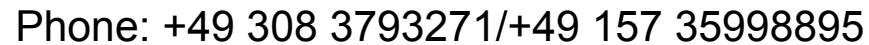# Code Labs Academy Berlin - Coding Bootcamp
Lobeckstraße 36-40, 10969 Berlin
Phone: +49 308 3793271/+49 157 35998895

Welcome, Cryptography enthusiasts! Are you ready for a challenge that will test your skills and push you to the limit? Today, we invite you to dive into a set of beginner-friendly CTF challenges that will take you on an exciting journey through the world of cryptography. From simple ciphers to complex encryption algorithms, these challenges will put your problem-solving abilities to the test and help you develop your cryptographic skills. So, gear up and get ready to crack the code! Are you up for the challenge?

Rules and Regulations:
1. All participants are required to read the instructions carefully before starting the CTF challenge.
2. Participants are encouraged to take the time to analyze the challenge before attempting to solve it.
3. Participants should report any bugs or glitches in the challenge to the event organizers.
4. Participants must respect the privacy and intellectual property rights of others.
5. This CTF challenge is meant to be a fun and engaging experience for all participants. While we encourage everyone to take the challenge seriously, we also want to emphasize that it's okay to make mistakes and learn from them.
6. We hope that all participants will enjoy the challenge and use it as an opportunity to develop new skills and knowledge in the field of cybersecurity.
7. We encourage participants to collaborate with their peers, share ideas and help each other out if needed.
8. Remember, this challenge is not about winning or losing, but about the journey and the learning experience.
9. Wrap all the flags in this format CLACTF{your flag}

1. 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?

67 76 65 67 84 70 123 121 79 117 95 71 111 84 95 116 72 101 95 70 108 65 103 125.

2. Can you decipher the Morse code and reveal the hidden message? Sharpen your cryptography skills and put your knowledge to the test in this exciting CTF challenge!

-.-. --- -. --. .-. .- - .. .-.. .- - .. --- -. ... / -.-- --- ..- / --. --- / - .... / ..- . .-.. . --. / ..-. .-. --- -- / - .... . / -- --- .-. ... . / -.-. --- -... . / -.-. .-.. .- -.-. - ..- ..--.- -- --- .-. ... . ..--.- -.-. --- -... .

3. 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.

   I'm not sure what this means, but it was left lying around: BLORPY

DWOwayh{NwgwcsdOitYxpgfbc-JegRKghpbvgcDtdytp}

4. 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:

0100001101010100010001100111101101000010011010010111010001011111010001100110110001101001011100000111000001101001011011001111101

5. Meet ROXy, a coder obsessed with being exclusively the world's 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 CLACTF{0xflag}.

0xc4115 0x4cf8

6. Do you have what it takes to crack the mono-alphabetic substitution cipher and uncover the secret message? This challenge will put your cryptanalysis skills to the test! With patience and persistence, you can decipher the code and reveal the hidden flag. Good luck!

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 OFEKTGZST LHAET ZWBL OF EGDDGFSB CIOST GMITKEGSOLT OM'L FADT OL FGMAZST LMGKBSOFT UAXT MIT GHHGKMWFOMOTL BGW EAFETSSAMOGF MITLAFROYTK, 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

7. You have intercepted a message from a suspected hacker, but it is encrypted and you need to decode it. The intercepted message is:

INGECQ2UIZ5VI2DJOMQGS4ZAIJQXGZJAGMZCAZLOMNXWI2LOM56Q====

8. You have intercepted another similar message from a suspected hacker, but it is encrypted and you need to decode it. The intercepted message is:

Q0xBQ1RGe1RoaXNfaXNfQmFzZTY0X2VuY29kaW5nfQ==

9. You have intercepted a suspicious message that appears to contain a flag. It seems that the message has been encoded using URL encoding. Can you crack the code and reveal the original flag?The message reads:

CLACTF%7BThis%5Fshould%5Fbe%5Fan%5Feasy%5Fcracking%5Fbecause%5Fit%5Fis%5FURL%5Fencoding%7D

10. You have intercepted a highly-encrypted message containing what appears to be a flag. The message is in a complex format. Your task is to decipher the message and extract the flag, which has been encrypted using a sophisticated substitution cipher. Your decryption skills will be put to the test as you work to uncover the hidden message and reveal the flag. Do you have what it takes to crack the code?

031201032006{141502150425_030114_0318010311_20080919_02050301211905_092019_080907081225_19050 3180520_1908080808}

11. Ooh, do you like a challenge? Well, get ready to put your code-breaking skills to the test! There's a secret message hidden within this seemingly random sequence of letters, and I bet you're just dying to find out what it says. But here's the catch - I can't just give it away! Instead, I'll give you a hint to get you started. Let's just say this particular cipher is named after a portion of delicious breakfast food. Hmm, I wonder what it could be? Ready to dive in and crack the code?

AAADA ADADA AAAAA AAADA DAADA AADAD DAADA AADDD ADAAA DAAAD AAADA ADAAA ADDDA AADDD
AADAA DAAAA ADAAA DAAAD AAADA AAAAA ADADA ADADA AADAA AAADD AAAAD AAAAA AAADA ADDAD
ADDAA AAADA ADAAA ADDDA AADDD AADAA DAAAA

12. 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?

01000011 01001100 01000001 01000011 01010100 01000110 01111011 01010100 01101000 01101001 01110011 01011111 01011111 01101001 01110011 01011111 01011111 01100001 01011111 01011111 01110011 01100101 01100011 01110010 01100101 01110100 01011111 01011111 01101101 01100101 01110011 01110011 01100001 01100111 01100101 01011111 00101100 01011111 01100101 01101110 01100011 01101111 01100100 01100101 01100100 01011111 01011111 01101001 01101110 01011111 01011111 01000010 01101001 01101110 01100001 01110010 01111001 01011111 01011111 01100110 01101111 01110010 01101101 01100001 01110100 01011111 00101100 01011111 01100110 01101001 01101110 01100100 01011111 01011111 01101101 01100101 01111101 00101110.

13. Cryptography can be easy, do you know what ROT13 is?

EBG13 ("ebgngr ol 13 cynprf", hfhnyyl ulcurangrq EBG-13) vf n fvzcyr Pnrfne pvcure hfrq sbe bofphevat grkg ol ercynpvat rnpu yrggre jvgu gur yrggre guvegrra cynprf qbja gur nycunorg. N orpbzrf A, O orpbzrf B, naq fb ba hc gb Z, juvpu orpbzrf M, gura gur frdhrapr erirefrf: A orpbzrf N, B orpbzrf O, naq fb ba gb M, juvpu orpbzrf Z. Gur nytbevguz vf hfrq va bayvar sbehzf nf n zrnaf bs uvqvat wbxr chapuyvarf, chmmyr fbyhgvbaf, zbivr naq fgbel fcbvyref, naq bssrafivr zngrevnyf sebz gur pnfhny tynapr. EBG13 unf orra qrfpevorq nf gur " Hfrarg rdhvinyrag bs n zntnmvar cevagvat gur nafjre gb n dhvm hcfvqr qbja" . Gur anzr

"EBG13" bevtvangrq ba Hfrarg va gur rneyl 1980f, naq gur zrgubq unf orpbzr n qr snpgb fgnaqneq. Nf n Pnrfne pvcure (n zrgubq bs rapelcgvba gubhfnaqf bs lrnef byq), EBG13 cebivqrf ab erny pelcgbtencuvp frphevgl naq vf abg hfrq sbe fhpu; va snpg vg vf bsgra hfrq nf gur pnabavpny rknzcyr bs jrnx rapelcgvba. Na nqqvgvbany srngher bs gur pvcure vf gung vg vf flzzrgevpny; gung vf, gb haqb EBG13, gur fnzr nytbevguz vf nccyvrq, fb gur fnzr pbqr pna or hfrq sbe rapbqvat naq qrpbqvat.

PYNPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_uJdSftmh}

14. A type of transposition cipher is the rail fence cipher. Here is one such cipher encrypted using the rail fence with 4 rails. Can you decrypt it? Put the decoded message in the CLACTF flag format, CLACTF{decoded_message}. The message reads

Ta _7N6DDDhlg:W3D_H3C31N__0D3ef sHR053F38N43D0F i33___NA

15. Hashing is a system by which information is encrypted so it can never be decrypted. theoretically, websites will often hash passwords so that if their passwords are ever leaked, bad actors won't actually learn the user's password; they'll just get an encrypted form. However, the same password will always hash to the same ciphertext, so if the attacker can guess your password, they can figure out the hash. Can you guess the password for this hash?

cb78e77e659c1648416cf5ac43fca4b65eeaefe1

16. smh I can't even crack this password:

b0439fae31f8cbba6294af86234d5a28

17. This is the flag that is encrypted! Can you discover the flagged content?

395f4dfc82f56b796b23c3fa1b5150cbe568d71e

18. This is the flag that is encrypted! Can you discover the flagged content?

2412f72f0f0213c98c1f9f6065728da4529000e5c3a2e16c4e1379bd3e13ccf543201eec4eb7b400eb5a6c9b774b
f0c0eeda44869e08f3a54a0b13109a7644aa

19. Get the validation password. - Encoding - UU

B5F5R>2!S:6UP;&4@.RD*4$%34R`](%5,5%)!4TE-4$Q%"@``
`

20. Hash - SHA-2 -> This hash was stolen during a session interception on a critical application, errors may have occurred during transmission. No crack attempt has succeeded so far; the hash format seems unknown. Find the corresponding plaintext. The answer is the SHA-1 of this password.

96719db60d8e3f498c98d94155e1296aac105ck4923290c89eeeb3ba26d3eef92

Tools:

Crack station

Cyberchef.org

dCode

Decode online

Rail fence cipher: Encode and decode online - cryptii

Inspired from

1. picoCTF
2. Root Me
3. CTFlearn
4. CTFtime

Code Labs Academy Berlin - Coding Bootcamp
Lobeckstraße 36-40, 10969 Berlin
Phone: +49 308 3793271/+49 157 35998895

We hope you enjoyed the CTF challenge and learned something new! We would love to hear your thoughts and feedback on how we can improve future sessions. Please take a moment to share your experience and let us know how much you enjoyed the challenge. Your feedback is important to us and will help us continue to provide engaging and informative events. Thank you for participating!

[We value your feedback](#)