

Forum:[Hack Forums](#)

Thread: [\[Challenge\] Introductory cryptanalysis.](#)

Phizo - September 6, 2017, 11:27 am

Solve for the following ciphertext:

Code 0000000 22 5c 78 43 33 27 5c 78 38 45 2a 7a 5c 78 44 35
0000010 38 5c 78 38 42 5c 78 41 42 5c 78 46 46 54 45 31
0000020 5c 78 30 32 4e 5c 78 38 30 33 50 5c 78 39 46 5c
0000030 78 45 44 5c 78 42 32 5c 78 46 46 2b 5c 78 45 46
0000040 59 53 3b 5c 78 45 38 5c 78 45 37 7b 5c 78 46 44
0000050 5c 72 5c 78 46 32 5c 78 46 46 5c 78 30 35 5c 78
0000060 30 35 5c 78 44 30 5c 78 31 39 5c 78 41 35 5c 78
0000070 43 37 5c 22 26 26 5c 78 43 36 5c 78 30 30 5c 78
0000080 31 35 5c 78 30 45 5c 78 38 43 5c 78 44 35 5c 78
0000090 42 32 58 31 5c 78 44 42 5c 78 45 35 5c 78 31 34
00000a0 6a 63 5c 78 41 34 5c 78 46 37 5c 78 39 30 5c 78
00000b0 44 44 5c 78 44 36 5c 78 44 41 5c 78 42 39 25 5c
00000c0 78 31 44 5c 78 41 36 5c 78 43 46 5c 78 42 43 5c
00000d0 78 44 45 5c 78 30 30 5c 78 39 46 5c 78 42 44 5c
00000e0 66 37 5c 78 46 32 5c 78 41 36 76 5c 78 38 36 29
00000f0 51 55 5c 78 43 43 5c 78 43 31 57 59 3d 5c 78 31
0000100 36 5c 78 46 32 5c 78 43 32 48 5c 78 30 30 5c 78
0000110 39 33 5c 78 31 30 5c 78 41 42 5c 78 39 44 5c 78
0000120 38 43 5c 78 44 33 6d 5c 78 39 33 5c 78 42 37 6d
0000130 5c 78 38 36 5c 78 44 41 73 5c 78 38 35 5c 78 44
0000140 33 5c 78 46 46 3c 65 5c 78 46 46 5c 78 43 39 5c
0000150 78 45 32 5c 78 39 44 5c 78 39 43 5c 78 41 33 5c
0000160 78 46 31 34 5c 78 31 37 5c 78 43 41 70 5c 78 30
0000170 34 5c 78 44 43 4d 5c 78 44 31 5c 78 44 45 5c 78
0000180 45 37 5c 78 39 36 5c 78 46 41 5c 78 44 38 5c 78
0000190 43 46 5c 78 30 35 60 5f 5c 78 46 42 41 5c 78 46
00001a0 36 5c 78 41 38 2d 5c 78 30 45 5c 78 38 46 3b 56
00001b0 2d 23 5c 78 39 42 5c 78 38 33 7a 5c 78 45 39 5c
00001c0 78 43 30 5c 78 43 46 5c 78 39 38 5c 78 38 41 5c
00001d0 78 44 32 5c 78 39 33 5c 78 44 38 5c 78 38 34 5c
00001e0 78 39 39 5c 78 39 30 5c 78 45 37 57 5c 78 41 38
00001f0 5c 78 46 46 5c 78 43 42 5c 78 30 33 5c 78 31 32
0000200 5c 78 42 35 5c 78 39 30 5c 78 42 45 5c 66 31 5c
0000210 78 42 31 5c 78 45 43 5c 78 44 33 5c 78 44 41 5c
0000220 78 43 46 5c 78 44 45 5c 78 43 44 5c 78 44 45 5c
0000230 78 43 39 5c 78 39 42 5c 78 43 43 5c 78 44 32 5c
0000240 78 44 37 5c 78 44 37 5c 78 39 42 5c 78 43 32 5c
0000250 78 44 34 5c 78 43 45 5c 78 39 42 5c 78 44 46 5c
0000260 78 44 34 5c 78 39 42 5c 78 44 35 5c 78 44 34 5c
0000270 78 43 43 5c 78 38 34 4b 21 5c 78 38 44 32 5c 78
0000280 30 33 5c 78 43 30 5c 78 38 43 5c 6e 2f 7b 5c 78
0000290 44 46 31 5c 78 44 37 5c 78 45 45 5c 78 44 37 5c
00002a0 78 38 43 44 78 5c 78 30 46 6a 5c 78 46 37 5c 78
00002b0 42 41 35 5c 78 42 39 5c 78 43 30 36 72 5c 78 30

00002c0 46 5c 78 44 46 43 5c 78 43 41 5c 78 41 41 5c 78
00002d0 43 31 5c 78 46 39 4f 5c 78 44 31 25 5c 78 44 32
00002e0 76 5c 78 42 36 24 5c 78 39 31 5c 78 38 31 3a 5c
00002f0 78 43 34 31 5c 78 44 34 5c 22 70 41 73 5c 78 44
0000300 31 3c 46 2e 5c 78 43 34 5a 5c 78 43 39 5c 78 41
0000310 46 5c 78 30 45 5c 78 46 42 2e 26 74 5c 74 5c 78
0000320 38 33 5c 65 2b 3c 5c 78 46 38 5c 78 45 44 5c 78
0000330 39 43 5c 6e 7a 5c 78 31 32 5c 78 46 41 26 4a 5c
0000340 78 46 31 55 5c 78 39 45 5c 78 41 43 37 5c 78 44
0000350 45 5c 74 5c 78 30 33 5c 78 39 42 58 2c 5c 66 30
0000360 5c 78 41 46 5c 78 42 31 5c 78 41 30 76 5c 78 39
0000370 38 5c 78 46 41 5c 78 41 42 5c 78 43 31 7b 5c 78
0000380 38 44 77 5c 78 31 43 68 51 5c 78 30 46 5c 78 46
0000390 45 57 5c 78 45 45 5c 78 42 37 5c 78 44 32 5c 78
00003a0 45 36 5c 78 41 45 53 5c 78 30 31 5c 78 43 46 25
00003b0 5c 78 38 46 24 26 6d 5c 78 46 46 6e 52 4f 5c 78
00003c0 42 32 65 77 48 5c 78 30 30 5c 78 43 30 5c 78 31
00003d0 38 5c 78 42 30 37 2c 5e 5c 78 41 32 5c 61 5c 78
00003e0 31 37 5c 78 43 39 5c 78 45 41 5c 78 41 44 39 56
00003f0 5f 5c 78 42 41 5c 78 38 32 5c 78 43 33 5c 78 43
0000400 44 5c 78 41 39 63 5c 78 44 45 32 5c 62 5c 78 46
0000410 46 5c 78 39 35 4c 5c 78 42 46 5c 78 45 39 32 41
0000420 5c 78 45 31 5c 78 45 45 39 5c 78 46 33 71 59 5c
0000430 78 42 34 5c 78 46 35 2d 5c 78 31 44 5c 78 42 35
0000440 22 0a

I'll give a hint if no one makes it through the first stage. Although, I would prefer not to, as this is beginner-level cryptanalysis. You shouldn't need hints.

Good luck.

Phizo - January 2, 2018, 7:48 pm

Bumping to potentially attract interested people. This one is much easier than my previous challenges. Give it a try if you're new to cryptography/cryptanalysis and want to learn something. Try my other challenges after to learn even more.

Red-1 - January 3, 2018, 12:48 am

Looks interesting, I have some understanding of cryptography but cryptanalysis not yet.

I will give it a shot sometimes soon.

Would I need a strong computer for this introductory challenge (as cryptanalysis sometimes requires)?

Phizo - January 3, 2018, 11:22 pm

(Jan 3, 2018 01:48 AM)Red-1 Wrote: [\[CITE\]](#) Looks interesting, I have some understanding of cryptography but cryptanalysis not yet.

I will give it a shot sometimes soon.

Would I need a strong computer for this introductory challenge (as cryptanalysis sometimes requires)?

No, you don't require a good CPU/GPU. Cryptanalysis generally does not require it, in fact. The only time it is necessary is when you are attempting to crack (e.g. brute-force/wordlist attack on keys), which is not really cryptanalysis. There is no analysis of the cipher involved in such attacks. In general (and in this case), the computations required are inexpensive.

sheekh.amir - January 4, 2018, 1:17 am

This awesome technic and how to learn is this best way in platform

Phizo - January 8, 2018, 8:25 am

Any attempts? Feel free to ask questions.

[BLANK] - January 8, 2018, 2:01 pm

I haven't figured it out yet, the format looks very familiar like a hex dump found in a debugger. But after that I am not sure what I can do with the data.

CryptixHacking - January 8, 2018, 2:08 pm

(Jan 8, 2018 03:01 PM)EasyGhost Wrote: [\[CITE\]](#) I haven't figured it out yet, the format looks very familiar like a hex dump found in a debugger. But after that I am not sure what I can do with the data.

From what I can see and tell it is a hex data dump so I believe you are right here. I would guess the next stage would be to convert the hex to ascii form. Once the hex is converted to ascii then you should be able to get a understanding of the encrypted data. Like what type of encryption / algorithm it might it be using, Give its not a salted hash encryption should be crackable.

For example converting the first few lines of hex data to ascii results in the following which does seem to be encrypted data.

Code "\xC3\x8E*z\xD58\x8B\xAB\xFFTE1\x02N\x803P\x9F\xED\xB2\xFF+\xEFYS;

\xE8xE7{\xFD\r\xF2\xFF\x05\x05\xD0\x19xA5\xC7"&&\xC6\x00\x15\x0E\x8C\xD5\xB2X1\xDB\xE5\x14jc\xA4\xF7\x90\x

If I had to guess it looks almost like a UTF-8 encoding sequence at this stage. So from this point you might just need to convert the UTF-8 back to byte sequence data.

L0-kae - January 8, 2018, 2:45 pm

When i convert hex to ascii i get all these special characters (that look like a small square with 4 small numbers in it susualy four 0s) appearing in groups of 3s and 2s in amongst the code, i know that ascii converts into text useing numbers in groups of 3 ?

doing some research on how to decrypt ascii.

I don't know anything at all about decryption so excuse my total ignorance i just like a challenge.

CryptixHacking - January 8, 2018, 2:52 pm

(Jan 8, 2018 03:45 PM)L0-kae Wrote: [\[CITE\]](#) When i convert hex to ascii i get all these special characters (that look like a small square with 4 small numbers in it susualy four 0s) appearing in groups of 3s and 2s in amongst the code, i know that ascii converts into text useing numbers in groups of 3 ?

doing some research on how to decrypt ascii.

I don't know anything at all about decryption so excuse my total ignorance i just like a challenge. Sounds like you are getting a charmap issue with the dumped ascii data.

Try using <https://www.rapidtables.com/convert/number/hex-to-ascii.html>

L0-kae - January 8, 2018, 3:05 pm

That's the exact converter i was using, I tryed typing the 3 didget groups into a ascii to text converter i found but that's not it as the output was plain text nonsense like" ?, ' " to i don't think that's the right direction to take,.

I'm going to try the same thing on another computer and OS to see if the characters I'm missing show up differently, they look like the filler icon for special characters not recognized (i think?) they looks like EG.

l00l

l04l

but in one character space.

. UPDATE: Still getting the same special character issue on other systems

CryptixHacking - January 8, 2018, 3:19 pm

(Jan 8, 2018 04:05 PM)L0-kae Wrote: [\[CITE\]](#) That's the exact converter i was using, I tried typing the 3 didget groups into a ascii to text converter i found but that's not it as the output was plain text nonsense like " ?, ' " to i don't think that's the right direction to take,.

I'm going to try the same thing on another computer and OS to see if the characters I'm missing show up differently, they look like the filler icon for special characters not recognized (i think?) they looks like EG.

l00l

l04l

but in one character space.

. UPDATE: Still getting the same special character issue on other systems

You are putting it in wrong then my guess is you are including the line numbers of the hex data which should not be the case.

Paste like so

Code 38 5c 78 38 42 5c 78 41 42 5c 78 46 46 54 45 31

5c 78 30 32 4e 5c 78 38 30 33 50 5c 78 39 46 5c

78 45 44 5c 78 42 32 5c 78 46 46 2b 5c 78 45 46

That is HEX

Dont include the

0000000

0000010

Then convert the HEX to ASCII

L0-kae - January 8, 2018, 3:31 pm

I'm such a stupid C#@\$, thanks so much.

?q ' ???? U? ?Xt?]mGz??????8YGb=??#}??? ?P?Q

K? ~?????y?m2k ?

This is what i get when i convert the ascii (as it's converted) to text so i don't think that is the right thing todo still.

im going to look up other ways to decrypt it.

Update: Put it threw a a decoder (<https://www.dcode.fr/ascii-code>) and got more gibberish (to me) but it seems that looking at it that i need to clean up or do something to the ascii code to make it look more like this (64 43 6F 64 65 20 41 53 43 49 49) but i feel very stupid right now i need to do a bit more research into howcypher decryption works as this is supposed to be easy and i'm finding it quite hard, i've never looked at a cypher thou.

Will update if i get anywhere with it.

CryptixHacking - January 8, 2018, 3:57 pm

(Jan 8, 2018 04:31 PM)L0-kae Wrote: [\[CITE\]](#) I'm such a stupid C#@\$, thanks so much.

?q ' ???? U? ?Xt?]mGz??????8YGb=??#}??? ?P?Q
K? ~?????y?m2k ?

This is what i get when i convert the ascii (as it's converted) to text so i don't think that is the right thing todo still.

im going to look up other ways to decrypt it.
Thats because you are not doing it right lol

you convert the HEX code to ASCII

DONE thats it you are finished.

YOU DONT CONVERT THE ASCII TO TEXT

The ASCII is text already !

Now that the HEX data is converted to readable ASCII you have the encrypted data which looks like.

Code "\xC3\xE*z\xD58\x8B\xAB\xFFTE1\x02N\x803P\x9F\xED\xB2\xFF+\xEFYS;

\xE8\xE7{\xFD\r\F2\xFF\x05\x05\xD0\x19\xA5\xC7"&&\xC6\x00\x15\x0E\x8C\xD5\xB2X1\xDB\xE5\x14jc\xA4\xF7\x90\xThis is the encrypted ASCII data "ENCRYPTED"

You must decrypt this data now, Simply converting the ASCII to text will do nothing for you at this point.

You must now find what this new ASCII encrypted data is storing and its algorithm.

L0-kae - January 8, 2018, 4:00 pm

Right i'll do some research now.

pleas excuse my total ignorance

CryptixHacking - January 8, 2018, 4:11 pm

(Jan 8, 2018 05:00 PM)L0-kae Wrote: [\[CITE\]](#) Right i'll do some research now.

This should be the entire encrypted data converted from HEX

Code

"\xC3\xE*z\xD58\x8B\xAB\xFFTE1\x02N\x803P\x9F\xED\xB2\xFF+\xEFYS;\xE8\xE7{\xFD\r\F2\xFF\x05\x05\xD0\x19\xA5\xC7"&&\xC6\x00\x15\x0E\x8C\xD5\xB2X1\xDB\xE5\x14jc\xA4\xF7\x90\xD\xD6\xDA\xB9%\x1D\xA6\xCF\xBC\xDE\x00\x9F\xBD\xf7\xF2\xA6v\x86)QU\xCC\xC1WY=\x16\xF2\xC2H\x00\x93\x10\xAB\x9D\x8C\xD3m\x93\xB7m\x86\xDAs\x85\xD3\xFF<e\xFF\xC9\xE2\x9D\x9C\x

xA3\xF14\x17\xCAp\x04\xDCM\xD1\xDE\xE7\x96\xFA\xD8\xCF\x05`_\xFBA\xF6\xA8-\x0E\x8F;V-#\x9B\x83z\xE9\xC0\xCF\x98\x8A\xD2\x93\xD8\x84\x99\x90\xE7W\xA8\xFF\xCB\x03\x12\xB5\x90\xBE\xf1\xB1\xEC\xD3\xDA\xCF\xDE\xCD\xDE\xC9\x9B\xCC\xD2\xD7\xD7\x9B\xC2\xD4\xCE\x9B\xDF\xD4\x9B\xD5\xD4\xCC\x84K!\x8D2\x03\xC0\x8C\n/{\xDF1\xD7\xEE\xD7\x8CDx\x0Fj\xF7\xBA5\xB9\xC06r\x0F\xDFC\xCA\xAA\xC1\xF9O\xD1%\xD2v\xB6\$\x91\x81:\xC41\xD4"pAs\xD1<F.\xC4Z\xC9\xAF\x0E\xFB.&t\t\x83)e+<\xF8\xED\x9C\nz\x12\xFA&J\xF1U\x9E\xAC7\xDE\t\x03\x9BX,\f0\xAF\xB1\xA0v\x98\xFA\xAB\xC1{\x8Dw\x1ChQ\x0F\xFEW\xEE\xB7\xD2\xE6\xAES\x01\xCF%\x8F\$&m\xFFnRO\xB2ewH\x00\xC0\x18\xB07,^\xA2\ax17\xC9\xEA\xAD9V_\xBA\x82\xC3\xCD\xA9c\xDE2\b\xFF\x95L\xBF\xE92A\xE1\xEE9\xF3qY\xB4\xF5-\x1D\xB5"

This is the encryption that needs solved.

L0-kae - January 8, 2018, 4:47 pm

I've got that already I've just never decrypted anything before like this and thought here and now would be the best time to try learn what i can trying to solve this but i've not got any practical knowledge of encryption other than how to use the software that encrypts things for you so i don't know where i'd begin to decrypt it other than very stupid and simple sounding (in my own head) brute forcing.

I'm going to go away and learn more and hopefully return with less shame...

Phizo - January 8, 2018, 6:48 pm

(Jan 8, 2018 03:08 PM)CryptixHacking Wrote: [\[CITE\]](#) From what I can see and tell it is a hex data dump so I believe you are right here. I would guess the next stage would be to convert the hex to ascii form. Once the hex is converted to ascii then you should be able to get a understanding of the encrypted data. Like what type of encryption / algorithm it might it be using, Give its not a salted hash encryption should be crackable.

For example converting the first few lines of hex data to ascii results in the following which does seem to be encrypted data.

Code "\xC3'\x8E*z\xD58\x8B\xAB\xFFTE1\x02N\x803P\x9F\xED\xB2\xFF+\xEFYS;

\xE8\xE7{\xFD\r\xF2\xFF\x05\x05\xD0\x19\xA5\xC7"&&\xC6\x00\x15\x0E\x8C\xD5\xB2X1\xDB\xE5\x14jc\xA4\xF7\x90\x

If I had to guess it looks almost like a UTF-8 encoding sequence at this stage. So from this point you might just need to convert the UTF-8 back to byte sequence data.

You don't "crack" encryption, if by "crack" you mean brute-force the plaintext-ciphertext mapping like with hash-cracking. That is computationally infeasible. The reason you brute-force hashes is because it is difficult to compute the inverse function given the image of a random input (i.e. it is a one-way mapping; you do not [and cannot] decrypt a hash). Encryption, on the other hand, implies decryption (the inverse/decryption function necessarily exists). Also, yes, it is a hex dump. UTF-8 encoding is completely irrelevant here, and "UTF-8 back to byte sequence data" doesn't make sense. There is no indication of UTF-8 encoding. In fact, the data actually implies a lack of encoding: it can be observed the data contains raw (unencoded) bytes. Many people seem to misunderstand UTF. They seem to think it's some sort of scheme in which you encode raw data for pretty-printing and/or compliance over transport layers (like with base64 and hex). This is not the case. They serve different purposes. UTF is a Unicode standard, which is a universal format for displaying character sets. Any character of the UTF-x charset itself may be expressed as the character itself (which is extended far beyond ASCII), or a variable-length sequence of bits (binary), hex, or any other encoding scheme. UTF-x is not an "encoding scheme" in the same sense.

Baud - January 10, 2018, 4:58 pm

I'm following the thread out of curiosity (and to prevent it getting buried) because I don't have the skills necessary to solve this challenge, but I am very curious to see if anyone can do it - and how.

I can go as far as saying that after converting the hex dump into ASCII the result is mostly made of other hexadecimal numbers, the two numbers that follow every \x to be exact but that's pretty obvious, and at a first glance I don't know what to do with all the other characters. Can we have a hint?

[BLANK] - January 11, 2018, 7:35 am

Hey Phizo, I have always been interested in cryptography but never got around to studying it because it wasn't part of my career path. Thanks for providing an equation but honestly for someone like me it doesn't help much. Would you have a good resource/book that I could study to eventually solve this? I don't want a direct answer or anything, but if you know of great study material that would help I would appreciate it.

Phizo - January 13, 2018, 5:40 pm

(Jan 10, 2018 05:58 PM)Baud Wrote: [\[CITE\]](#) I'm following the thread out of curiosity (and to prevent it getting buried) because I don't have the skills necessary to solve this challenge, but I am very curious to see if anyone can do it - and how.

I can go as far as saying that after converting the hex dump into ASCII the result is mostly made of other hexadecimal numbers, the two numbers that follow every \x to be exact but that's pretty obvious, and at a first glance I don't know what to do with all the other characters. Can we have a hint?

Given the lack-of-success-to-post ratio, I suppose it is time for a hint. The cipher may be expressed as the composite function $E(x) = f(g(x))$. Determine the algorithms which are f and g to determine the inverse/decryption functions f^{-1} and g^{-1} and compute $x = g^{-1}(f^{-1}(y))$. One big hint is that f utilises XOR. Note that XOR is an involutory function, i.e. $f(f(x)) = x$ if and only if $f = f^{-1}$.

(Jan 11, 2018 08:35 AM)EasyGhost Wrote: [\[CITE\]](#) Hey Phizo, I have always been interested in cryptography but never got around to studying it because it wasn't part of my career path. Thanks for providing an equation but honestly for someone like me it doesn't help much. Would you have a good resource/book that I could study to eventually solve this? I don't want a direct answer or anything, but if you know of great study material that would help I would appreciate it.

I'm afraid that isn't really possible without spoiling the definition of f , as I would need to provide you with some paper on it specifically. It is an introductory-level challenge. The only direction I can point you towards is look into XOR (exclusive-OR) and Caesar's cipher. f is not Caesar's cipher, but it is very similar. The aforementioned equations do not really matter: it is just a mathematical representation/description of the problem. While you would have an advantage if you did understand it, you don't need to concern yourself too much with it if you don't. Basically, you have two "phases" of the cipher that you must undo to map the ciphertext back to its respective plaintext.

Handling - January 14, 2018, 12:16 pm

This is a gawdly code o.o

Phizo - May 24, 2018, 3:36 am

(Jan 14, 2018 01:16 PM)Handling Wrote: [\[CITE\]](#) This is a gawdly code o.o
So godly that only you can see this supposed code. That's a neat trick.

tulamba - May 29, 2018, 7:49 pm

(May 24, 2018 03:36 AM)Phizo Wrote: [\[CITE\]](#) So godly that only you can see this supposed code. That's a neat trick.

Didn't understand neither godly's comment nor yours. Please elaborate and educate all of us.

Phizo - May 31, 2018, 7:02 am

(May 29, 2018 07:49 PM)tulamba Wrote: [\[CITE\]](#) Didn't understand neither godly's comment nor yours. Please elaborate and educate all of us.
His comment isn't understandable because it makes no sense: there is no "code." My reply to him was just sarcasm.

tulamba - June 2, 2018, 8:10 pm
@Phizo

Lets make this thread active. I would suggest giving more hints so people who are stuck like me can get started. Remember we are on hackforums to share and learn together. Lets keep this spirit alive

sophrosyne - June 2, 2018, 9:02 pm

OP has given a lot of information, mainly here:

(Jan 13, 2018 06:40 PM)Phizo Wrote: [\[CITE\]](#) Given the lack-of-success-to-post ratio, I suppose it is time for a hint. The cipher may be expressed as the composite function $E(x) = f(g(x))$. Determine the algorithms which are f and g to determine the inverse/decryption functions f^{-1} and g^{-1} and compute $x = g^{-1}(f^{-1}(y))$. One big hint is that f utilises XOR. Note that XOR is an involutory function, i.e. $f(f(x)) = x$ if and only if $f = f^{-1}$.

The first part of the puzzle was nice simple Hex to ASCII.

Phizo - January 4, 2019, 9:45 am

(Jun 2, 2018 09:02 PM)sophrosyne Wrote: [\[CITE\]](#) OP has given a lot of information, mainly here:

The first part of the puzzle was nice simple Hex to ASCII.

That isn't really part of the challenge. That's necessary. You're dealing with raw bytes which may be non-printable, so you necessarily have to use some form of encoding for pretty-printing. The common two are hexadecimal and base64. This is something that you deal with for pretty much all ciphertext.