Eric Sisson

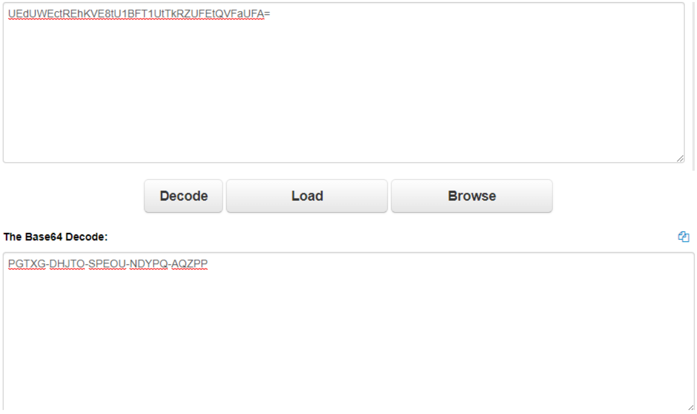
8/16/19

CS 373

Final Write Up

Obtaining an Account

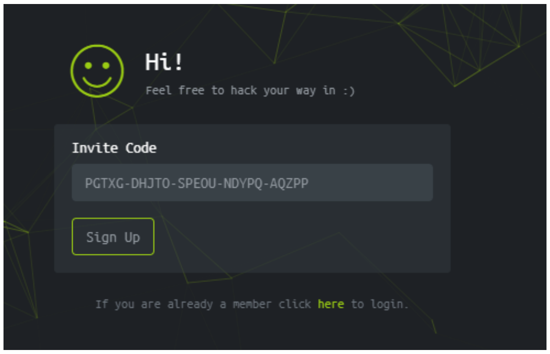
Below is the code I generated using the makeInviteCode function and used to create an account.



```
UEdUWEctREhKVE8tU1BFT1UtTkRZUFEtQVFaUFA=
```

The Base64 Decode:

```
PGTXG-DHJTO-SPEOU-NDYPQ-AQZPP
```



Hi!

Feel free to hack your way in :)

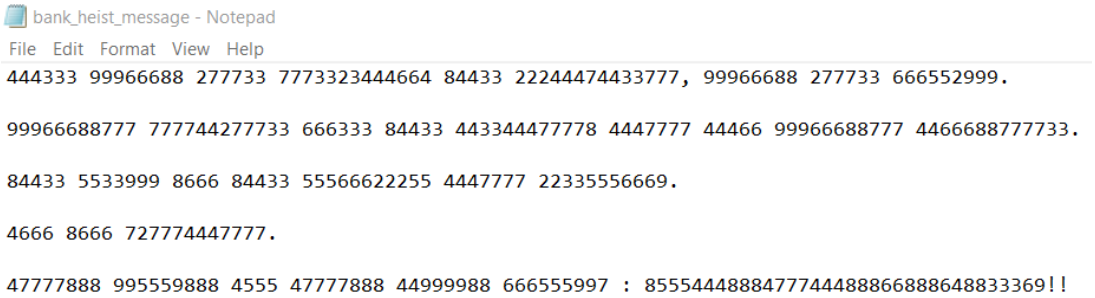
Invite Code: PGTXG-DHJTO-SPEOU-NDYPQ-AQZPP

If you are already a member click here to login.

Congratulations!

Challenge 1: Bank Heist (Crypto – 20 points)

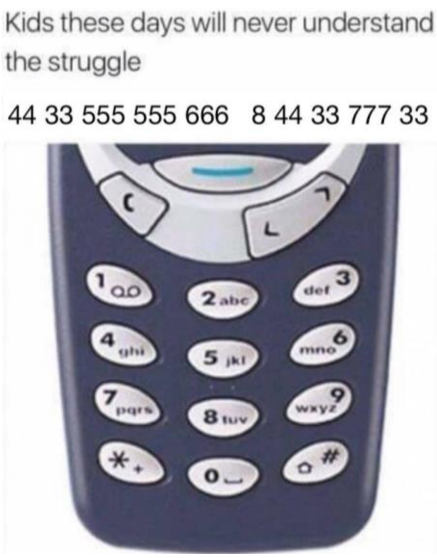
The setup for this challenge goes as follows: “You get to the scene of a bank heist and find that you have caught one person. Under further analysis of the persons flip phone you see a message that seems suspicious. Can you figure out what the message to put this guy in jail?”. The challenge has a single text file to decrypt and is shown below.



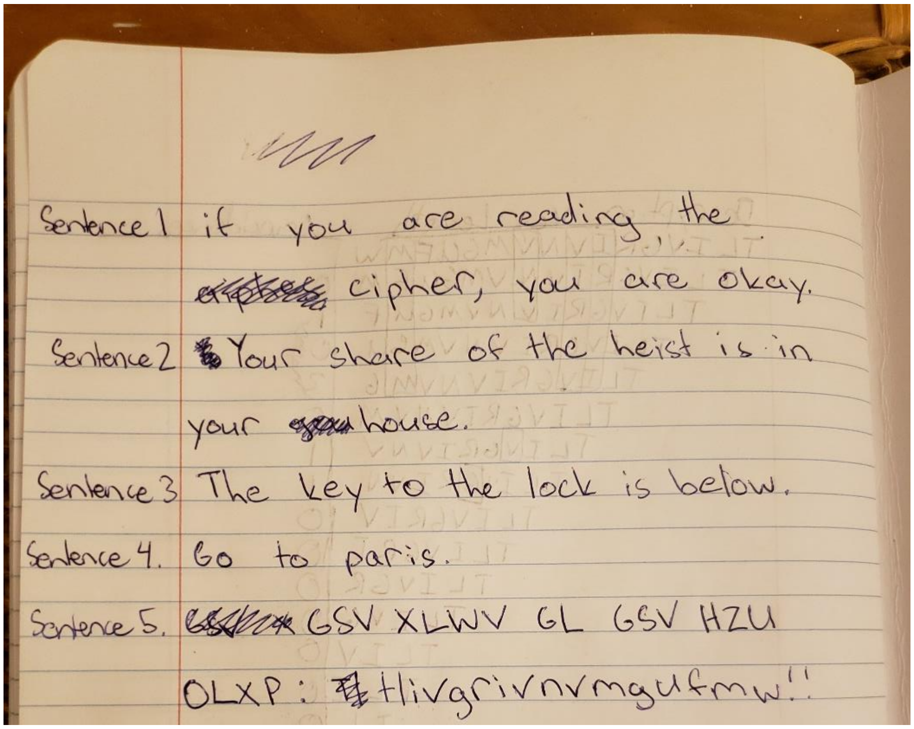
bank_heist_message - Notepad

```
444333 99966688 277733 7773323444664 84433 22244474433777, 99966688 277733 666552999.

99966688777 777744277733 666333 84433 443344477778 4447777 44466 99966688777 4466688777733.

84433 5533999 8666 84433 55566622255 4447777 22335556669.

4666 8666 727774447777.

47777888 995559888 4555 47777888 44999988 666555997 : 855544488847774448886688864883369!!
```

Initially, I started plugging in the numbers into various decoders. I used sites like https://jackstromberg.com/letters-numbers-encoder-decoder/ and https://cryptii.com/ to do this. I couldn't find anything so I started looking for different numbers to letter encryption techniques. I finally made progress when I found a reddit post (https://www.reddit.com/r/PrequelMemes/comments/9zl0fr/imagine_not_having_holograms/) that was making a joke using the picture below.

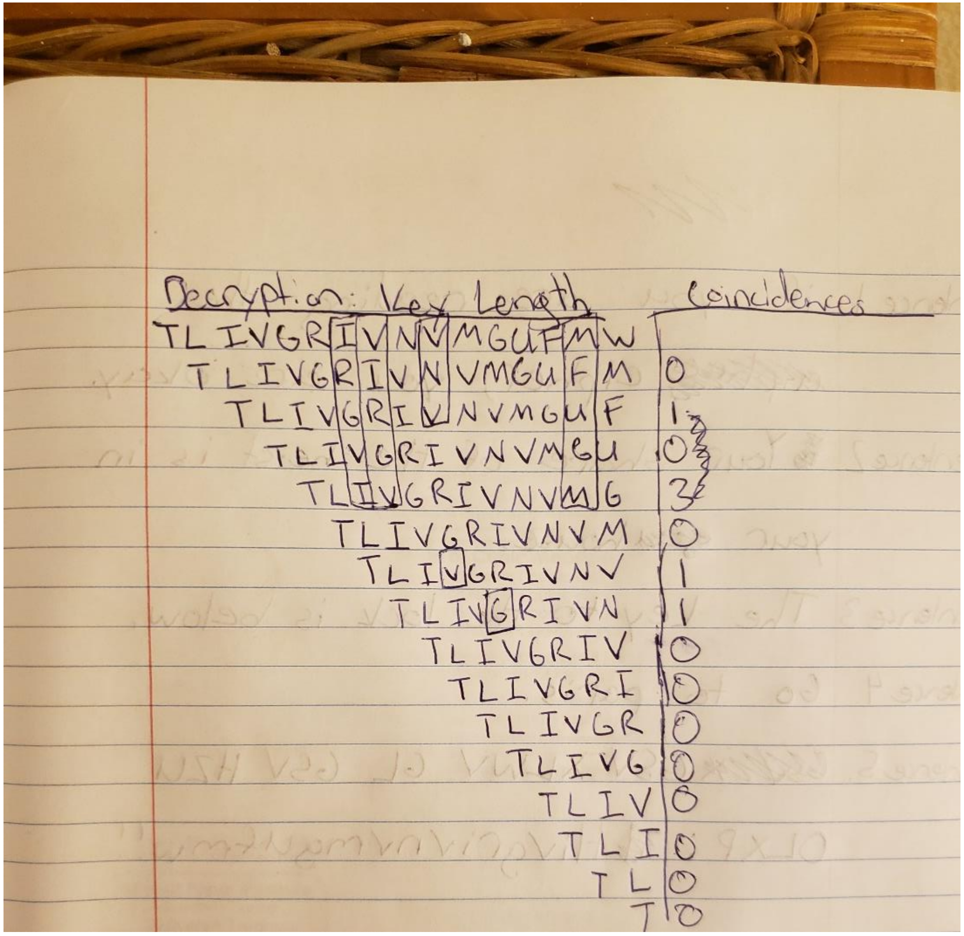


It hadn't occurred to me that the numbers were a message using phone keypads. After discovering this I was able to translate the numbers to text. With the translation, I can see that the money stolen from the bank is in the robber's home in a safe. The key is in the message but it looks like gibberish and can't be read.



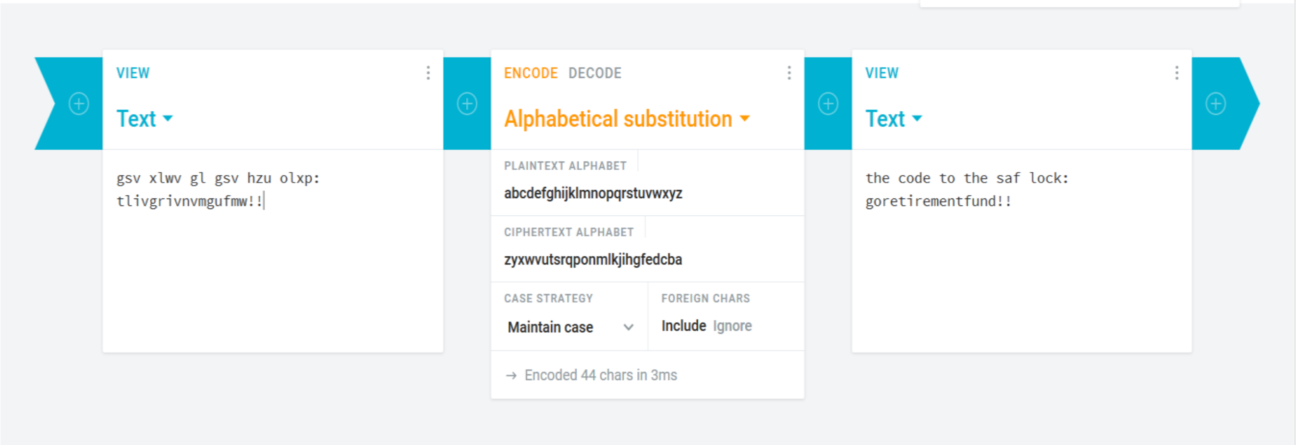
Sentence 1 if you are reading the
cipher, you are okay.
Sentence 2 Your share of the heist is in
your house.
Sentence 3 The key to the lock is below.
Sentence 4. Go to paris.
Sentence 5. GSV XLWV GL GSV HZU
OLXP: tlivgrivnvmgufmw!!

Looking at the wording, I thought the text was being clever by pointing out the decryption technique is related to Paris. Because of this I looked up different encryption systems related to France and found the Vigenère cipher. I began using Cryptii's online vigenere cipher tool to try and decrypt the message. However, I couldn't decrypt it no matter what key I used. I tried "Paris", "France", "gotoparis", "gtp", and even "below", but none of the keys were working. I even looked up how to decrypt a vigenere cipher without a key with this YouTube video: https://www.youtube.com/watch?v=LaWp_Kq0cKs.



```
Decryption: Key Length            Coincidences
TLIVGRIVNVMGUFMW
 TLIVGRIVNVMGUFM                  0
  TLIVGRIVNVMGUF                  1
   TLIVGRIVNVMGU                  0
    TLIVGRIVNVMG                  3
     TLIVGRIVNVM                  0
      TLIVGRIVNV                  1
       TLIVGRIVN                  1
        TLIVGRIV                  0
         TLIVGRI                  0
          TLIVGR                  0
           TLIVG                  0
            TLIV                  0
             TLI                  0
              TL                  0
               T                  0
```

Ultimately, I gave up on the vigenere cipher and began playing with Cryptii's other tools. I found that using the alphabetical substitution tool for Atbash Latin was able to decrypt the message. What I thought was more complex ended up just having me substitute the alphabet with its reverse. With that, the final message is "If you are reading the cipher, you are okay. Your share of the heist is in your house. The key to the lock is below. Go to Paris. The code to the safe lock: goretirementfund!!”. The flag submitted was HTB{GORETIREMENTFUND!!}.



```
gsv xlwv gl gsv hzu olxp:
tlivgrivnvmgufmw!!
```

PLAINTEXT ALPHABET: abcdefghijklmnopqrstuvwxyz

CIPHERTEXT ALPHABET: zyxwvutsrqponmlkjihgfedcba

CASE STRATEGY: Maintain case

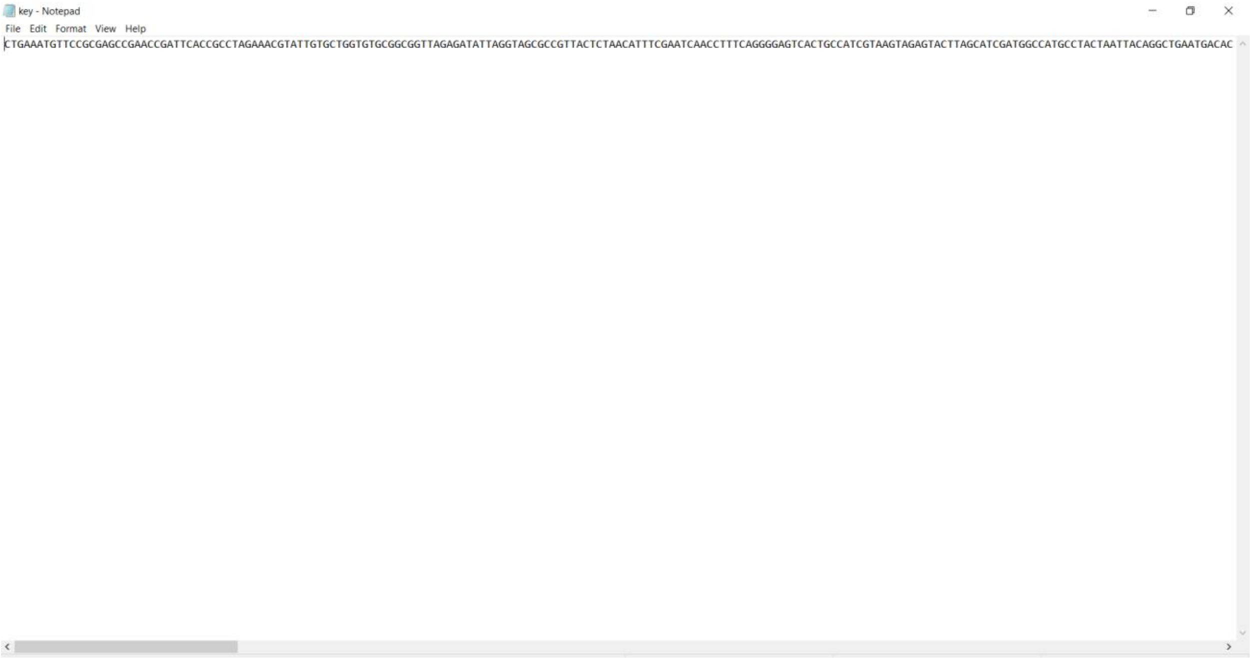
FOREIGN CHARS: Include Ignore

→ Encoded 44 chars in 3ms

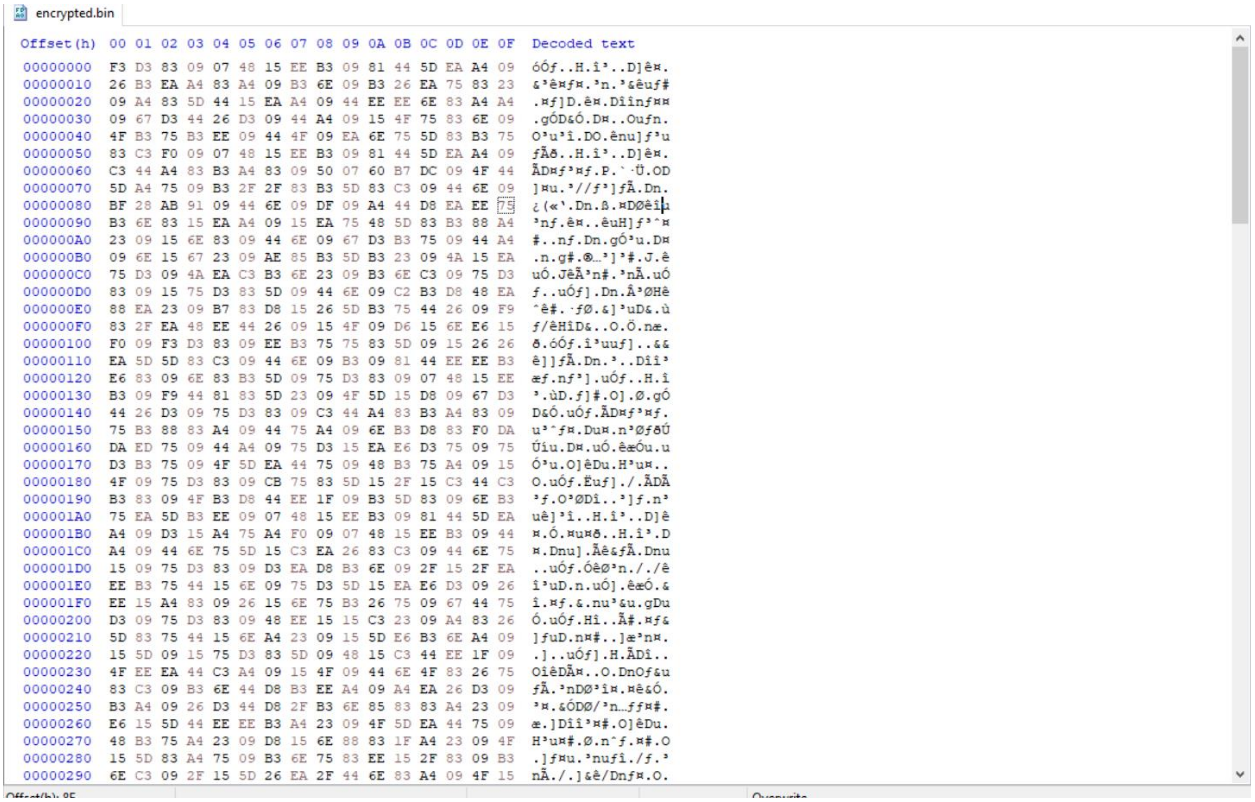
```
the code to the saf lock:
goretirementfund!!
```

Challenge 2: Ebola Virus (Crypto – 100 points)

The challenge tells me that “We suspect that some terrorists have a plan to use the Ebola virus. We have managed to collect an encrypted message and its key. Can you help us decrypt the message?”. The challenge provides a key and an encrypted bin file. Below are pictures of the two files.



```
CTGAAATGTTCCGCGAGCCGAACCGATTCACCGCCTAGAAACGTATTGTGCTGGTGTGCGGCGGTTAGAGATATTAGGTAGCGCCGTTACTCTAACATTTCGAATCAACCTTTCAGGGGAGTCACTGCCATCGTAAGTAGAGTACTTAGCATCGATGGCCATGCCTACTAATTACAGGCTGAATGACAC
```

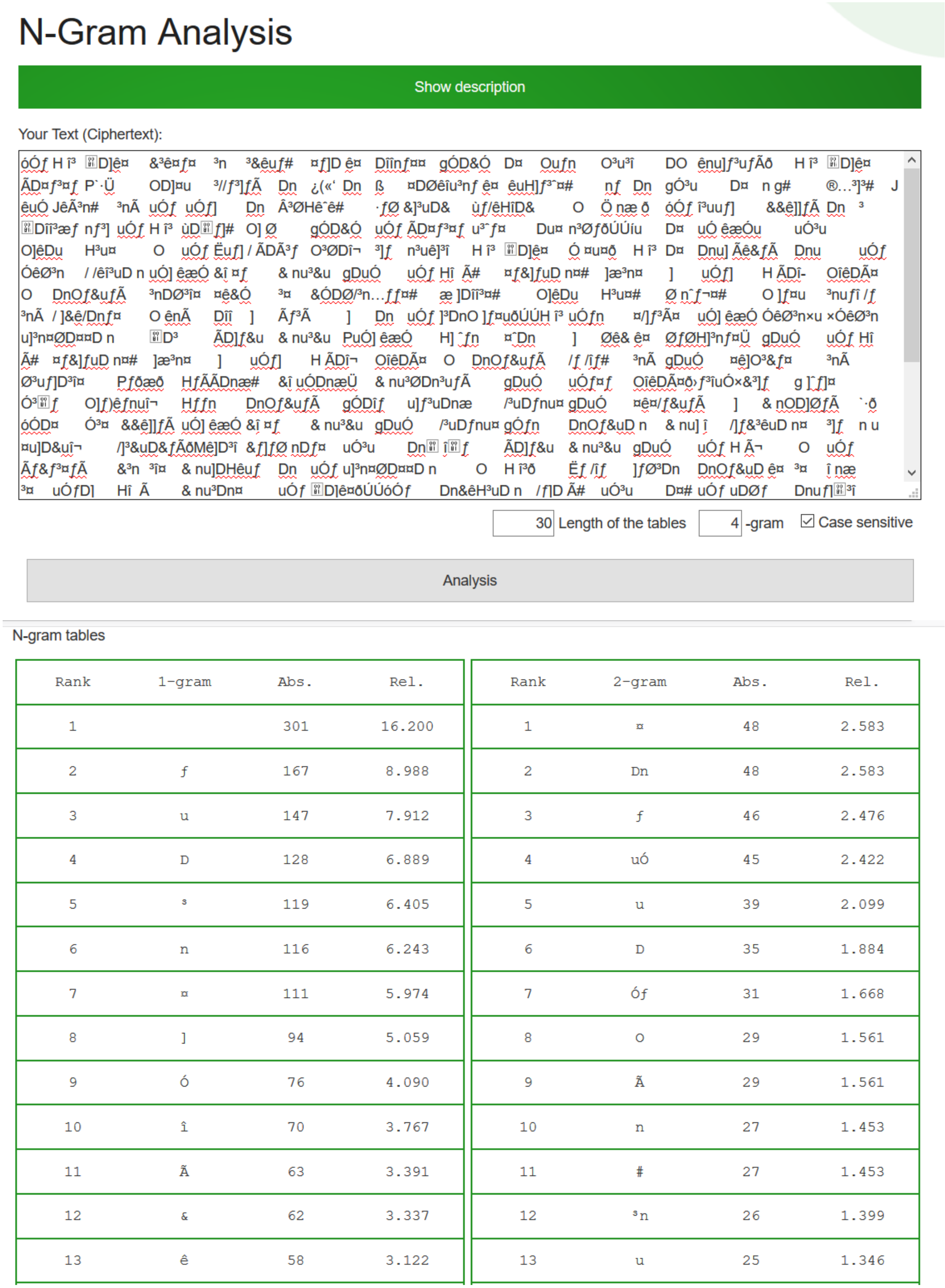


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  F3 D3 83 09 07 48 15 EE B3 09 81 44 5D EA A4 09  óÓƒ..H.î³..D]ê¤.
00000010  26 B3 EA A4 83 A4 09 B3 6E 09 B3 26 EA 75 83 23  &³ê¤ƒ¤.³n.³&êuƒ#
00000020  09 A4 83 5D 44 15 EA A4 09 44 EE EE 6E 83 A4 A4  .¤ƒ]D.ê¤.Dîînƒ¤¤
00000030  09 67 D3 44 26 D3 09 44 A4 09 15 4F 75 83 6E 09  .gÓD&Ó.D¤..Ouƒn.
00000040  4F B3 75 B3 EE 09 44 4F 09 EA 6E 75 5D 83 B3 75  O³u³î.DO.ênu]ƒ³u
00000050  83 C3 F0 09 07 48 15 EE B3 09 81 44 5D EA A4 09  ƒÃð..H.î³..D]ê¤.
00000060  C3 44 A4 83 B3 A4 83 09 50 07 60 B7 DC 09 4F 44  ÃD¤ƒ³¤ƒ.P.`·Ü.OD
00000070  5D A4 75 09 B3 2F 2F 83 B3 5D 83 C3 09 44 6E 09  ]¤u.³//ƒ³]ƒÃ.Dn.
00000080  BF 28 AB 91 09 44 6E 09 DF 09 A4 44 D8 EA EE 75  ¿(«'.Dn.ß.¤DØêîu
00000090  B3 6E 83 15 EA A4 09 15 EA 75 48 5D 83 B3 88 A4  ³nƒ.ê¤..êuH]ƒ³ˆ¤
000000A0  23 09 15 6E 83 09 44 6E 09 67 D3 B3 75 09 44 A4  #..nƒ.Dn.gÓ³u.D¤
000000B0  09 6E 15 67 23 09 AE 85 B3 5D B3 23 09 4A 15 EA  .n.g#.®…³]³#.J.ê
000000C0  75 D3 09 4A EA C3 B3 6E 23 09 B3 6E C3 09 75 D3  uÓ.JêÃ³n#.³nÃ.uÓ
000000D0  83 09 15 75 D3 83 5D 09 44 6E 09 C2 B3 D8 48 EA  ƒ..uÓƒ].Dn.Â³ØHê
000000E0  88 EA 23 09 B7 83 D8 15 26 5D B3 75 44 26 09 F9  ˆê#.·ƒØ.&]³uD&.ù
000000F0  83 2F EA 48 EE 44 26 09 15 4F 09 D6 15 6E E6 15  ƒ/êHîD&..O.Ö.næ.
00000100  F0 09 F3 D3 83 09 EE B3 75 75 83 5D 09 15 26 26  ð.óÓƒ.î³uuƒ]..&&
00000110  EA 5D 5D 83 C3 09 44 6E 09 B3 09 81 44 EE EE B3  ê]]ƒÃ.Dn.³..Dîî³
00000120  E6 83 09 6E 83 B3 5D 09 75 D3 83 09 07 48 15 EE  æƒ.nƒ³].uÓƒ..H.î
00000130  B3 09 F9 44 81 83 5D 23 09 4F 5D 15 D8 09 67 D3  ³.ùD.ƒ]#.O].Ø.gÓ
00000140  44 26 D3 09 75 D3 83 09 C3 44 A4 83 B3 A4 83 09  D&Ó.uÓƒ.ÃD¤ƒ³¤ƒ.
00000150  75 B3 88 83 A4 09 44 75 A4 09 6E B3 D8 83 F0 DA  u³ˆƒ¤.Du¤.n³ØƒðÚ
00000160  DA ED 75 09 44 A4 09 75 D3 15 EA E6 D3 75 09 75  Úíu.D¤.uÓ.êæÓu.u
00000170  D3 B3 75 09 4F 5D EA 44 75 09 48 B3 75 A4 09 15  Ó³u.O]êDu.H³u¤..
00000180  4F 09 75 D3 83 09 CB 75 83 5D 15 2F 15 C3 44 C3  O.uÓƒ.Ëuƒ]./.ÃDÃ
00000190  B3 83 09 4F B3 D8 44 EE 1F 09 B3 5D 83 09 6E B3  ³ƒ.O³ØDî..³]ƒ.n³
000001A0  75 EA 5D B3 EE 09 07 48 15 EE B3 09 81 44 5D EA  uê]³î..H.î³..D]ê
000001B0  A4 09 D3 15 A4 75 A4 F0 09 07 48 15 EE B3 09 44  ¤.Ó.¤u¤ð..H.î³.D
000001C0  A4 09 44 6E 75 5D 15 C3 EA 26 83 C3 09 44 6E 75  ¤.Dnu].Ãê&ƒÃ.Dnu
000001D0  15 09 75 D3 83 09 D3 EA D8 B3 6E 09 2F 15 2F EA  ..uÓƒ.ÓêØ³n./../ê
000001E0  EE B3 75 44 15 6E 09 75 D3 5D 15 EA E6 D3 09 26  î³uD.n.uÓ].êæÓ.&
000001F0  EE 15 A4 83 09 26 15 6E 75 B3 26 75 09 67 44 75  î.¤ƒ.&.nu³&u.gDu
00000200  D3 09 75 D3 83 09 48 EE 15 15 C3 23 09 A4 83 26  Ó.uÓƒ.Hî..Ã#.¤ƒ&
00000210  5D 83 75 44 15 6E A4 23 09 15 5D E6 B3 6E A4 09  ]ƒuD.n¤#..]æ³n¤.
00000220  15 5D 09 15 75 D3 83 5D 09 48 15 C3 44 EE 1F 09  .]..uÓƒ].H.ÃDî..
00000230  4F EE EA 44 C3 A4 09 15 4F 09 44 6E 4F 83 26 75  OîêDÃ¤..O.DnOƒ&u
00000240  83 C3 09 B3 6E 44 D8 B3 EE A4 09 A4 EA 26 D3 09  ƒÃ.³nDØ³î¤.¤ê&Ó.
00000250  B3 A4 09 26 D3 44 D8 2F B3 6E 85 83 83 A4 23 09  ³¤.&ÓDØ/³n…ƒƒ¤#.
00000260  E6 15 5D 44 EE EE B3 A4 23 09 4F 5D EA 44 75 09  æ.]Dîî³¤#.O]êDu.
00000270  48 B3 75 A4 23 09 D8 15 6E 88 83 1F A4 23 09 4F  H³u¤#.Ø.nˆƒ.¤#.O
00000280  15 5D 83 A4 75 09 B3 6E 75 83 EE 15 2F 83 09 B3  .]ƒ¤u.³nuƒî./ƒ.³
00000290  6E C3 09 2F 15 5D 26 EA 2F 44 6E 83 A4 09 4F 15  nÃ./.]&ê/Dnƒ¤.O.
```

The first thing I did was take the decoded text and key and try to decrypt the text using https://cryptii.com/. I placed the encrypted text and used every technique that required a key. I couldn't find anything so I started looking for ways to decrypt bin files. Unfortunately, there isn't really a way other than manually or with a script (https://stackoverflow.com/questions/12167839/depack-decrypt-extract-application-bin-files).

Looking back on Hack the Box, I found some hints in the forums for people doing the challenge. The first one is that there are two ways of solving it, and one of them doesn't require the key. Apparently this is actually how most people solved this problem and what I assume is the "manual" way of decrypting the code (https://forum.hackthebox.eu/discussion/1402/crypto-about-ebola-virus-key). The other hint is that one of the ways, what I assume is the way without the key, is take frequency analysis into account (https://forum.hackthebox.eu/discussion/309/get-stuck-on-ebola#alamot).

Frequency analysis is finding the frequency of characters in encrypted data and compare those frequencies against the most frequent characters in English communication. The first site I used to analyze the bin file was https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html. However, it wasn't recognizing special characters like ƒ or Ó. So I found this site: https://www.cryptool.org/en/cto-cryptanalysis/n-gram-analysis. The results when putting in the decrypted bin file is listed below.



N-Gram Analysis

Your Text (Ciphertext):

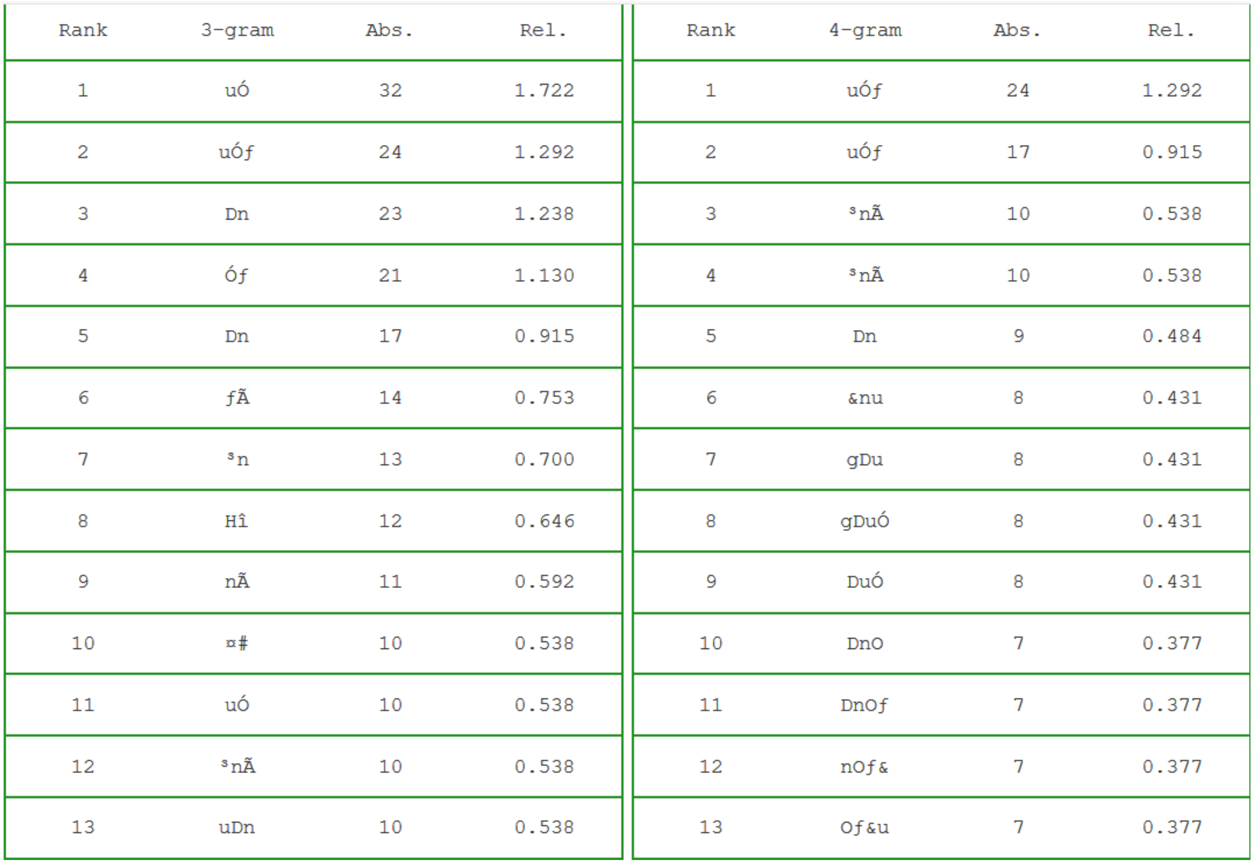
```
óÓƒ H î³ □D]ê¤   &³ê¤ƒ¤   ³n   ³&êuƒ#   ¤ƒ]D ê¤   Dîînƒ¤¤   gÓD&Ó   D¤   Ouƒn   O³u³î   DO  ênu]ƒ³uƒÃð   H î³ □D]ê¤
ÃD¤ƒ³¤ƒ P`·Ü   OD]¤u   ³//ƒ³]ƒÃ   Dn   ¿(«'  Dn   ß   ¤DØêîu³nƒ ê¤  êuH]ƒ³ˆ¤#   nƒ  Dn  gÓ³u   D¤   n g#   ®…³]³#   J
êuÓ JêÃ³n#   ³nÃ  uÓƒ  uÓƒ]   Dn   Â³ØHêˆê#   ·ƒØ &]³uD&   ùƒ/êHîD&   O   Ö næ ð   óÓƒ î³uuƒ]   &&ê]]ƒÃ  Dn   ³
□Dîî³æƒ nƒ³]  uÓƒ H î³  ùD□ƒ]#  O] Ø   gÓD&Ó  uÓƒ ÃD¤ƒ³¤ƒ  u³ˆƒ¤   Du¤ n³ØƒðÚÚíu   D¤   uÓ êæÓu   uÓ³u
O]êDu   H³u¤   O   uÓƒ Ëuƒ] / ÃDÃ³ƒ  O³ØDî¬  ³]ƒ   n³uê]³î   H î³ □D]ê¤   Ó ¤u¤ð   H î³  D¤   Dnu] Ãê&ƒÃ   Dnu   uÓƒ
ÓêØ³n   / /êî³uD n uÓ] êæÓ &î ¤ƒ   & nu³&u   gDuÓ   uÓƒ Hî  Ã#   ¤ƒ&]ƒuD n¤#   ]æ³n¤   ]   uÓƒ]   H ÃDî-   OîêDÃ¤
O   DnOƒ&uƒÃ   ³nDØ³î¤   ¤ê&Ó   ³¤   &ÓDØ/³n…ƒƒ¤#   æ ]Dîî³¤#   O]êDu   H³u¤#   Ø nˆƒ¬¤#   O ]ƒ¤u   ³nuƒî /ƒ
³nÃ  / ]&ê/Dnƒ¤   O ênÃ   Dîî   ]   Ãƒ³Ã   ]   Dn  uÓƒ ]³DnO ]ƒ¤uðÚÚH î³ uÓƒn   ¤/]ƒ³Ã¤   uÓ] êæÓ ÓêØ³n×u ×ÓêØ³n
u]³n¤ØD¤¤D n   □D³   ÃD]ƒ&u   & nu³&u   PuÓ] êæÓ   H] ˆƒn   ¤ˆDn   ]   Øê& ê¤   ØƒØH]³nƒ¤Ü  gDuÓ   uÓƒ Hî
Ã#   ¤ƒ&]ƒuD n¤#   ]æ³n¤   ]   uÓƒ]   H ÃDî¬   OîêDÃ¤   O   DnOƒ&uƒÃ   /ƒ /îƒ#   ³nÃ  gDuÓ   ¤ê]O³&ƒ¤   ³nÃ
Ø³uƒ]D³î¤   Pƒðæð   HƒÃÃDnæ#   &î uÓDnæÜ   & nu³ØDn³uƒÃ   gDuÓ   uÓƒ¤ƒ   OîêDÃ¤ð›ƒ³îuÓ×&³]ƒ   g ]ˆƒ]¤
Ó³□ƒ   O]ƒ)êƒnuî¬   Hƒƒn   DnOƒ&uƒÃ   gÓDîƒ   u]ƒ³uDnæ   /³uDƒnu¤ gDuÓ   ¤ê¤/ƒ&uƒÃ   ]   & nOD]ØƒÃ   `·ð
óÓD¤   Ó³¤   &&ê]]ƒÃ  uÓ] êæÓ &î ¤ƒ   & nu³&u  gDuÓ   /³uDƒnu¤ gÓƒn   DnOƒ&uD n   & nu] î   /]ƒ&³êuD n¤   ³]ƒ   n u
¤u]D&uî¬   /]³&uD&ƒÃðMê]D³î  &ƒ]ƒØ nDƒ¤   uÓ³u   Dn□ î□ƒ   ÃD]ƒ&u   & nu³&u   gDuÓ   uÓƒ H Ã¬   O   uÓƒ
Ãƒ&ƒ³¤ƒÃ   &³n  ³î¤   & nu]DHêuƒ   Dn   uÓƒ u]³n¤ØD¤¤D n   O   H î³ð   Ëƒ /îƒ   ]ƒØ³Dn   DnOƒ&uD ê¤  ³¤   î næ
³¤   uÓƒD]   Hî  Ã   & nu³Dn¤   uÓƒ □D]ê¤ðÚÚóÓƒ Dn&êH³uD n   /ƒ]D Ã#   uÓ³u   D¤#  uÓƒ uDØƒ   Dnuƒ]□³î
```

30 Length of the tables 4 -gram ☑ Case sensitive

N-gram tables

Rank	1-gram	Abs.	Rel.
1		301	16.200
2	ƒ	167	8.988
3	u	147	7.912
4	D	128	6.889
5	³	119	6.405
6	n	116	6.243
7	¤	111	5.974
8	]	94	5.059
9	Ó	76	4.090
10	î	70	3.767
11	Ã	63	3.391
12	&	62	3.337
13	ê	58	3.122

Rank	2-gram	Abs.	Rel.
1	¤	48	2.583
2	Dn	48	2.583
3	ƒ	46	2.476
4	uÓ	45	2.422
5	u	39	2.099
6	D	35	1.884
7	Óƒ	31	1.668
8	O	29	1.561
9	Ã	29	1.561
10	n	27	1.453
11	#	27	1.453
12	³n	26	1.399
13	u	25	1.346



Rank	3-gram	Abs.	Rel.
1	uÓ	32	1.722
2	uÓƒ	24	1.292
3	Dn	23	1.238
4	Óƒ	21	1.130
5	Dn	17	0.915
6	ƒÃ	14	0.753
7	³n	13	0.700
8	Hî	12	0.646
9	nÃ	11	0.592
10	¤#	10	0.538
11	uÓ	10	0.538
12	³nÃ	10	0.538
13	uDn	10	0.538

Rank	4-gram	Abs.	Rel.
1	uÓƒ	24	1.292
2	uÓƒ	17	0.915
3	³nÃ	10	0.538
4	³nÃ	10	0.538
5	Dn	9	0.484
6	&nu	8	0.431
7	gDu	8	0.431
8	gDuÓ	8	0.431
9	DuÓ	8	0.431
10	DnO	7	0.377
11	DnOƒ	7	0.377
12	nOƒ&	7	0.377
13	Oƒ&u	7	0.377

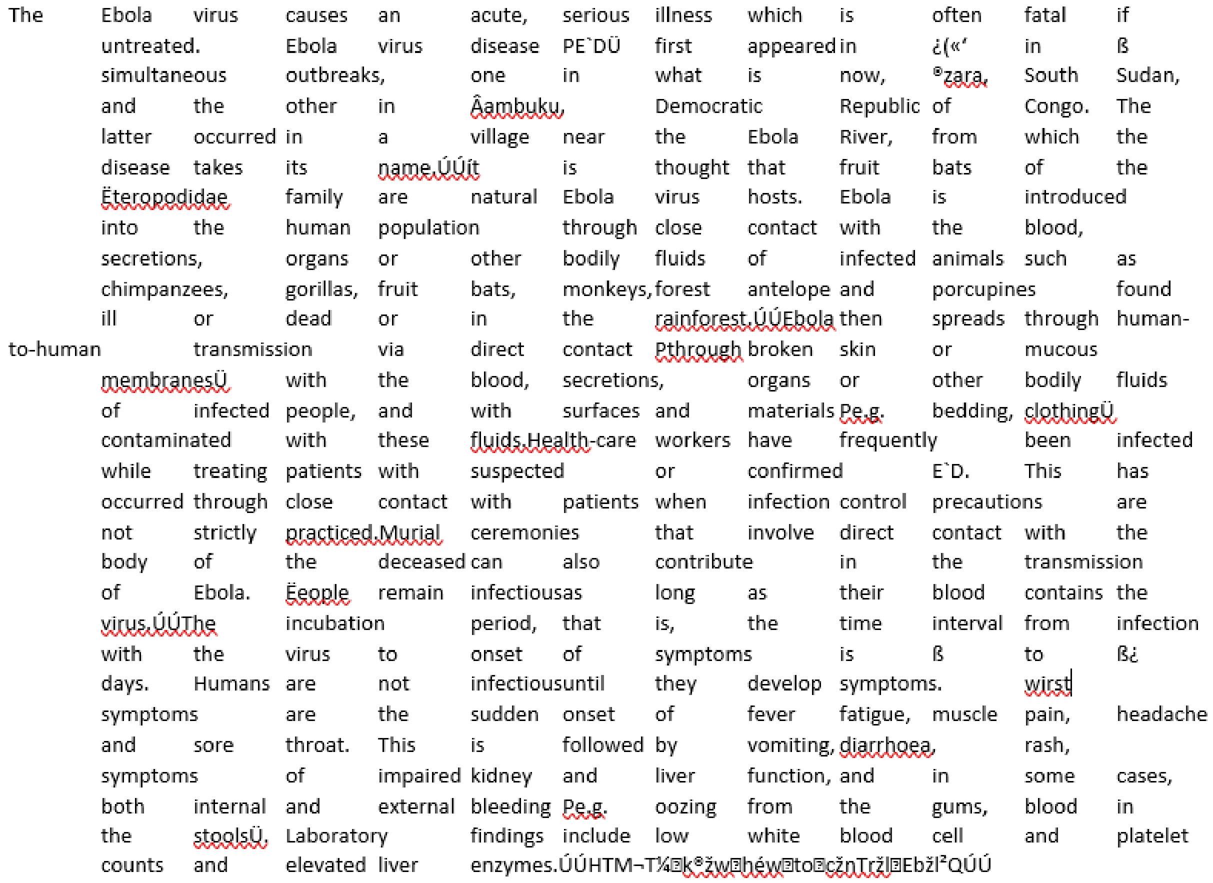
Looking at the results and information on the most common letters (https://learncryptography.com/attack-vectors/frequency-analysis), I could see what characters are meant to be. For example, the most common letter is "e", and the results show that *ƒ* is the most common character in the bin file. From here I started replacing letters in the bin file until something coherent starts forming. I also guessed letters based on the words already formed. For example in this picture, ¤.th³t.Dn..î.e.Ã , I see the word "th³t", but I can guess it's the word "that", and therefore the character "³" is "a".

I also noticed that there were case sensitive characters. For example in this picture, óhe.., h is "Ó" but "ó" is a different letter. I figured ó is a capital "T" since it is at the beginning of a sentence. Along with that there are periods with different hex numbers that appear to be a letter. In this picture we can assume the period in c.ntact , is supposed to be an "o". This period has a different hex value then the spaces and should be replaced differently.

Original	Replacement
u	t
Ó	h
ƒ	e
¤	s
³	a
ê	u

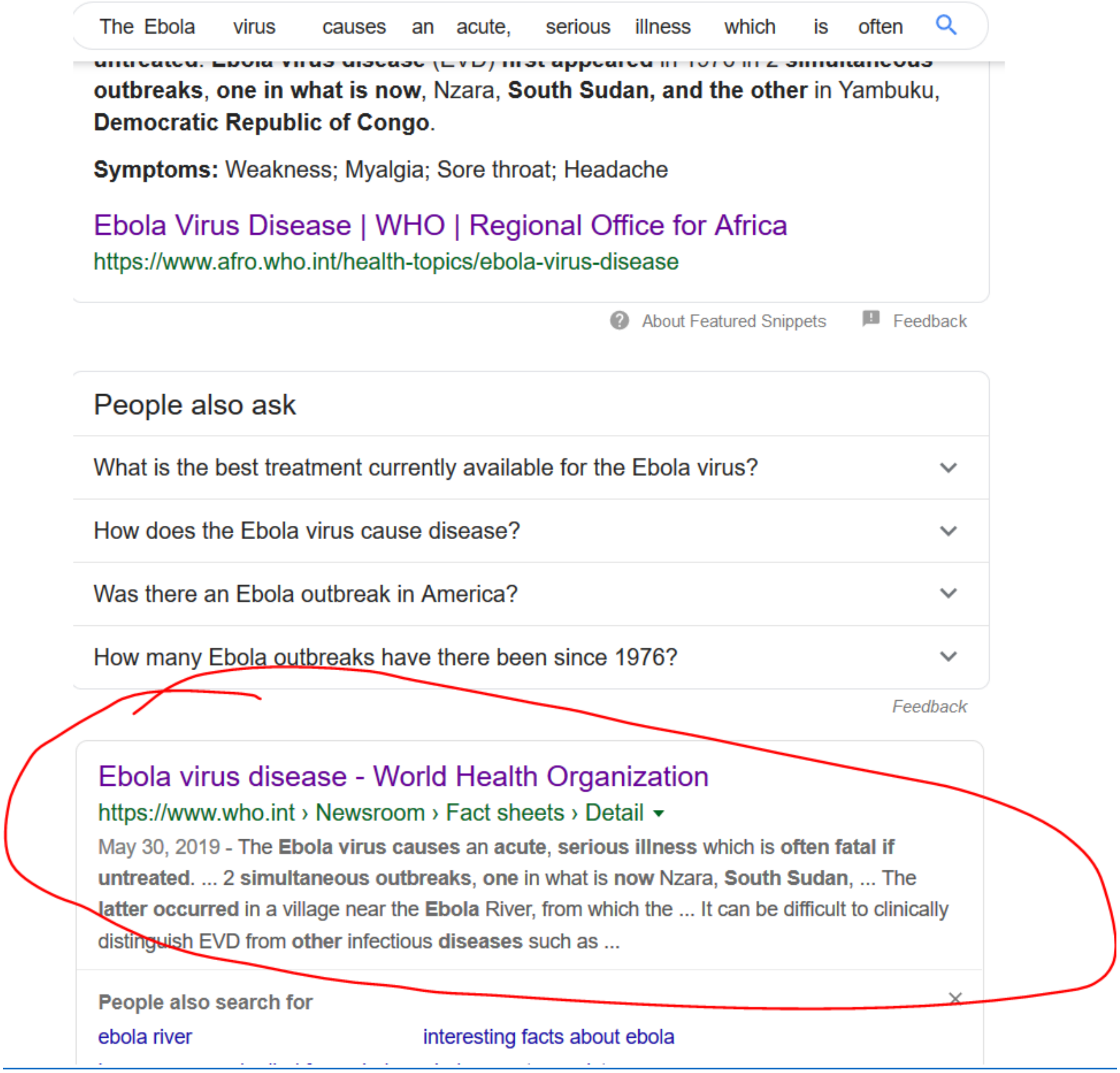
&	c
ó	T
î	l
D	i
Hex: 15	o
]	r
g	w
Hex: 81	v
H	b
Ã	d
Hex: 07	E
/	p
ˆ	k
Ø	m
æ	g
#	,
Hex: 1F	y
ð	.
…	z
\	L
·	d
ù	R
Ö	C
·	D
J	S
Hex: 00	x
›	H
)	q
×	-

With this much finish we can see that there is an actual essay in the text.



The Ebola virus causes an acute, serious illness which is often fatal if
untreated. Ebola virus disease PE`DÜ first appeared in ¿(«' in ß
simultaneous outbreaks, one in what is now, ®zara, South Sudan,
and the other in Âambuku, Democratic Republic of Congo. The
latter occurred in a village near the Ebola River, from which the
disease takes its name.ÚÚít is thought that fruit bats of the
Ëteropodidae family are natural Ebola virus hosts. Ebola is introduced
into the human population through close contact with the blood,
secretions, organs or other bodily fluids of infected animals such as
chimpanzees, gorillas, fruit bats, monkeys, forest antelope and porcupines found
ill or dead or in the rainforest.ÚÚEbola then spreads through human-
to-human transmission via direct contact Pthrough broken skin or mucous
membranesÜ with the blood, secretions, organs or other bodily fluids
of infected people, and with surfaces and materials Pe.g. bedding, clothingÜ
contaminated with these fluids.Health-care workers have frequently been infected
while treating patients with suspected or confirmed E`D. This has
occurred through close contact with patients when infection control precautions are
not strictly practiced.Murial ceremonies that involve direct contact with the
body of the deceased can also contribute in the transmission
of Ebola. Ëeople remain infectious as long as their blood contains the
virus.ÚÚThe incubation period, that is, the time interval from infection
with the virus to onset of symptoms is ß to ß¿
days. Humans are not infectious until they develop symptoms. wirst
symptoms are the sudden onset of fever fatigue, muscle pain, headache
and sore throat. This is followed by vomiting, diarrhoea, rash,
symptoms of impaired kidney and liver function, and in some cases,
both internal and external bleeding Pe.g. oozing from the gums, blood in
the stoolsÜ. Laboratory findings include low white blood cell and platelet
counts and elevated liver enzymes.ÚÚHTM¬T¼k®žwhéwtočžnTržlEbžl²QÚÚ

Searching the google with the first few lines, I found a website with an exact match of the text (https://www.who.int/news-room/fact-sheets/detail/ebola-virus-disease).



The Ebola virus causes an acute, serious illness which is often

untreated. Ebola virus disease (EVD) first appeared in 1976 in 2 simultaneous outbreaks, one in what is now, Nzara, South Sudan, and the other in Yambuku, Democratic Republic of Congo.

Symptoms: Weakness; Myalgia; Sore throat; Headache

Ebola Virus Disease | WHO | Regional Office for Africa
https://www.afro.who.int/health-topics/ebola-virus-disease

People also ask

What is the best treatment currently available for the Ebola virus?

How does the Ebola virus cause disease?

Was there an Ebola outbreak in America?

How many Ebola outbreaks have there been since 1976?

Ebola virus disease - World Health Organization
https://www.who.int › Newsroom › Fact sheets › Detail

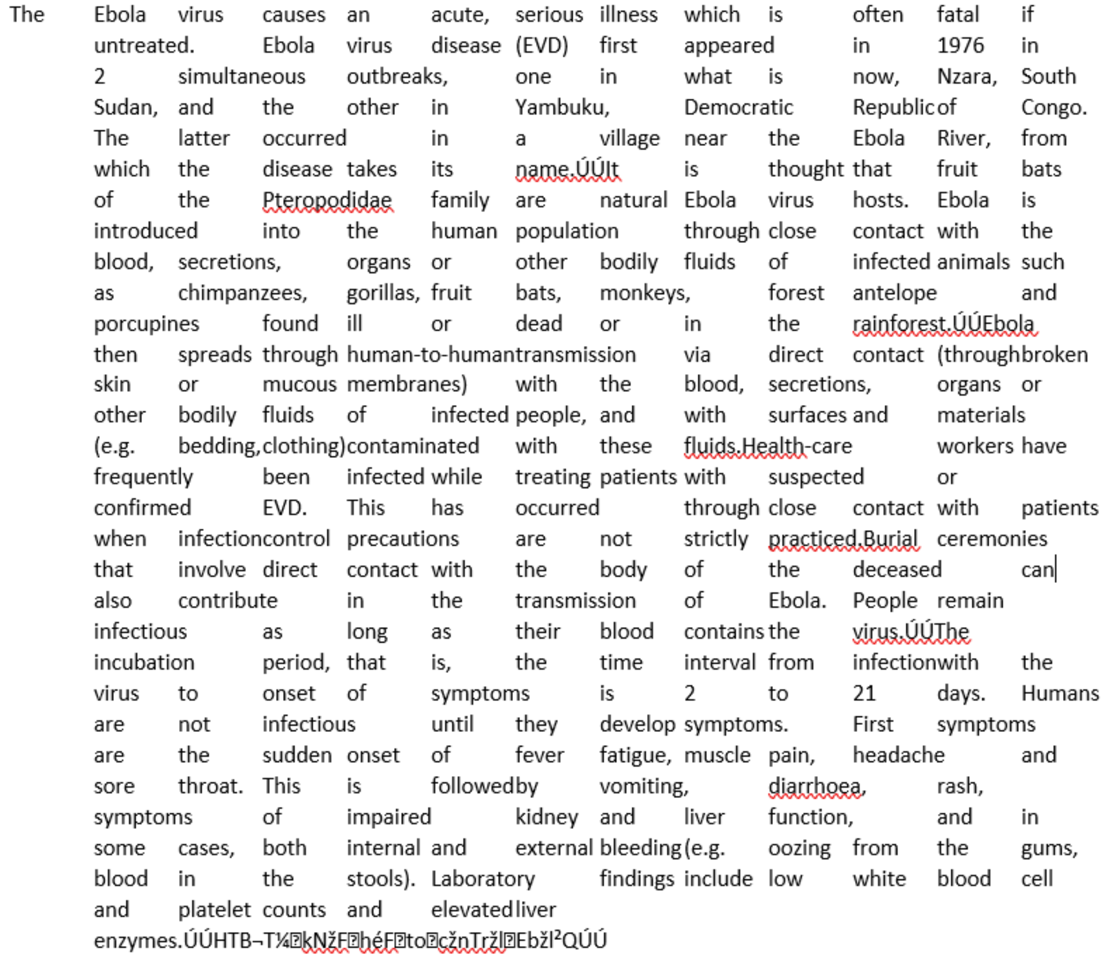
May 30, 2019 - The **Ebola virus causes** an **acute**, **serious illness** which is **often fatal if untreated**. ... 2 **simultaneous outbreaks**, **one** in what is **now** Nzara, **South Sudan**, ... The **latter occurred** in a village near the **Ebola** River, from which the ... It can be difficult to clinically distinguish EVD from **other** infectious **diseases** such as ...

People also search for

ebola river

interesting facts about ebola

With the actual text, I can translate the rest of the encrypted text. With that we get this.

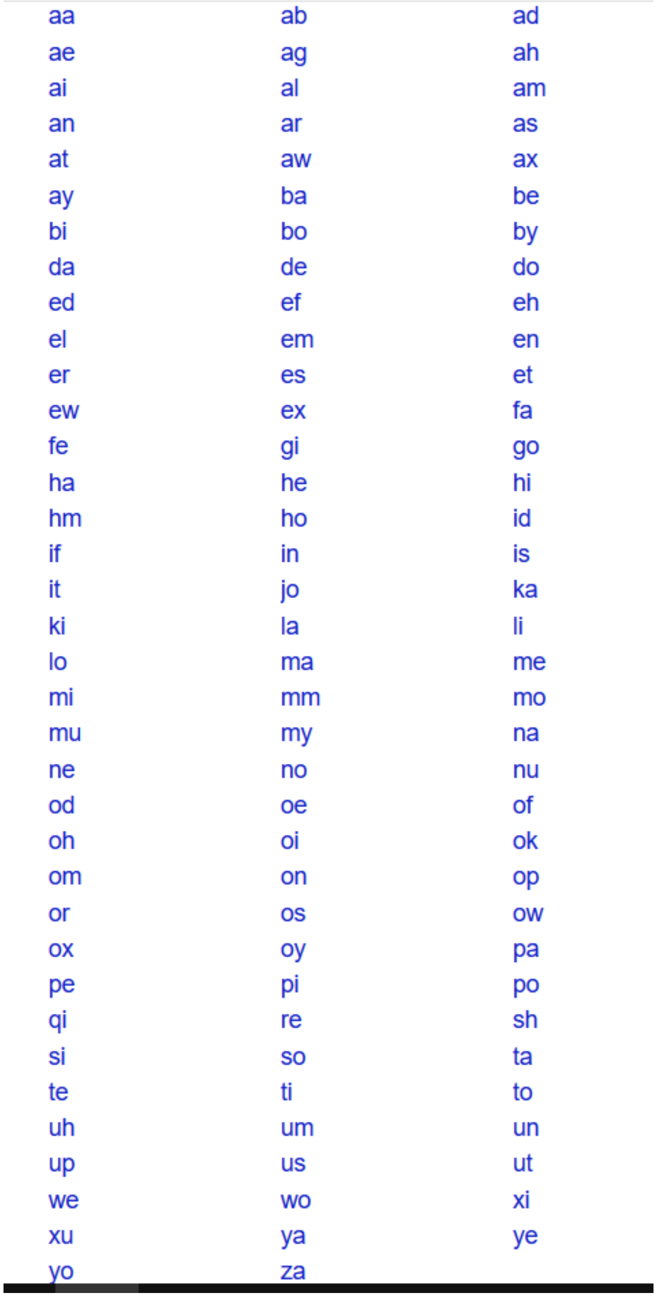


```
The Ebola virus causes an acute, serious illness which is often fatal if
untreated. Ebola virus disease (EVD) first appeared in 1976 in
2 simultaneous outbreaks, one in what is now, Nzara, South
Sudan, and the other in Yambuku, Democratic Republic of Congo.
The latter occurred in a village near the Ebola River, from
which the disease takes its name.ÚÚIt is thought that fruit bats
of the Pteropodidae family are natural Ebola virus hosts. Ebola is
introduced into the human population through close contact with the
blood, secretions, organs or other bodily fluids of infected animals such
as chimpanzees, gorillas, fruit bats, monkeys, forest antelope and
porcupines found ill or dead or in the rainforest.ÚÚEbola
then spreads through human-to-human transmission via direct contact (through broken
skin or mucous membranes) with the blood, secretions, organs or
other bodily fluids of infected people, and with surfaces and materials
(e.g. bedding, clothing) contaminated with these fluids.Health-care workers have
frequently been infected while treating patients with suspected or
confirmed EVD. This has occurred through close contact with patients
when infection control precautions are not strictly practiced.Burial ceremonies
that involve direct contact with the body of the deceased can
also contribute in the transmission of Ebola. People remain
infectious as long as their blood contains the virus.ÚÚThe
incubation period, that is, the time interval from infection with the
virus to onset of symptoms is 2 to 21 days. Humans
are not infectious until they develop symptoms. First symptoms
are the sudden onset of fever fatigue, muscle pain, headache and
sore throat. This is followed by vomiting, diarrhoea, rash,
symptoms of impaired kidney and liver function, and in
some cases, both internal and external bleeding (e.g. oozing from the gums,
blood in the stools). Laboratory findings include low white blood cell
and platelet counts and elevated liver
enzymes.ÚÚHTB¬T¼□kNžF□héF□to□čžnTržl□Ebžl²QÚÚ
```

The last sentence appears to be be the answer that is needed for the challenge. The first thing that can be eliminated from the sentence is “ÚÚ” since this appears to be a break between sentences or paragraphs. I also see that there appears to be 6 words that are separated from one another, and some of them share the same letters. The 5th word, “čžnTržl”, looks like the word “control”, meaning that “ž” is “o”. But we already had an “o” decrypted above, so perhaps it’s a “O” or a “0”? The “T” should stay capitalized since it is one of the letters we decrypted above replacing “ó”.

So now we have “HTB¬T¼kNOFhéFtocOnTrOlEbol²Q”. We see that there is “HTB” in the beginning so perhaps this is in flag format so, “HTB{T¼kNOFhéFtocOnTrOlEbol²}”. The second word looks like “know” so the “F” can be a “w”, “HTB{T¼kNOwhéwtocOnTrOlEbOl²}”. Now the third word looks like “how” so we can replace “é” with “0”. The last word also looks like “Ebola”, but “a” is already taken by “³”. Because of this “²” must be something different like “A”.

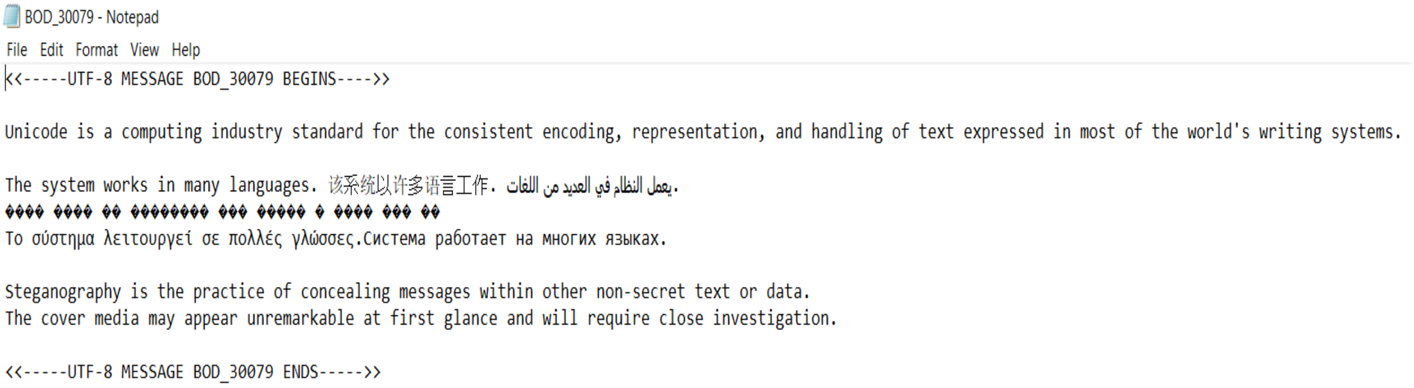
With that the message says “HTB{T¼kNOwh0wtocOnTrOlEbOlA}”. Looking at “T¼”, it looks like a two-letter word. So I looked up all two letter words. From this list of words there, the word that makes the most sense is “we”. A “W” hasn’t been used but “e” and “E” has, so it could be a “3”. The final message should be something among the lines of “W3 kNOw h0w to cOnTrOl EbOlA”. After many tries, the final message is HTB{W3_kN0w_hOw_to_c0nTr0l_Eb0l4}.



aa	ab	ad
ae	ag	ah
ai	al	am
an	ar	as
at	aw	ax
ay	ba	be
bi	bo	by
da	de	do
ed	ef	eh
el	em	en
er	es	et
ew	ex	fa
fe	gi	go
ha	he	hi
hm	ho	id
if	in	is
it	jo	ka
ki	la	li
lo	ma	me
mi	mm	mo
mu	my	na
ne	no	nu
od	oe	of
oh	oi	ok
om	on	op
or	os	ow
ox	oy	pa
pe	pi	po
qi	re	sh
si	so	ta
te	ti	to
uh	um	un
up	us	ut
we	wo	xi
xu	ya	ye
yo	za	

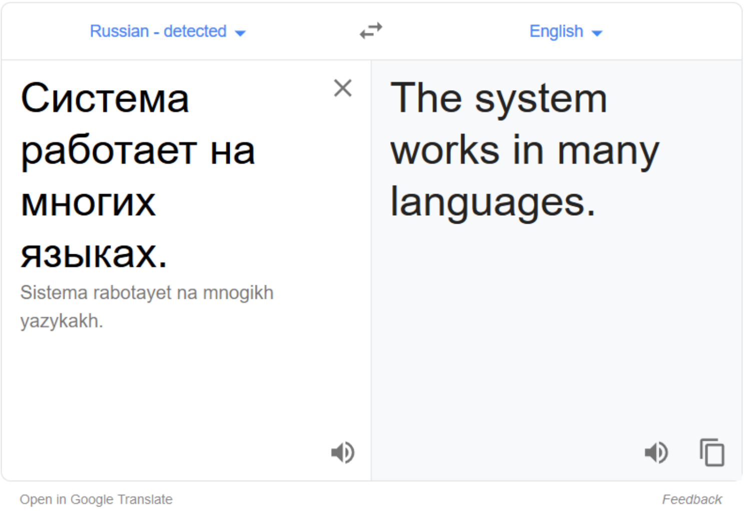
Challenge 3: Unified (Stego– 20 points)

For this challenge we are given a file and are told “This file seems to contain innocuous information. What is the true message?”. The contents of the file is below.



```
<<-----UTF-8 MESSAGE BOD_30079 BEGINS---->>

Unicode is a computing industry standard for the consistent encoding, representation, and handling of text expressed in most of the world's writing systems.

The system works in many languages. 该系统以许多语言工作. يعمل النظام في العديد من اللغات.
���� ���� �� �������� ��� ����� � ���� ��� ��
Το σύστημα λειτουργεί σε πολλές γλώσσες.Система работает на многих языках.

Steganography is the practice of concealing messages within other non-secret text or data.
The cover media may appear unremarkable at first glance and will require close investigation.

<<-----UTF-8 MESSAGE BOD_30079 ENDS----->>
```

It’s clear that I’m supposed to decode the messages to get the HTB flag that has to be submitted. The first thing I did was translate the languages, but they all ended up saying the same thing as thing, “The system works in many languages”.

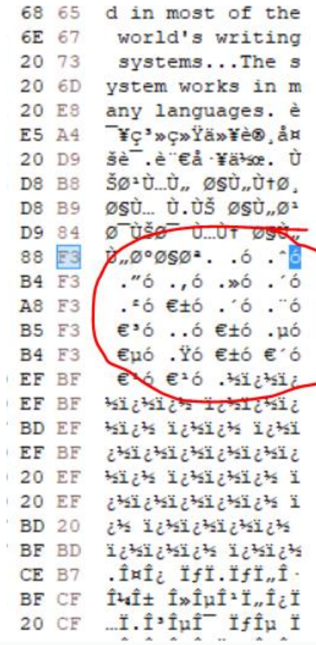


Система работает на многих языках.

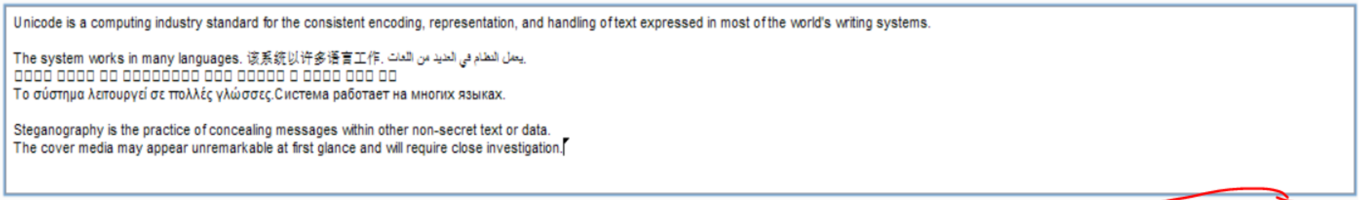
Sistema rabotayet na mnogikh yazykakh.

The system works in many languages.

From here, I decided to use my hex editor to see if that can decode the mystery phrase in the middle. However, it didn't appear to do so, and its characters don't match any characters from the other languages. Because the hex editor couldn't decode, I looked for other tools that could decode the � characters. I actually found on a hack the box forum that I should use a web application called Burp Suite (https://forum.hackthebox.eu/discussion/614/unified-challange). With the decoder function on the application, the � characters were decoded. The phrase is actually a the HTB flag for the challenge which is "HTB {tr1th3m1u5_1499}.



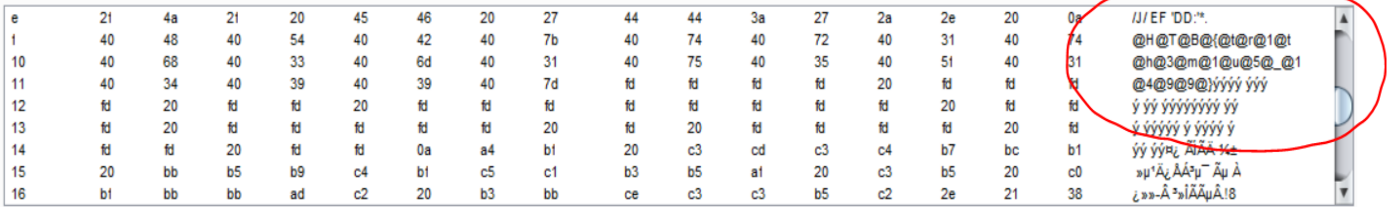
```
68 65  d in most of the
6E 67   world's writing
20 73   systems...The s
20 6D  ystem works in m
20 E8  any languages. è
E5 A4  ¯¥ç³»ç»Ÿä»¥è®¸å¤
20 D9  šè¯.è¨€å·¥ä½œ. Ù
D8 B8  ŠØ¹Ù…Ù„ Ø§Ù„Ù†Ø¸
D8 B9  Ø§Ù… Ù.ÙŠ Ø§Ù„Ø¹
D9 84  Ø¯ÙŠØ¯ Ù…Ù† Ø§Ù„
88 F3  Ù„Ø°Ø§Ø¹. .ó .ˆó
B4 F3   .”ó .‚ó .»ó .´ó
A8 F3   .ªó €±ó .´ó .¨ó
B5 F3   €³ó ..ó €±ó .µó
B4 F3   €µó .Ÿó €±ó €´ó
EF BF   €¹ó €¹ó .½ï¿½ï¿
EF BF  ½ï¿½ï¿½ ï¿½ï¿½ï¿
BD EF  ½ï¿½ ï¿½ï¿½ ï¿½ï
EF BF  ¿½ï¿½ï¿½ï¿½ï¿½ï¿
20 EF  ½ï¿½ ï¿½ï¿½ï¿½ ï
20 EF  ¿½ï¿½ï¿½ï¿½ï¿½ ï
BD 20  ¿½ ï¿½ï¿½ï¿½ï¿½
BF BD  ï¿½ï¿½ï¿½ ï¿½ï¿½
CE B7  .Î¤Î¿ ÏƒÏ.ÏƒÏ„Î·
BF CF  Î¼Î± Î»ÎµÎ¹Ï„Î¿Ï
20 CF  …Ï.Î³ÎµÎ¯ ÏƒÎµ Ï
```



Unicode is a computing industry standard for the consistent encoding, representation, and handling of text expressed in most of the world's writing systems.

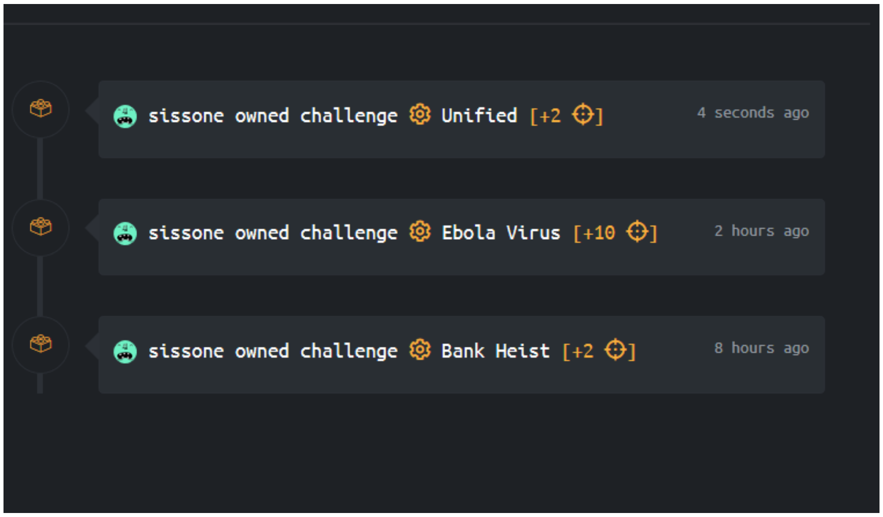
The system works in many languages. 该系统以许多语言工作. يعمل النظام في العديد من اللغات.
□□□□ □□□□ □□ □□□□□□□□□ □□□ □□□□□□ □ □□□□ □□□ □□
Το σύστημα λειτουργεί σε πολλές γλώσσες.Система работает на многих языках.

Steganography is the practice of concealing messages within other non-secret text or data.
The cover media may appear unremarkable at first glance and will require close investigation.



```
e    21  4a  21  20  45  46  20  27  44  44  3a  27  2a  2e  20  0a  /J/ EF 'DD:'*.
1    40  48  40  54  40  42  40  7b  40  74  40  72  40  31  40  74  @H@T@B@{@t@r@1@t
10   40  68  40  33  40  6d  40  31  40  75  40  35  40  51  40  31  @h@3@m@1@u@5@_@1
11   40  34  40  39  40  39  40  7d  fd  fd  fd  fd  20  fd  fd  fd  @4@9@9@}ýýýý ýýý
12   fd  20  fd  fd  20  fd  fd  fd  fd  fd  fd  fd  fd  20  fd  fd  ý ýý ýýýýýýýý ýý
13   fd  20  fd  fd  fd  fd  fd  20  fd  20  fd  fd  fd  fd  20  fd  ý ýýýýý ý ýýýý ý
14   fd  fd  20  fd  fd  0a  a4  b1  20  c3  cd  c3  c4  b7  bc  b1  ýý ýý¤¿ ÃÍÃÄ·¼±
15   20  bb  b5  b9  c4  b1  c5  c1  b3  b5  a1  20  c3  b5  20  c0   »µ¹Ä¿ÅÁ³µ¯ Ãµ À
16   b1  bb  bb  ad  c2  20  b3  bb  ce  c3  c3  b5  c2  2e  21  38  ¿»»-Â ³»ÎÃÃµÂ.!8
```

Evidence of Completion



sissone owned challenge Unified [+2 ⌖] 4 seconds ago

sissone owned challenge Ebola Virus [+10 ⌖] 2 hours ago

sissone owned challenge Bank Heist [+2 ⌖] 8 hours ago