of self is the essence of  
matsubayashi ryu karate do i shall try to elucidate the movements of the kata according to my  
interpretation based on forty years of study it is not an easy task to explain each movement and its  
significance and some must remain unexplained to give a complete explanation one would have to be  
qualified and inspired to such an extent that he could reach the state of enlightened mind capable of  
recognizing soundless sound and shapeless shape i do not deem myself the final authority but my  
experience with kata has left no doubt that the following is the proper application and interpretation i  
offer my theories in the hope that the essence of okinawan karate will remain intact

Fue escrito por:

Un japonés del área de okinawa (lo que creia).

Después de buscar en internet:

The Essence of Okinawan Karate-Do - Page 56

by Shoshin Nagamine

### Como lo resolví:

Primero hice un programa para sacar las frecuencias de las letras a las que hay en el texto (el programa se llama proporcionesLetras.c con su ejecutable propo)

Copie el resultado en un archivo y luego use :

```
#cat archivo | sort -nr
```

Para tenerlos ordenados por número. A esto le agregué las letras de frecuencias en el orden que aparecen en wikipedia ([https://en.wikipedia.org/wiki/Letter\\_frequency](https://en.wikipedia.org/wiki/Letter_frequency) )

Después hice otro programa donde le marcaba con que letra debe cambiarse cada uno (programa: descifrado letras, ejecutable dl)

La primera descifración no se veía como algo legible pero había un par de palabras que sí, entonces fui cambiando las letras para sustituir hasta que todas las palabras tenían sentido y logré conseguir el texto (me basaba en las palabras que eran casi seguras de ser algo y sólo tenían 1 error).

## Ejercicio 2:

Mensaje original:

xultpaajcxitltlxaarpjhtiwtgxktghidhipxcwtvgtpilpitghlxiwiwtxgqadds

Mensaje descifrado:

ifweallunitewewillcausetheriverstostainthegreatwaterswiththeirblood

Lo escribió: buscando en internet encontré que fue Tecumseh durante un discurso que dio ante las aldeas.

### Como lo resolví:

Usé mi programa de descifrado cesar y busqué la linea que tuviera más sentido  
screenshot:

```
vihellor scriptsc # ./decifrado
Escribe la palabra a intentar descifrar con cesar
xultpaajcxitltlxaarpjhtiwtgxktghidhipxcwtvgtpilpitghlxiwiwtxgqadds
0 xultpaajcxitltlxaarpjhtiwtgxktghidhipxcwtvgtpilpitghlxiwiwtxgqadds
1 yvmuqbbkdyjumumybbsqkiujxuhyluhijeijqydxuwhuqjmquhijyxxuyhrbeet
2 zwnvrcclezkvnvzccctrljvkvizmvijkfjkrzekyvixvrknrkvijnzkykyvziscffu
3 axowsddmfalwwoaddusmkwlzwanwjklgklsafzwyjwsloslwjkoalzlzawjtdggv
4 bypxteengbmxpxpbeevtnlxmaxkboxklmhlmtbgmaxzxtmptmxklpbmamaxbkuehww
5 czqyuffohcnyqyqcffwuomynbylcpylmnimnuchnbyalyunqunylmqcnbnbyclvfiix
6 darzvggpidozrzrdggxvpnzoczmzmqnojnovidiozbmzvovozmnrdococzdmgwjy
7 ebsawhhqjepasasehhywqoapdaneranopkopwejpdacnawpswanosepdpdaenxhkkz
8 fctbxiirkfqbttbftiizxrbqebobfsbopqlpqxfkqebdobxqtxqbopftfqqebfoylla
9 gducyjjslgrcucugjjaysqcrfcpgtcprmqryglrfcepcyruyrpcpugrfrfcgpszjmbb
10 hevdkkktmhsdvdvhkkbzttrdsqgdhudqrsnrszhsmsgdqdzsvzsdqrvhsgsgdhqaknnc
11 ifweallunitewewillcausetheriverstostainthegreatwaterswiththeirblood
12 jgxfbmvmvojufxfxjmmdbvtfuifsjwfstuptubjouifhsfbuxbufstxjuuiufjscmppe
13 khygcnnwpkvgygyknnecwugvjgtxgtuvquvckpvjgitgcvcvgtuykvjvjgktdnqqf
14 lizhdooxqlwhzhzloofdxxvhwkhulyhuvwrwvdlqwkjhuhdwzdwuhvzlwkwkhlueorrg
15 mjaieppyrmxiaiamppgeywxlivmzivwxswxemrxlikviexaexivwamxlmvfpssh
16 nkbjfqqsnybjbnqqhfzxxymjwnajwxytxyfnsymjlwjfybfywxbnymymjnwgtti
17 olckgrratozkckcorrigaykznkxobkxyzuyzgotznmkxkgzcgzkxycoznznkoxhruuj
18 pmdlhssbupalldpssjhbzlaolypclyzavzahpuaolnylhadhalyzdpaoalpyisvvk
19 qnemittcvqbmemeqttkicambpmzqdmzabwabiqbpmozmibeibmzaeqbpbpmqzjtwl
20 rofnjuudwrcnfnfruuljdbncqnarenabcbxbrwcqnpanjcfjcnabfrqcqnrakuxxm
21 spgokvvexsdogogsvvmkecodrobsfobcdycdksxdroqbokdgdobcgsdrdrosblvyyn
22 tqhplwfytephptwnlfdpespctgpcdezdeltyesprcplehlepcdhtesesptcmwzzo
23 uriqmxxgzufqiqiuxxomgeqftqduhqdefaefmuzftqsdqmfimfqdeiufuftqudnxaap
24 vsjrnyyhavgrjrjvyypnhfrgurevirefgbfgnvagurterngjngrefjvgugurveoybbq
25 wtksozzibwhskskwzzqoigshvswfjsfghcgchowbhvsufsohkohsfgkwhvhvswfzccr
vihellor scriptsc #
```