**CTFLEARN**

1. Cryptography
2. HEXTRAORDINARY

Meet ROXy, a coder obsessed with being exclusively the worlds best hacker. She specializes in short cryptic hard to decipher secret codes. The below hex values for example, she did something with them to generate a secret code, can you figure out what? Your answer should start with 0x. 0xc4115 0x4cf8

Clue: ROX = XOR

How to solve: Lakukan operasi XOR antara 0x4115 dengan 0x4cf8, didapat flag **0xc0ded**

1. BASE 2 2 THE 6

There are so many different ways of encoding and decoding information nowadays... One of them will work! Q1RGe0ZsYWdneVdhZ2d5UmFnZ3l9

Clue: Base 2\*2 the 6 = Base64

How to solve: Lakukan dekripsi string “Q1RGe0ZsYWdneVdhZ2d5UmFnZ3l9”” yang menggunakan encoding base64, didapat string **CTF{FlaggyWaggyRaggy}**

1. BRUXOR

There is a technique called bruteforce. Message: q{vpln'bH\_varHuebcrqxetrHOXEj No key! Just brute .. brute .. brute ... :D

Clue: BruXor = Brute Forcing XOR

How to solve: Lakukan Brute Force XOR di <https://gchq.github.io/CyberChef/#recipe=XOR_Brute_Force(1,100,0,'Standard',true,true,false,'')&input=cXt2cGxuJ2JIX3Zhckh1ZWJjcnF4ZXRySE9YRWo>

Didapat flag **flag{y0u\_Have\_bruteforce\_XOR}**

1. Vigenere Cipher

The vignere cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword.<br /> I’m not sure what this means, but it was left lying around: blorpy gwox{RgqssihYspOntqpxs}

Clue: Vigenere

How to solve: Ciphertext adalah gwox{RgqssihYspOntqpxs}, lalu kita harus mencari kunci dari ciphertext itu, yang adalah **blorpy**, lakukan dekripsi, didapat **flag{CiphersAreAwesome}**

1. Morse Code

..-. .-.. .- --. ... .- -- ..- . .-.. -- --- .-. ... . .. ... -.-. --- --- .-.. -... -.-- - .... . .-- .- -.-- .. .-.. .. -.- . -.-. .... . . ...

Clue: Morse Code

How to solve: Decode morse code didapat flag **samuelmorseiscoolbythewayilikechees**

1. Hyperstream Test #2

ABAAAABABAABBABBAABBAABAAAAAABAAAAAAAABAABBABABBAAAAABBABBABABBAABAABABABBAABBABBAABB

Clue: Hyperstream

How to solve: Setelah meriset, didapat bahwa enkripsi yang dipakai adalah Baconian Cipher, maka lakukan dekripsi didapat flag **ILOUEBACONDONTYOU**

1. RSA NOOB

These numbers were scratched out on a prison wall. Can you help me decode them? https://mega.nz/#!al8iDSYB!s5olEDK5zZmYdx1LZU8s4CmYqnynvU\_aOUvdQojJPJQ

1. Top of Form

Hint: RSA

How to solve:

Isi dari file adalah

e: 1

c:9327565722767258308650643213344542404592011161659991421

n: 245841236512478852752909734912575581815967630033049838269083

Karena sudah diketahui c, n dan e, selanjutnya dilakukan deskripsi dengan rumus

didapat res = 245841236512478852752909734912575581815967630033049838269083

Lakukan konversi ke teks, didapat flag **abctf{b3tter\_up\_y0ur\_e}**

1. AlexCTF CR2: Many Time Secrets

This time Fady learned from his old mistake and decided to use onetime pad as his encryption technique, but he never knew why people call it one time pad! Flag will start with ALEXCTF{. <https://mega.nz/#!DGxBjaDR!tMWkHf0s0svmkboGd-IASHsS9jACxSYx4zi_ETsyzyQ>

Clue: One Time Pad

How to solve:

Di dalam file terdapat hex:

0529242a631234122d2b36697f13272c207f2021283a6b0c7908

2f28202a302029142c653f3c7f2a2636273e3f2d653e25217908

322921780c3a235b3c2c3f207f372e21733a3a2b37263b313012

2f6c363b2b312b1e64651b6537222e37377f2020242b6b2c2d5d

283f652c2b31661426292b653a292c372a2f20212a316b283c09

29232178373c270f682c216532263b2d3632353c2c3c2a293504

613c37373531285b3c2a72273a67212a277f373a243c20203d5d

243a202a633d205b3c2d3765342236653a2c7423202f3f652a18

2239373d6f740a1e3c651f207f2c212a247f3d2e65262430791c

263e203d63232f0f20653f207f332065262c3168313722367918

2f2f372133202f142665212637222220733e383f2426386b

1. Reverse Polarity

I got a new hard drive just to hold my flag, but I'm afraid that it rotted. What do I do? The only thing I could get off of it was this: 01000011010101000100011001111011010000100110100101110100010111110100011001101100011010010111000001110000011010010110111001111101

How to solve: Just decode the binary, dan dapatkan flag **CTF{Bit\_Flippin}**

1. Substitution Cipher

Someone gave me this, but I haven't the slightest idea as to what it says! https://mega.nz/#!iCBz2IIL!B7292dJSx1PGXoWhd9oFLk2g0NFqGApBaItI\_2Gsp9w Figure it out for me, will ya?

How to solve: Et tu brute?

MIT YSAU OL OYGFSBDGRTKFEKBHMGCALSOQTMIOL. UTFTKAMTR ZB DAKQGX EIAOF GY MIT COQOHTROA HAUT GF EASXOF AFR IGZZTL. ZT CTKT SGFU, MIT YSACL GF A 2005 HKTLTFM MODTL MIAF LMADOFA GK A CTTQSB LWFRAB, RTETDZTK 21, 1989 1990, MIT RKTC TROMGKL CAL WHKGGMTR TXTKB CGKSR EAF ZT YGWFR MIT EGFMOFWTR MG CGKQ AM A YAOMIYWS KTHSOTL CITKT IGZZTL, LMBST AOD EASXOF, AMMAEQ ZGMI LORTL MG DAKQL, "CIAM RG EGFMKGSSOFU AF AEMWAS ZGAKR ZGVTL OF MIT HKTHAKTFML FADT, OL ODHWSLOXT KADHAUTL OF CIOEI ASCABL KTYTKTFETL MIT HALLCGKR, CIOEI DGFTB, AFR MITB IAR SOMMST YKGFM BAKR IOL YKWLMKAMTR EGSGK WFOJWT AZOSOMB COMI AFR OFROLHTFLAMT YGK MTAEI GMITK LMWROTL, AKT ACAKRL ZARUTL, HWZSOLITR ZTYGKT CTSS AL A YOKT UKGLL HSAFL CTKT GKOUOFASSB EIAKAEMTKL OF MIT LMKOH MG CIOEI LTTD MG OM CITF MTDHTKTR OF AFR IASSGCOFU MITB'KT LODHSB RKACOFU OF UOXTL GF" HKOFEOHAS LHOMMST ROLMGKM, KTARTKL EGDOEL AKT WLT, CAMMTKLGF MGGQ MCG 16-DGFMIL AYMTK KTLOLMAQTL A DGKT EKTAM RTAS MG EASXOF GYMTF IGZZTL MG ARDOML "LSODB, "ZWM OM'L FADTR A FOUIM GWM LIT OL HGOFM GY FGM LTTF IGZZTL MIT ZGGQL AM MIAM O KTDAOFOFU ZGGQ IADLMTK IWTB AKT AHHTAKAFET: RTETDZTK 6, 1995 DGD'L YKADTL GY EASXOF UOXTF A CAUGF, LGDTMODTL MIAM LG OM'L YAMITKT'L YADOSB FG EAFETSSAMOGFLIOH CAL HKTLTFML YKGD FGXTDZTK 21, 1985 SALM AHHTAK AZLTFET OF AFGMITKCOLT OM IAHHB MG KWF OM YGK MIOL RAR AL "A SOMMST MG MGSTKAMT EASXOF'L YADOSB RKACF ASDGLM EGDDTFRTR WH ZTOFU HTGHST OFLMAFET, UTM DAKKOTR ZB A RAFET EASXOF'L GWMSAFROLOFU MIT FTCLHAHTK GK MAZSGOR FTCLHAHTK ZWLOFTLL LIGC OL GF!" AFR LHKOFML GY EIOSRKTF'L RAR'L YKWLMKAMTR ZB MWKF IWDGK, CAL HWZSOE ROASGU MITKT'L FGM DWEI AL "'94 DGRTKFOLD" CAMMTKLGF IAL RTSOUIML GY YAFMALB SOYT CAMMTKLGF LABL LTKXTL AL AF AKMOLML OL RTLMKWEMOGF ZWLOFTLL, LHAETYAKTK GY MIT GHHGKMWFOMOTL BGW ZGMI A MGHOE YGK IOL IGDT MGFUWT-OF-EITTQ HGHWSAK MIAM OM CAL "IGF" AFR JWAKMTK HAUT DGKT LHAEOGWL EAFETSSAMOGF MIT HAOK AKT ESTAKSB OF HLBEIOE MKAFLDGUKOYOTK'L "NAH" LGWFR TYYTEM BGW MIOFQTK CAMMTKLGF ASLG UKTC OFEKTROZST LHAET ZWBL OF EGDDGFSB CIOST GMITKCOLT OM'L FADT OL FGMAZST LMGKBSOFT UAXT MIT GHHGKMWFOMOTL BGW EAFETSSAMOGF MIT "EASXOF GYYTK MG DAQT IOD OFEGKKTEM AFLCTKL CAMMTK AKMCGKQ GMITK GYMTF CIOEI OL TXORTFM MG GMITK LMKOH OL MG MITOK WLT GY KWSTL MIAM LIGCF GF LAFROYTK, CIG WLTL A EKGCJWOSS ZT LTTF "USWTR" MG MIT GFSB HTKL AFR IOL YAMITK LWHHGKM OL SWFEISOFT UAXT MITLT MIOF A BTAK OF DWSMODAMTKOAS AFR GZMAOF GF LAFMALB, IOL WLT, CAMMTKL ROASGUWT OL AF "AKMOLM'L LMAMWL AL "A ROD XOTC OF MIT TLLTFMOASSB MG DAQT IOD LTTD MG OFESWRTR MIAM EASXOF OL AF GRR ROASGUWT DGLM GY MIT ESWZ IAL TVHKTLLOGF GWMLORT AXAOSAZST MG

Pakai Substitution Solver di guballa.de/substitution-solver, didapat:

THE FLAG IS **IFONLYMODERNCRYPTOWASLIKETHIS**. GENERATED BY MARKOV CHAIN OF THE WIKIPEDIA PAGE ON CALVIN AND HOBBES. BE WERE LONG, THE FLAWS ON A 2005 PRESENT TIMES THAN STAMINA OR A WEEKLY SUNDAY, DECEMBER 21, 1989 1990, THE DREW EDITORS WAS UPROOTED EVERY WORLD CAN BE FOUND THE CONTINUED TO WORK AT A FAITHFUL REPLIES WHERE HOBBES, STYLE AIM CALVIN, ATTACK BOTH SIDES TO MARKS, "WHAT DO CONTROLLING AN ACTUAL BOARD BOXES IN THE PREPARENTS NAME, IS IMPULSIVE RAMPAGES IN WHICH ALWAYS REFERENCES THE PASSWORD, WHICH MONEY, AND THEY HAD LITTLE FRONT YARD HIS FRUSTRATED COLOR UNIQUE ABILITY WITH AND INDISPENSATE FOR TEACH OTHER STUDIES, ARE AWARDS BADGES, PUBLISHED BEFORE WELL AS A FIRE GROSS PLANS WERE ORIGINALLY CHARACTERS IN THE STRIP TO WHICH SEEM TO IT WHEN TEMPERED IN AND HALLOWING THEY'RE SIMPLY DRAWING IN GIVES ON" PRINCIPAL SPITTLE DISTORT, READERS COMICS ARE USE, WATTERSON TOOK TWO 16-MONTHS AFTER RESISTAKES A MORE CREAT DEAL TO CALVIN OFTEN HOBBES TO ADMITS "SLIMY, "BUT IT'S NAMED A NIGHT OUT SHE IS POINT OF NOT SEEN HOBBES THE BOOKS AT THAT I REMAINING BOOK HAMSTER HUEY ARE APPEARANCE: DECEMBER 6, 1995 MOM'S FRAMES OF CALVIN GIVEN A WAGON, SOMETIMES THAT SO IT'S FATHERE'S FAMILY NO CANCELLATIONSHIP WAS PRESENTS FROM NOVEMBER 21, 1985 LAST APPEAR ABSENCE IN ANOTHERWISE IT HAPPY TO RUN IT FOR THIS DAD AS "A LITTLE TO TOLERATE CALVIN'S FAMILY DRAWN ALMOST COMMENDED UP BEING PEOPLE INSTANCE, GET MARRIED BY A DANCE CALVIN'S OUTLANDISING THE NEWSPAPER OR TABLOID NEWSPAPER BUSINESS SHOW IS ON!" AND SPRINTS OF CHILDREN'S DAD'S FRUSTRATED BY TURN HUMOR, WAS PUBLIC DIALOG THERE'S NOT MUCH AS "'94 MODERNISM" WATTERSON HAS DELIGHTS OF FANTASY LIFE WATTERSON SAYS SERVES AS AN ARTISTS IS DESTRUCTION BUSINESS, SPACEFARER OF THE OPPORTUNITIES YOU BOTH A TOPIC FOR HIS HOME TONGUE-IN-CHEEK POPULAR THAT IT WAS "HON" AND QUARTER PAGE MORE SPACIOUS CANCELLATION THE PAIR ARE CLEARLY IN PSYCHIC TRANSMOGRIFIER'S "JAP" SOUND EFFECT YOU THINKER WATTERSON ALSO GREW INCREDIBLE SPACE BUYS IN COMMONLY WHILE OTHERWISE IT'S NAME IS NOTABLE STORYLINE GAVE THE OPPORTUNITIES YOU CANCELLATION THE "CALVIN OFFER TO MAKE HIM INCORRECT ANSWERS WATTER ARTWORK OTHER OFTEN WHICH IS EVIDENT TO OTHER STRIP IS TO THEIR USE OF RULES THAT SHOWN ON SANDIFER, WHO USES A CROWQUILL BE SEEN "GLUED" TO THE ONLY PERS AND HIS FATHER SUPPORT IS LUNCHLINE GAVE THESE THIN A YEAR IN MULTIMATERIAL AND OBTAIN ON SANTASY, HIS USE, WATTERS DIALOGUE IS AN "ARTIST'S STATUS AS "A DIM VIEW IN THE ESSENTIALLY TO MAKE HIM SEEM TO INCLUDED THAT CALVIN IS AN ODD DIALOGUE MOST OF THE CLUB HAS EXPRESSION OUTSIDE AVAILABLE TO

1. 5x5 Crypto

Ever heard of the 5x5 secret message system? If not, basically it's a 5x5 grid with all letters of the alphabet in order, without k because c is represented to make the k sound only. Google it if you need to. A letter is identified by Row-Column. All values are in caps. Try: 1-3,4-4,2-1,{,4-4,2-3,4-5,3-2,1-2,4-3,\_,4-5,3-5,}

Hint: 5x5 grid

How to solve: Buat grid 5x5 yang berisi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | B | C | D | E |
| F | G | H | I | J |
| L | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

Setelah dibuat gridnya, korespodensikan koordinat dengan grid, maka didapa flag

**CTF{THUMBS\_UP}**

1. Character Encoding

In the computing industry, standards are established to facilitate information interchanges among American coders. Unfortunately, I've made communication a little bit more difficult. Can you figure this one out? 41 42 43 54 46 7B 34 35 43 31 31 5F 31 35 5F 55 35 33 46 55 4C 7D

How to solve: Convert hex ke ASCII, didapat **45C11\_15\_U53FUL**