

Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 7

Integrantes

Juan Camargo

Diego Castellanos

Profesor

Daniel Esteban Vela Lopez

Bogotá 2024



LEVEL 0

Nos conectamos al servidor por el puerto 2331.

```
File Actions Edit View Help
(kali@kali)~$ ssh krypton1@krypton.labs.overthewire.org:2231
The authenticity of host '[krypton.labs.overthewire.org]:2231 ([51.20.13.48]:2231)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[krypton.labs.overthewire.org]:2231' (ED25519) to the list of known hosts.

      Home

      KRYPTON

      This is an OverTheWire game server.
      More information http://www.overthewire.org/wargames

krypton1@krypton.labs.overthewire.org's password:
```

Decodificamos con una página de cifrados base64.

Decodifique a partir del formato Base64

Simplemente introduzca los datos y pulse el botón de decodificar.

S1JZUFRPTkITR1JFQVQ=

Para binarios codificados (como imágenes, documentos, etc.) utilice el fe

UTF-8 Conjunto de caracteres de origen.

☐ Decodifique cada línea por separado (útil cuando tiene varias entradas).

Modo en directo DESACTIVADO Decodifica en tiempo real mientras

DECODIFICAR Decodifica sus datos en la zona de abajo.

KRYPTONISGREAT

Enjoy your stay!

krypton1@bandit\$

LEVEL 1

```
Enjoy!  
krypton1@bandit:/krypton/krypton1$ ls  
krypton2  README  
krypton1@bandit:/krypton/krypton1$
```

Nos dicen que el texto de este nivel se cifró con ROT13.

```
The first level is easy. The password for level 2 is in the file  
'krypton2'. It is 'encrypted' using a simple rotation called ROT13.  
It is also in non-standard ciphertext format. When using alpha characters for  
cipher text it is normal to group the letters into 5 letter clusters,  
regardless of word boundaries. This helps obfuscate any patterns.  
  
This file has kept the plain text word boundaries and carried them to  
the cipher text.
```

Entramos a una página de cifrado ROT13.

ROT-13

Input Text

YRIRY GJB CNFFJBEQ EBGGRA

Result

LEVEL TWO PASSWORD ROTTEN

La contraseña es ROTTEN.

Enjoy your stay!

krypton2@bandit:~\$

LEVEL 2

```
krypton2@bandit:~$ cd /krypton/  
krypton2@bandit:/krypton$ cd krypton2  
krypton2@bandit:/krypton/krypton2$ ls  
encrypt keyfile.dat krypton3 README  
krypton2@bandit:/krypton/krypton2$ cat krypton3  
OMQEMDUEQMEK  
krypton2@bandit:/krypton/krypton2$
```

Seguimos el ejemplo que nos da el enunciado, pero dándole la ruta del texto de “krypton3”

```
krypton2@bandit:~$ mktemp -d  
/tmp/tmp.o4isXeIRPd  
krypton2@bandit:~$ /tmp/tmp.o4isXeIRPd  
cd /tmp/tmp.o4isXeIRPd  
-bash: /tmp/tmp.o4isXeIRPd: Is a directory  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ ^M  
: command not found  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ ln -s /krypton/krypton2/keyfile.dat  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ ls  
keyfile.dat  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ chmod 777  
chmod: missing operand after '777'  
Try 'chmod --help' for more information.  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ chmod 777 .  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ /krypton/krypton2/encrypt /krypton/krypton2  
/krypton3  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ ls  
ciphertext keyfile.dat  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ cat ciphertext  
krypton2@bandit:/tmp/tmp.o4isXeIRPd$ cat ciphertext  
AYCQYPGQCYQWkrypton2@bandit:/tmp/tmp.o4isXeIRPd$
```

Si ponemos el texto en una página de cifrados caesar y le ponemos orden 2 nos suelta la contraseña del siguiente nivel.

VIEW
Plaintext
AYCQYPGQCYQW

ENCODE DECODE
Caesar cipher
SHIFT
2 a→c
ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
→ Encoded 12 chars

VIEW
Ciphertext
CAESARISEASY

Enjoy your stay!
krypton3@bandit:~\$

LEVEL 3

Entramos a una página de frecuencia de análisis y colocamos los textos encontrados de “found1”, “found2”, “found3” y “krypton4” y miramos las letras que más se repiten con las más usadas y usamos un poco de prueba y error para sacar la contraseña.

Single letters: (The letters E, T, A and O are the most common in English)

S	F	Q	J	U	C	R	N	D	Z	V	W	Y	T	L	M	X
10%	6%	6%	6%	6%	5%	5%	4%	4%	3%	3%	2%	2%	2%	1%	1%	1%

Bigrams: (The pairs TH, ER, ON, and AN are the most common in English)

DS	SN	CG	JD	JC	CU	SU	UJ	SW
1.7%	1.4%	1.3%	1.3%	1.2%	1.1%	1.1%	1%	0.9%

Single letters: (The letters E, T, A and O are the most common in English)

S	C	J	G	Q	H	B	U	D	V	W	Z	E	K	M	A	X
10%	8%	7%	6%	6%	5%	5%	4%	3%	3%	2%	2%	2%	2%	2%	1%	1%

Bigrams: (The pairs TH, ER, ON, and AN are the most common in English)

JD	CG	DS	NS	QG	SN	SQ	BG
1.7%	1.6%	1.6%	1.4%	1.4%	1.2%	1.2%	1%

Single letters: (The letters E, T, A and O are the most common in English)

S	Q	J	N	U	R	D	G	C	W	Z	V	M	T	E	X	Y	I
11%	8%	7%	6%	6%	6%	5%	5%	4%	3%	2%	2%	2%	1%	1%	1%	1%	1%

Bigrams: (The pairs TH, ER, ON, and AN are the most common in English)

JD	DS	SU	DQ	QN	SN	JS	NS	SQ
2%	1.3%	1.2%	1.2%	1.2%	1.1%	1%	1%	1%

Single letters: (The letters E, T, A and O are the most common in English)

S	Y	B	N	U	J	K	M	W	A	C	D	G	I	Q	X	Y
14%	9%	7%	7%	7%	4%	4%	4%	4%	2%	2%	2%	2%	2%	2%	2%	2%

Bigrams: (The pairs TH, ER, ON, and AN are the most common in English)

SV	AN	BG	BM	BN	CU	GS	IS	JD
4.8%	2.4%	2.4%	2.4%	2.4%	2.4%	2.4%	2.4%	2.4%

S → e

Q=24% → A
J=24% → T
C=18% → L
G=17% → N
U=23% → M
V=17% → B/C
B=23% → D
N=22% → I/N/S
D=14% → O
W=11% → L/C
X=5%
I=2%
Y=3%

JD=7.4%
↳ J=T
D=H

Guesses (clear guesses):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	o	i	h			n		v	t	w		u	r			a		e		s	l	d	f	p	

well done the level four password is brute

Enjoy your stay!

krypton4@bandit:~\$

LEVEL 4

El enunciado del ejercicio dice que se utiliza el encriptado de Vigenere Cipher y que la longitud de la llave es de 6 letras, si buscamos una página de este cifrado y colocamos lo encontrado en “found1” nos devuelve un texto humanamente legible.

VIGENERE CIPHER

Cryptography > Poly-Alphabetic Cipher > Vigenere Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT (?)

TTICS JIZIB AGTIX KIEWV IAXFN JOOVQ QVMDL CKKEB SLEYA
 RIQYI IOXQT WXRIC RVVKP BHZXI YLYZP DLCDI IKGFJ UXRIP
 TFQGL CWVXR IEZRV NMYSF JDLCL RXOWJ NMIXX FNJSP JGHVV
 ERJTT OOHXM VMBWN JTXKG JJJXY TSYKL OQZFT OSRFN JKBIY
 YSSHE LIKLO RFJGS VMRJC CYTCS VHDLC LRXOJ MWFYB JPNVR N
 WUMZ GRVMF UPOEB XKSDL CBZGU IBBZX MLMKK LOACX KECOC
 TIUSBS RMPXR TPJZW XSPTR HKROR VVOHR MVKEE PTZEX SDYYT

PARAMETERS

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

☐ KNOWING THE KEY/PASSWORD: KEY

☒ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 6

☐ KNOWING ONLY A PARTIAL KEY: KE?

☐ KNOWING A PLAINTEXT WORD: CODE

☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

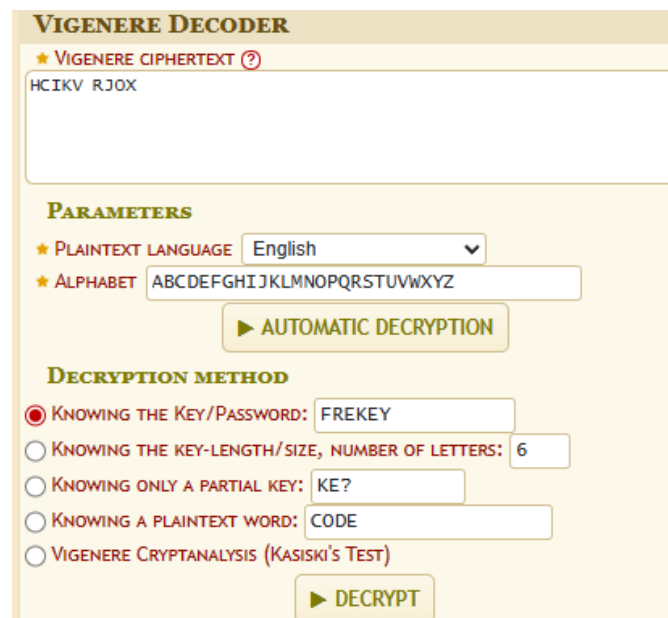
Observamos que nos devolvió una llave “FREKEY”, es posible que esta sea la llave que se utilizó para encriptar los textos.

Results	
Vigenere 6	
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)	
size limited to 500	
↑↓	↑↓
	THE SOLDIER WITH THE GREEN WHISKERS LED THEM
	THROUGH THE STREETS OF THE EMERALD CITY UNTIL
	THEY REACHED THE ROOM WHERE THE GUARDIAN OF THE
	GATES LIVED. THIS OFFICER UNLOCKED THE IR SPEC
	TACLES TO PUT THEM BACK IN HIS GREAT BOX AND THE
	NHE POLITELY OPENED THE GATE FOR OUR FRIENDS W
FREK	HICH ROAD LEAD TO THE WICKED WITCH OF THE WEST
EY	ASKED DOROTHY THERE IS NO ROAD ANSWERED THE GU
	ARDIAN OF THE GATES NO ONE EVER WISHES TO GO THA
	TWAY HOW THEN ARE WE TO FIND HER INQUIRED THE GI
	RL THAT WILL BE EASY REPLIED THE MAN FOR WHEN SH
	E KNOWS YOU ARE IN THE COUNTRY OF THE WINKIESSH
	E WILL FIND YOU AND MAKE YOU ALL HER SLAVES PERH
	APS NOT

Si hacemos lo mismo con lo encontrado en “found2” obtenemos otro texto legible y nos vuelve a dar “FREKEY” por lo que ahora si podemos asumir que la llave es de “FREKEY”

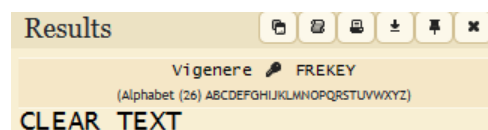
```
THEYWEROBLIGEDTOCAMPOUTTHATNIGHTUNDER  
ALARGETREEINTHEFORESTFORTHEREWERENOHO  
SESNEARTHETREEMADEAGOODTHICKCOVERINGTO  
PROTECTTHEMFROMTHEDEWANDTHETINWOODMANC  
HOPPEDAGREATPILEOFWOODWITHHISAXEANDDOR  
OTHYBUILTASPLENDIDFIRETHATWARMEDHERAND  
FREK MADEHERFEELLESSLONELYSHEANDTOTOTATHEL  
EY ASTOFTHEIRBREADANDNOWSHEDIDNOTKNOWWHAT  
THEYWULDDOFOBREAKFASTIFYOUWISHSAIDTH  
ELIONIWILLGOINTOTHEFORESTANDKILLADEERF  
ORYOUYOUCANROASTITBYTHEFIRESINCEYOURTA  
STESARESOPECULIARTHATYOUNPREFERCOOKEDFO  
ODANDTHENYOUWILLHAVEEVERYGGOODBREAKFAST  
DONTPL
```

Ahora que tenemos la llave podemos colocar lo que está dentro de “krypton2” con la llave y nos da la contraseña del siguiente nivel.



The image shows a web-based Vigenere Decoder interface. At the top, it says "VIGENERE DECODER". Below that is a section for "VIGENERE CIPHERTEXT" with a text input field containing "HCKV RJOX". Underneath is a "PARAMETERS" section with a "PLAINTEXT LANGUAGE" dropdown set to "English" and an "ALPHABET" input field containing "ABCDEFGHIJKLMNOPQRSTUVWXYZ". There is a button labeled "AUTOMATIC DECRYPTION". Below that is a "DECRYPTION METHOD" section with five radio button options: "KNOWING THE KEY/PASSWORD:" (selected), "KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS:", "KNOWING ONLY A PARTIAL KEY:", "KNOWING A PLAINTEXT WORD:", and "VIGENERE CRYPTANALYSIS (KASISKI'S TEST)". The "KNOWING THE KEY/PASSWORD:" option has a text input field containing "FREKEY". The "KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS:" option has a text input field containing "6". The "KNOWING ONLY A PARTIAL KEY:" option has a text input field containing "KE?". The "KNOWING A PLAINTEXT WORD:" option has a text input field containing "CODE". At the bottom right of the "DECRYPTION METHOD" section is a button labeled "DECRYPT".

Como no podemos colocar espacio en las contraseñas asumiremos que la contraseña en realidad es “CLEARTEXT”



The image shows the "Results" section of the Vigenere Decoder. It has a title "Results" and a toolbar with icons for copy, paste, download, print, and close. Below the toolbar, it says "Vigenere FREKEY" and "(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)". At the bottom, it says "CLEAR TEXT".

```
Enjoy your stay!  
krypton5@bandit:~$ |
```

LEVEL 5

El enunciado nos dice que la longitud de la llave no se conoce, por lo que haremos lo mismo del punto anterior, pero esta vez le descriptaremos automáticamente para tomar textos legibles y ver cuál es su llave.

The image shows a web application titled "VIGENERE CIPHER" with a subtitle "Cryptography · Poly-Alphabetic Cipher · Vigenere Cipher". Below this is a section titled "VIGENERE DECODER". It features a text input field labeled "★ VIGENERE CIPHERTEXT (?)". The input field contains a grid of 10 rows and 20 columns of random letters. Below the input field is a "PARAMETERS" section with two dropdown menus: "★ PLAINTEXT LANGUAGE" set to "English" and "★ ALPHABET" set to "ABCDEFGHIJKLMNOPQRSTUVWXYZ". At the bottom of the parameters section is a button labeled "▶ AUTOMATIC DECRYPTION".

Para "found1" nos retorna "KEYLENGTH", para confirmarlo haremos lo mismo con "found2"

```
ITWASTHEBESTOFTIMESITWASTHEWORSTOFTIME
SITWASTHEAGEOFWISDOMITWASTHEAGEOFFOOL I
SHNESSITWASTHEEPOCHOFBELIEFITWASTHEEPO
CHOFINCREDULITYITWASTHESEASONOFFLIGHTIT
WASTHESEASONOFDARKNESSITWASTHESPRINGOF
HOPEITWASTHEWINTEROFDESPAIRWEHADEVERYT
HINGBEFOREUSWEHADNOTHINGBEFOREUSWEWERE
ALLGOINGDIRECTTOHEAVENWEWEREALLGOINGDI
RECTTHEOTHERWAYINSHORTTHEPERIODWASSOFA
RLIKETHEPRESENTPERIODTHATSOMEOFITSNOIS
IESTAUTORITIESINSISTEDONITSBEINGRECEI
VEDFORGOODORFOREVILINTHESUPERLATIVEDEG
KEYL REEOFCOMPARISONONLYTHEREWEREAKINGWITHA
ENGT LARGEJAWANDAQUEENWITHAPLAINFACEONTHEH
H RONEOFENGLANDTHEREWEREAKINGWITHALARGEJ
AWANDAQUEENWITHAFAIRFACEONTHETHRONEOFF
RANCEINBOTHCOUNTRIESITWASCLEARERTHANC
YSTALTOTHELORDSOFTHESTATEPRESERVESOFLO
AVESANDFISHESTHATTHINGSINGENERALWERESE
TTLEDFOREVERITWASTHEYEAROFFOURLORDONETH
OUSANDSEVENHUNDREDANDSEVENTYFIVESPIRIT
UALREVELATIONSWERECONCEDEDTOENGLANDATT
HATFAVOUREDPERIODASATTHISMRSSOUTHCOTTH
ADRECENTLYATTAINEDHERFIVEANDTWENTIETHB
LESSEDBIRTHDAYOFWHOMAPROPHETICPRIVATEI
NTHELIFEGUARDSHADHERALDEDTHESUBLIMEAPP
EARANCEBYANN
```


Nos volvió a dar la llave “KEYLENGTH” por lo que podemos confirmar que esta fue la llave que se utilizó.

	WHENTHEMAILGOTSUCCESSFULLYTODOVERINTHE COURSEOFTHEFORENOONTHEHEADDRAWERATTHE ROYALGEORGEHOTELOPENEDTHECOACHDOORASHIS CUSTOMWASHEDIDITWITHSOMEFLOURISHOFCE MONYFORAMAILJOURNEYFROMLONDONINWINTERW ASANACHIEVEMENTTOCONGRATULATEANADVENTU ROUSTRAVELLERUPONBYTHATTIMETHEREWASONL YONEADVENTUROUSTRAVELLERLEFTBECONGRATU LATEDFORTHETWOTHOTHERSHADBEENSETDOWNATTH EIRRESPECTIVEROADSIDEDESTINATIONSTHEMI LDEWYINSIDEOFTHECOACHWITHITSDAMPANDDIR TYSTRAWITSDISAGEEABLESMELLANDITSOBSCUR KEYLITYWASRATHERLIKEALARGERDOGGKENNELMRLORR ENGTYTHEPASSENGERSHAKINGHIMSELFOUTOFITINCH HAINSOFSRAWATANGLEOFSHAGGYWRAPPERFLAPP INGHATANDMUDDYLEGSWASRATHERLIKEALARGER SORTOFDOGTHEREWILLBEAPACKETTOCALAISTOM ORROWDRAWERYESSIRIFTHEWEATHERHOLDSANDT HEWINDSETSTOLERABLEFAIRTHETIDEWILLSERV EPRETTYNICELYATABOUTTWOINTHEAFTERNOONS IRBEDSIRISHALLNOTGOTOBEDTILLNIGHTBUTIW ANTABEDROOMANDABARBERANDTHENBREAKFASTS IRYESSIRTHATWAYSIRIFYOUPLEASESHOWCONCO RDGENTLEMANSVALISEANDHOTWATERTOCONCORD PULLOFFGENTLEMANSBOOTSINCONCORDYOUWILL FINDAFINESEACOALFIRESIRFETCHBARBERTOCO NCORDSTIRABO
--	---

Ponemos el texto dentro de “krypton6” y ponemos la llave “KEYLENGTH”

VIGENERE CIPHER

Cryptography > Poly-Alphabetic Cipher > Vigenere Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT (?)

BELOS Z

PARAMETERS

★ PLAINTEXT LANGUAGE English

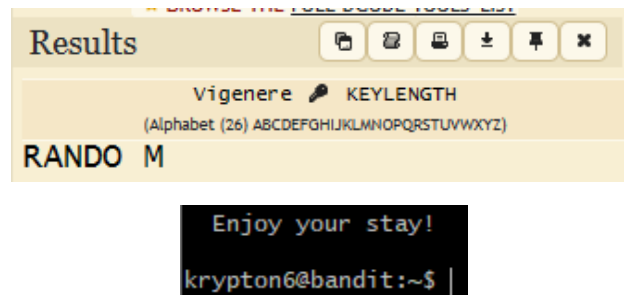
★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

AUTOMATIC DECRYPTION

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: KEYLENGTH

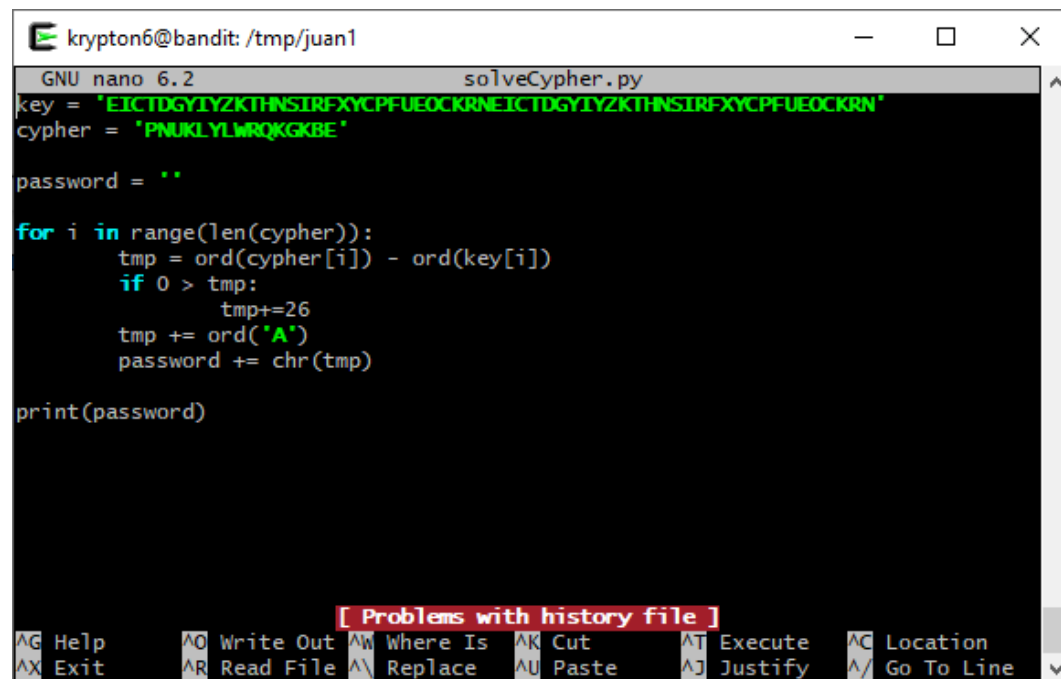
Nos retorna la palabra "RANDO M" y como en el ejercicio anterior, asumiremos que es "RANDOM"



LEVEL 6

Stream cipher.

```
krypton6@bandit:/tmp$ mkdir /tmp/juan1
krypton6@bandit:/tmp$ cd /tmp/juan1
krypton6@bandit:/tmp/juan1$ ln -s /krypton/krypton6/keyfile.dat
krypton6@bandit:/tmp/juan1$ ls
keyfile.dat
krypton6@bandit:/tmp/juan1$ python3 -c "print( 'A'*100 )" > test
krypton6@bandit:/tmp/juan1$ /krypton/krypton6/encrypt6 test cypherTest
krypton6@bandit:/tmp/juan1$ cat cypherTest
EICTDGYIYZKTHNSIRFXYPFUEOCKRNEICTDGYIYZKTHNSIRFXYPFUEOCKRNEICTDGYIYZKTHNSIRFXYPFUEOCKRNEICTDGYIYZKTHNSIRFXYPFUEOCKRNEICTDGYIYZkrypton6@bandit:/tmp/juan1$ nano solveCypher.py
```



```
krypton6@bandit:/tmp/juan1$ python3 ./solveCypher.py
LFSRISNOTRANDOM
```

Enjoy your stay!

krypton7@bandit:~\$ |