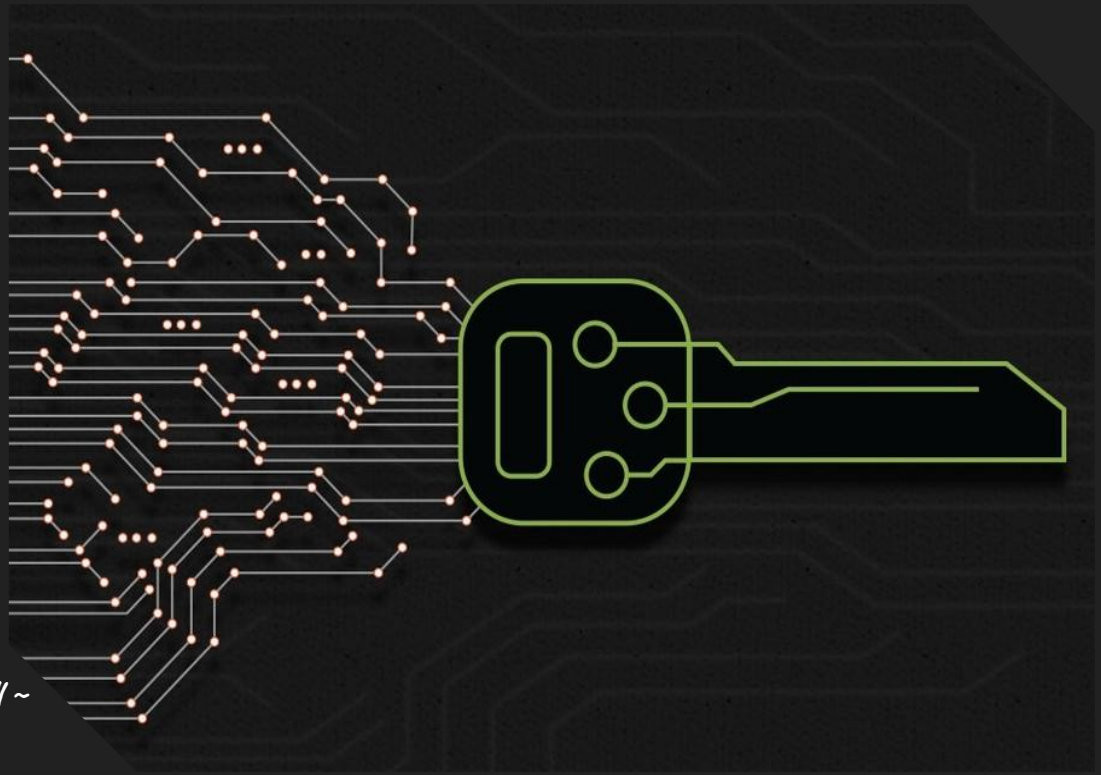
CCSC
BOOTCAMP TRAINING

Day 1 : Cryptography



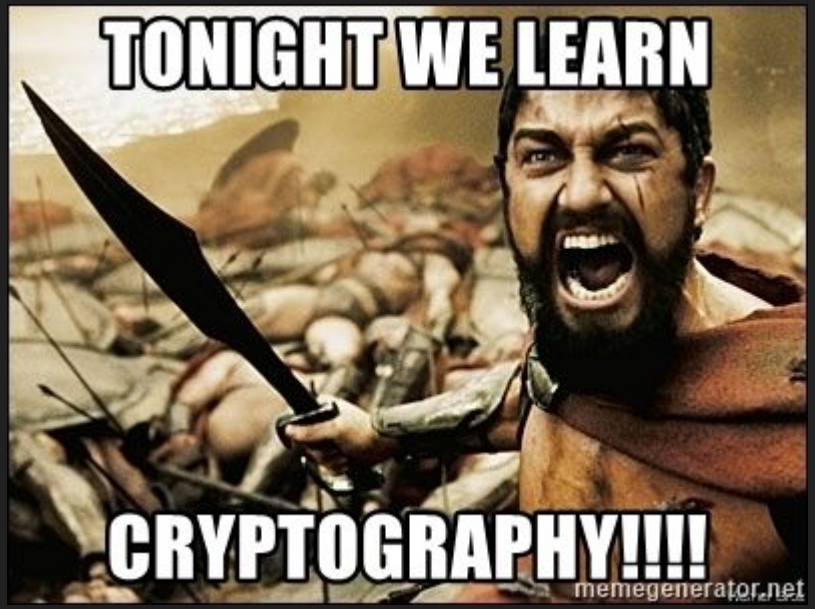
~ [CCSC] CIT Cyber Security Cell ~
OUSSAMA RAHALI
OMAR AOUAJ

CLUB INFORMATIQUE & TÉLÉCOM

cat README.md

Presentation outline

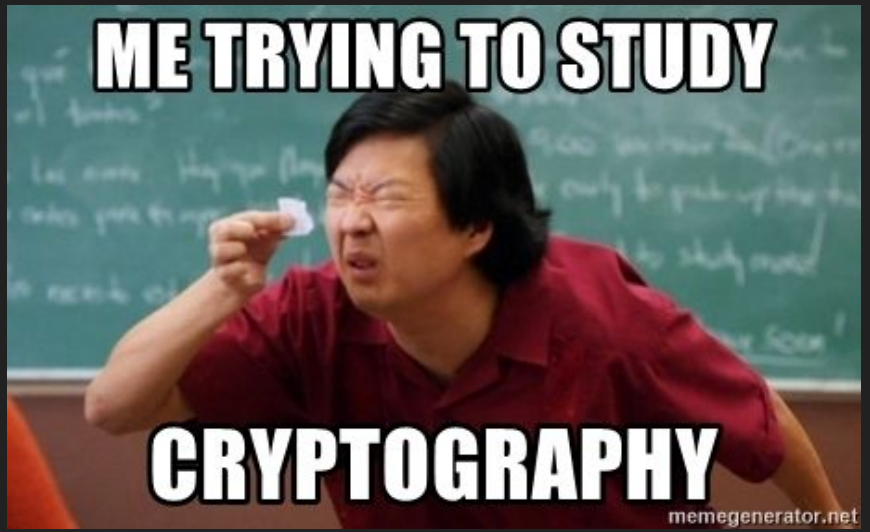
1. Cryptography :
   1.1 notions
2. General :
   2.1 Encoding
      2.1.1 ASCII
      2.1.2 HEX
      2.1.3 Base64 / 32
   2.2 Caesar cipher / ROT13
   2.3 XOR



`whatis` Cryptography

ideas

Familiarity (1-10) ?

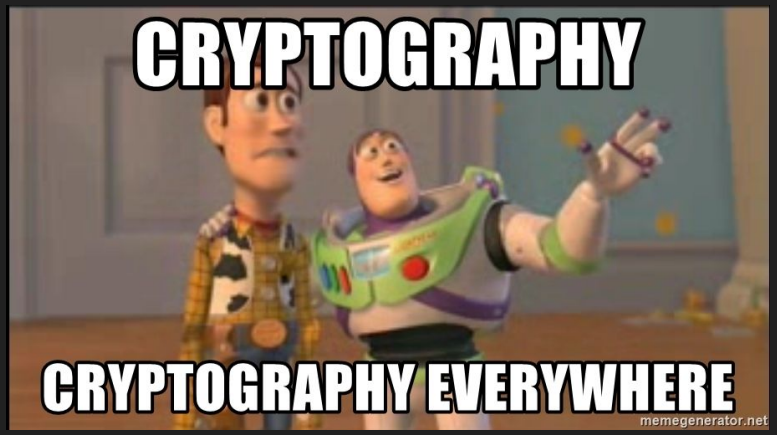


Warning !

As we head through this meeting, we're gonna have some challenges for you to answer.. If you were able to solve one, please write DONE in the chat without writing the solution.

Don't spoil solutions on your friends :) !

Cryptography



Cryptography refers almost exclusively to encryption, the process of converting ordinary information (plaintext) into ciphertext . Decryption is the reverse, moving from unintelligible ciphertext to plaintext.

Some Basic Notions

Plaintext : Our message that we want to encrypt

Ciphertext : The result of encrypting the plaintext

Encryption Function E : The method by which we transform the plaintext to ciphertext

Decryption Function D : The method by which we transform the ciphertext to plaintext

Some Basic Notions

Given :

- *Plaintext :* P
- *Ciphertext :* C

⇒

$$E(P) = C$$
$$D(C) = P$$

GENERAL

Encoding

ASCII

ASCII is a 7-bit encoding standard which allows the representation of text using the integers 0-127.

GENERAL

classic cryptography

Encoding

ASCII

DEMO - 1 : 5 min

>> Using the below integer array, convert the numbers to their corresponding ASCII characters to obtain a flag.

```
[70, 108, 97, 103, 123, 67, 67, 83, 67,
95, 99, 114, 121, 112, 116, 111, 125]
```

GENERAL

Encoding

HEX

The hexadecimal, or base-16, system was created to emulate some of the same properties of the common decimal system. The overall difference is, 16 digits are available instead of the 10 digits available to use to notate the value of a number.
The 16 symbols that the hexadecimal system uses are: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E and F.

GENERAL

classic cryptography

Encoding

HEX

DEMO - 2 : 5 min

>> Included below is a the flag encoded as a hex string. Decode this back into bytes to get the flag .

466c61677b434353435f63727970746f7d

GENERAL

Encoding

BASE-64

Base64 schemes represent binary data in an ASCII string format by translating it into a base64 representation. This basically means that all kind of characters with control characters can be mapped to an English alphabet a-z, A-Z, 0-9 and you would be able to read them all on the screen, or even print them out.

N.B: The encoded string must be have a length which is a multiple of 4, if that's not the case, the base64 complete the string with equal signs "=".

GENERAL

Encoding

BASE-64

DEMO - 3 : 5 min

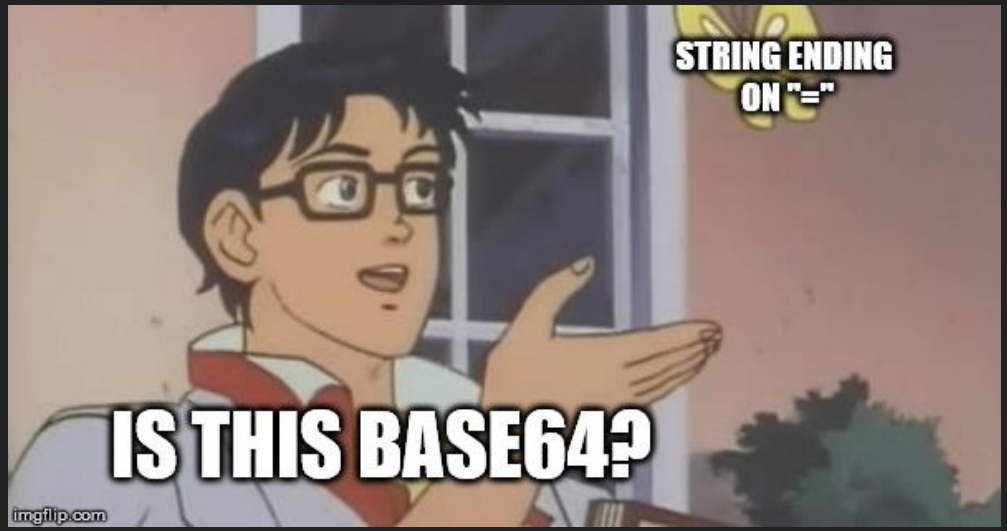
>> Take the below base64 encoded string, and decode it.

RmxhZ3tDQ1NDX2NyeXB0b30K

GENERAL

Encoding

BASE-32



GENERAL

Encoding

BASE-32

DEMO - 4 : 5 min

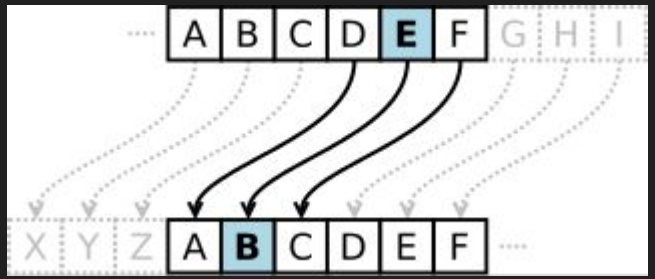
>> Take the below Base32 string, and decode it .

IZWGCZ33INBVGQ27MNZHS4DUN56Q====

Caesar Cipher

Classic cryptography

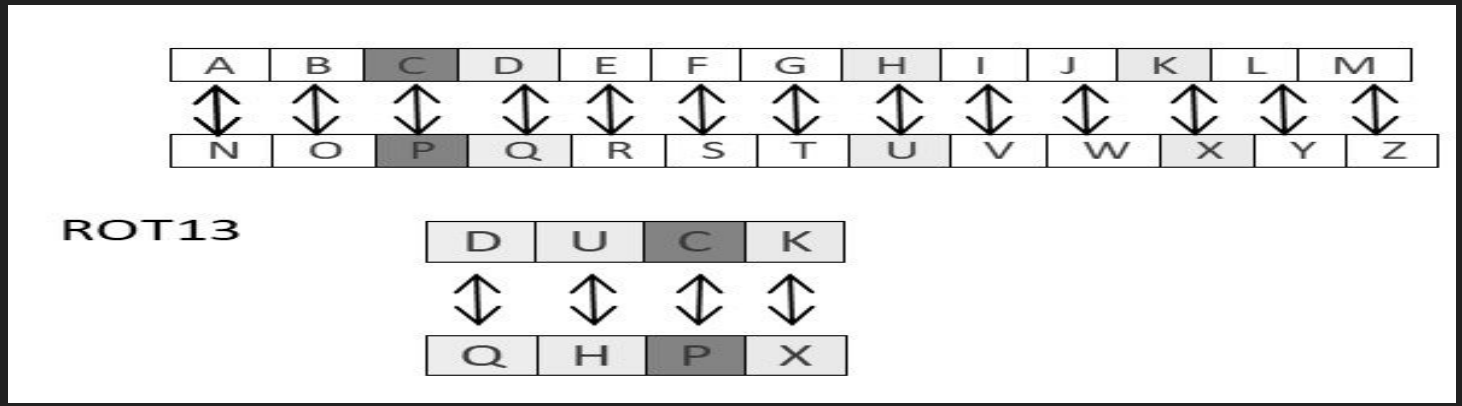
To pass an encrypted message from one person to another, it is first necessary that both parties have the 'key' for the cipher, so that the sender may encrypt it and the receiver may decrypt it. For the caesar cipher, the key is the number of characters to shift the cipher alphabet.



ROT-13

Classic cryptography

ROT13 cipher refers to the abbreviated form Rotate by 13 places. It is a special case of Caesar Cipher in which shift is always 13. Every letter is shifted by 13 places to encrypt or decrypt the message.



ROT-13

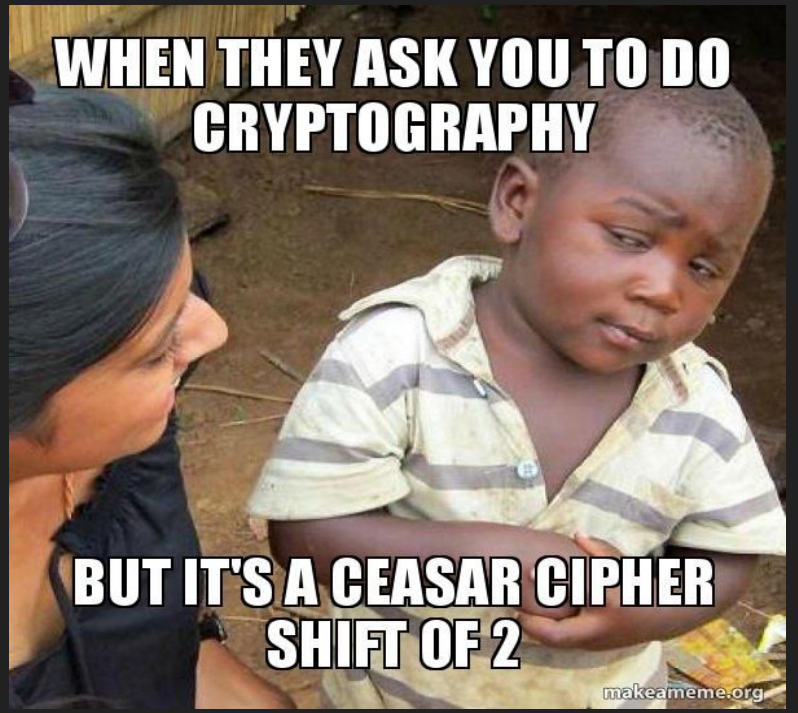
DEMO - 5 : 10 min

Tasks :

0x0 : Take the below string, and decode it w/ a python script !

0x1: Try to find the correct bash command line to decode it !

PPFP obbgpnzc genvavat ebg 13 qrzb



XOR Cipher

Classic cryptography

It's probably the most known cipher since i's based on a simple binary operation (in python it's represented by " ^ ").
It's useful in cryptography since it's fastly reversible.
Encoding: plain_text ^ key = cipher_text
Decoding: cipher_text ^ key = plain_text
P.s: It can also be used to encode images or any file and not just strings..

XOR Cipher

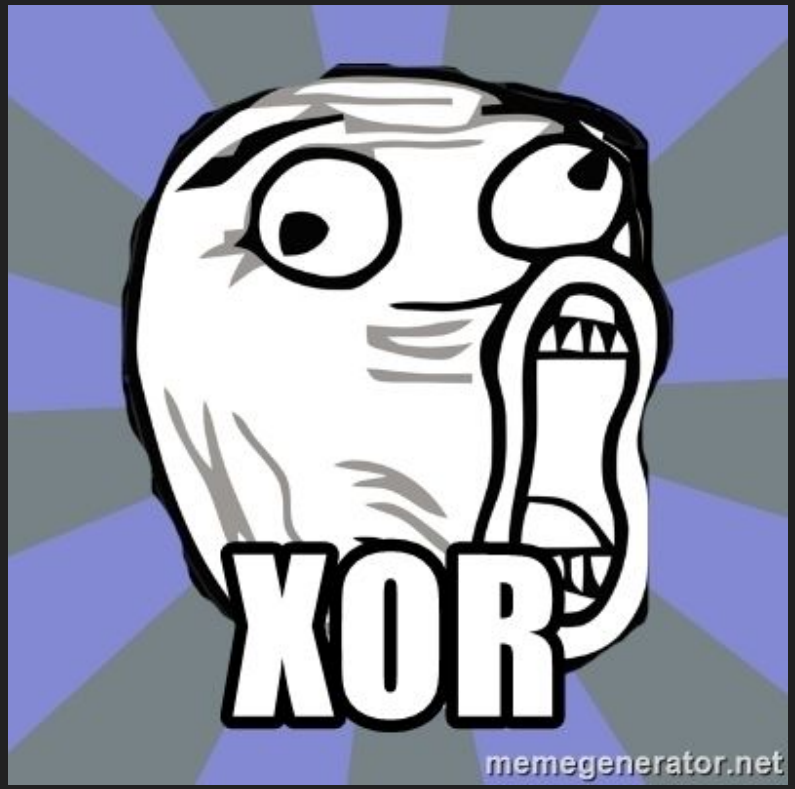
Classic cryptography

DEMO - 6 : 5 min

Task :

Take the below string, and decode it with the key: CCSC

```
>>>  ,=$1"'6/"'*,-
c,-s:,6!c%*!07c+,1c0+"/?
```



Tools

documentation

https://www.dcode.fr/

https://www.dcode.fr/frequency-analysis

https://cryptii.com/

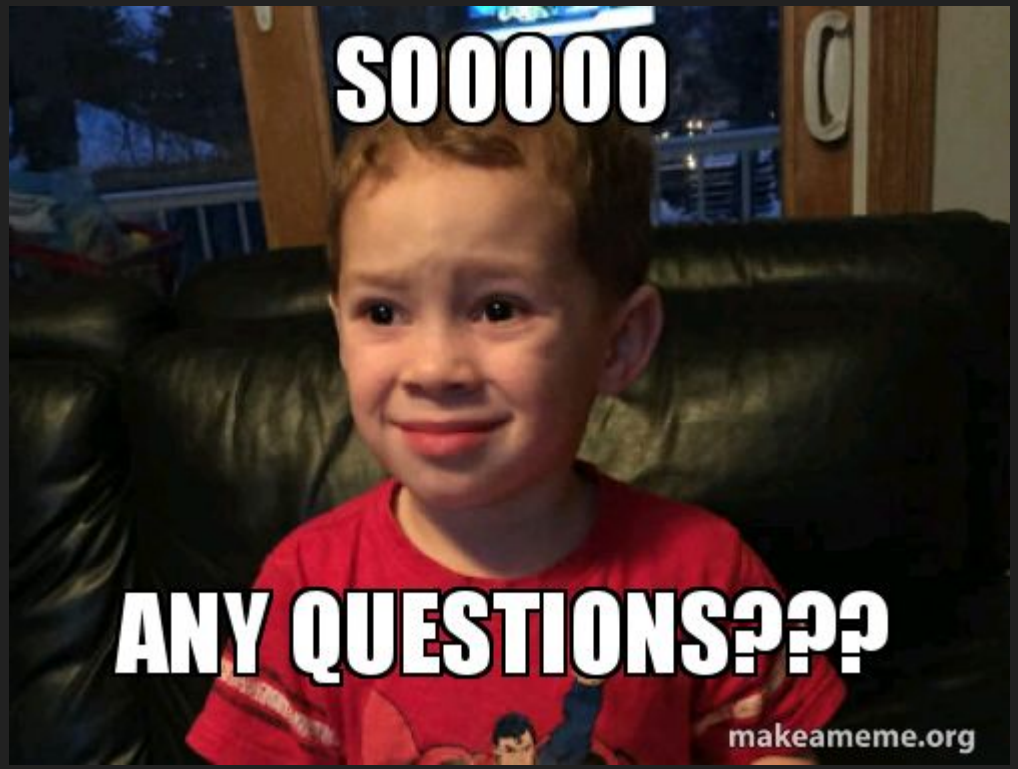
https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

https://quipqiup.com/

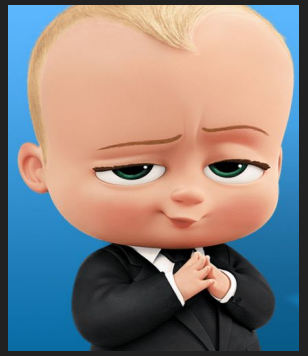
https://www.boxentriq.com/code-breaking/cipher-identifier

shutdown

tfi dak lmch9of



ls -al .Contact_us



OUSSAMA RAHALI

Facebook : /oussama.rahali.925

OMAR AOUAJ

Facebook : /omar.aouaj.77