CRYPTOGRAPHY – The CTF Resource

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. - Wikipedia

In CTF challenges there is a category called cryptography which ha an encrypted text which is not understandable by the player the aim of the challenge is to decrypt the text and find the flag!

In this challenge you would find many types of the cipher texts to find the cipher and the way to decrypt the cipher I had created this resource. This resource consists of cipher texts encryption and decryption techniques.

Before we start with cipher texts these are some tools used to decrypt the cipher text.

1. Cryptii:- this has multiple decoder like base64,ROT13 and many more. https://cryptii.com
2. Decode.fr:- Another wonderful tool for decoding it has multiple tolls in it and this is my personal favorite as it has option of brute forcing this helped me in many CTF challenges. https://www.dcode.fr/

Cipher text: -

- Caesar Cipher

  The most classic shift cipher. Tons of online tools like this: https://www.dcode.fr/caesar-cipher or use `caesar` as a command-line tool (`sudo apt install bsdgames`) and you can supply a key for it. Here's a one liner to try all letter positions:

  ```
   cipher='jeoi{geiwev_gmtliv_ws_svmkmrep}' ; for i in {0..25}; do echo
  $cipher | caesar $i; done
  ```

  Be aware! Some challenges include punctuation in their shift! If this is the case, try to a shift within all 255 ASCII characters, not just 26 alphabetical letters!

- `caesar`

  A command-line caesar cipher tool (noted above) found in the `bsdgames` package.

- Atbash Cipher

  If you have some text that you have no idea what it is, try the Atbash cipher! It's a letter mapping, but the alphabet is reversed: like `A` maps to `Z`, `B` maps to `Y` and so on. There are tons of online tools to do this (http://rumkin.com/tools/cipher/atbash.php), and you can build it with Python.

- Vigenere Cipher

  http://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx, https://www.guballa.de/vigenere-solver and personal Python code here: https://pastebin.com/2Vr29g6J

- Gronsfeld Cipher

  A variant of the Vignere cipher that uses numbers insteads of letters. http://rumkin.com/tools/cipher/gronsfeld.php

- Beaufourt Cipher

  https://www.dcode.fr/beaufort-cipher

- Python random module cracker/predictor

  https://github.com/tna0y/Python-random-module-cracker... helps attack the Mersenne Twister used in Python's random module.

- Transposition Cipher
- RSA: Classic RSA

  Variables typically given: `n`, `c`, `e`. *ALWAYS* try and give to http://factordb.com. If `p` and `q` are able to be determined, use some RSA decryptor; handmade code available here: https://pastebin.com/ERAMhJ1v

- RSA: Multi-prime RSA

  When you see multi-prime RSA, you can use calculate `phi` by still using all the factors.

```
phi = (a - 1) * (b - 1) * (c - 1)    # ... etcetera
```

If FactorDB cannot find factors, try alpertron: https://www.alpertron.com.ar/ECM.HTM

- RSA: `e` is 3 (or small)

  If `e` is 3, you can try the cubed-root attack. If you the cubed root of `c`, and if that is smaller than the cubed root of `n`, then your plaintext message `m` is just the cubed root of `c`! Here is Python code to take the cubed root:

```
def root3rd(x):
    y, y1 = None, 2
    while y!=y1:
        y = y1
        y3 = y**3
        d = (2*y3+x)
        y1 = (y*(y3+2*x)+d//2)//d
    return y
```

- RSA: Wiener's Little D Attack

  The telltale sign for this kind of challenge is an enormously large `e` value. Typically `e` is either 65537 (0x10001) or `3` (like for a Chinese Remainder Theorem challenge).

- RSA: Boneh-Durfee Attack The tellgate sign for this kind of challenge is also an enormously large `e` value (`e` and `n` have similar size).
- RSA: Chinese Remainder Attack These challenges can be spotted when given mutiple `c` cipher texts and multiple `n` moduli. `e` must be the same number of given `c` and `n` pairs.

To solve this there is a wonderful tool available in git hub which has a 6 types of RSA decoders and many more cipher :- https://github.com/AdityaSec/dagger

I personally prefer this tool for RSA decodeing.

- LC4

  This is an adaptation of RC4... just not. There is an implementation available in Python. https://github.com/dstein64/LC4/blob/master/documentation.md

- Elgamal:-

  ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange

- Affine Cipher

  The affine is a type of monoalphabetic substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

- Substitution Cipher (use quip quip!)

  https://quipqiup.com/

- Railfence Cipher

  http://rumkin.com/tools/cipher/railfence.php

- Playfair Cipher

  racker: http://bionsgadgets.appspot.com/ww_forms/playfair_ph_web_worker3.html

- Polybius Square

  https://www.braingle.com/brainteasers/codes/polybius.php

- The Engima

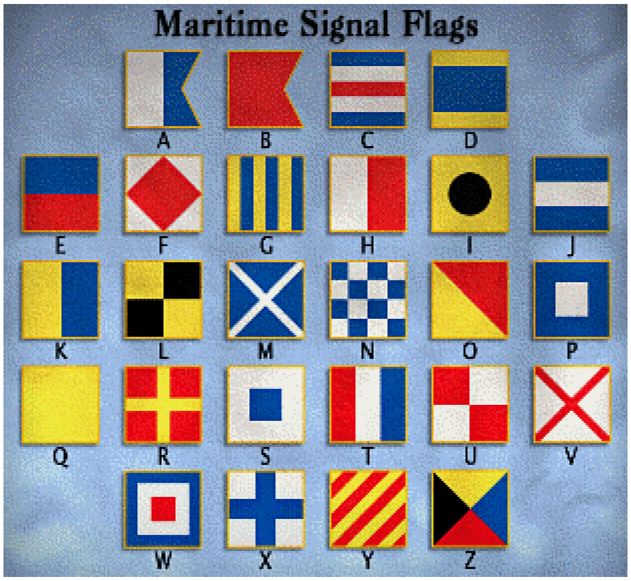
  http://enigma.louisedade.co.uk/enigma.html, https://www.dcode.fr/enigma-machine-cipher

- AES ECB

  The "blind SQL" of cryptography... leak the flag out by testing for characters just one byte away from the block length.

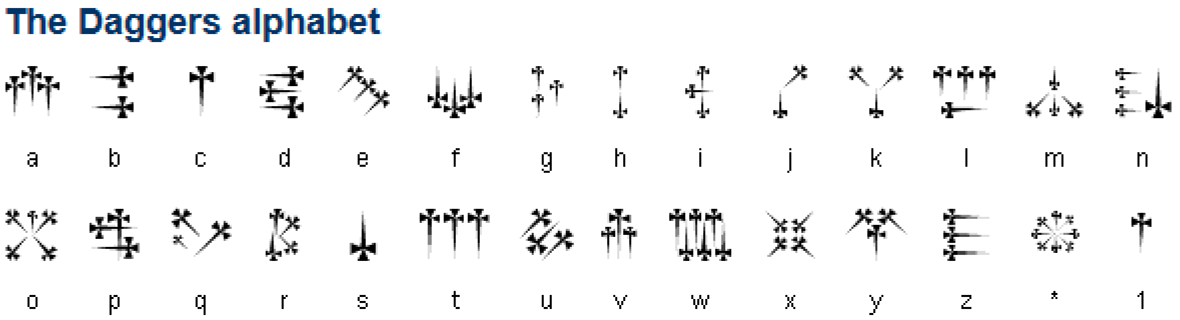
- Two-Time Pad
- International Code of Signals Maritime

  First drafted by the British Board of Trade in 1855 and adopted as a world-wide standard on 1 January 1901. It is used for communications with ships, but also occasionally used by geocaching mystery caches (puzzle caches), CTFs and various logic puzzles. You may want to give a look at the tool maritime flags translator.



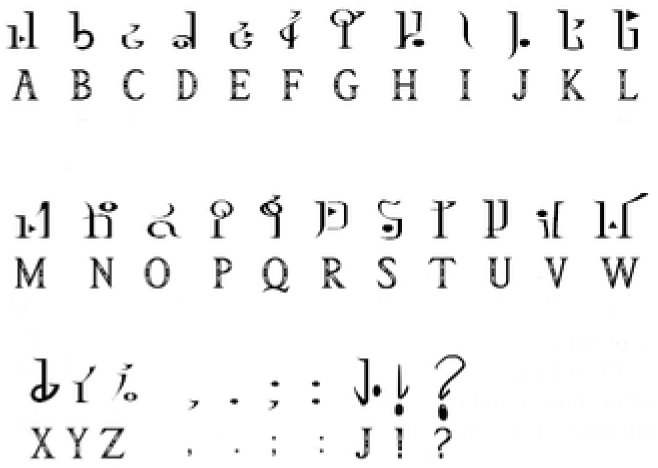
- Daggers Cipher

The daggers cipher is another silly text-to-image encoder. This is the key, and you can find a decoder on https://www.dcode.fr/daggers-alphabet.



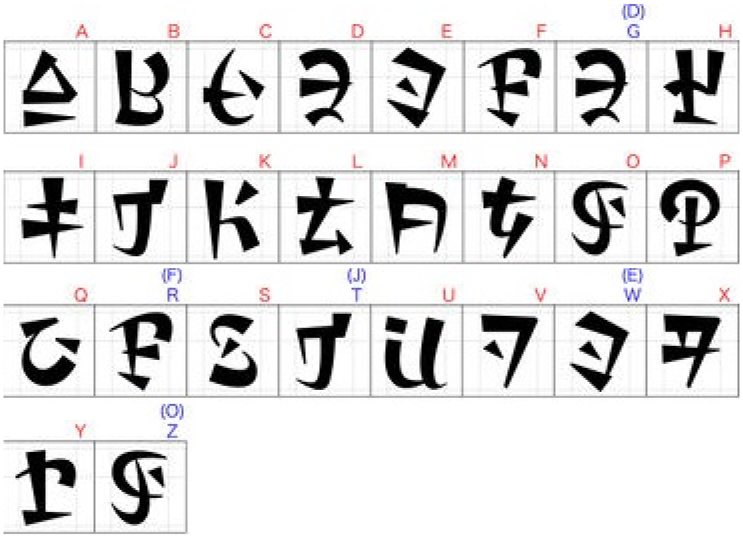
- Hylian Language (Twilight Princess)

The Hylian language is another silly text-to-image encoder. This is the key, and you can find a decoder on https://www.dcode.fr/hylian-language-twilight-princess.



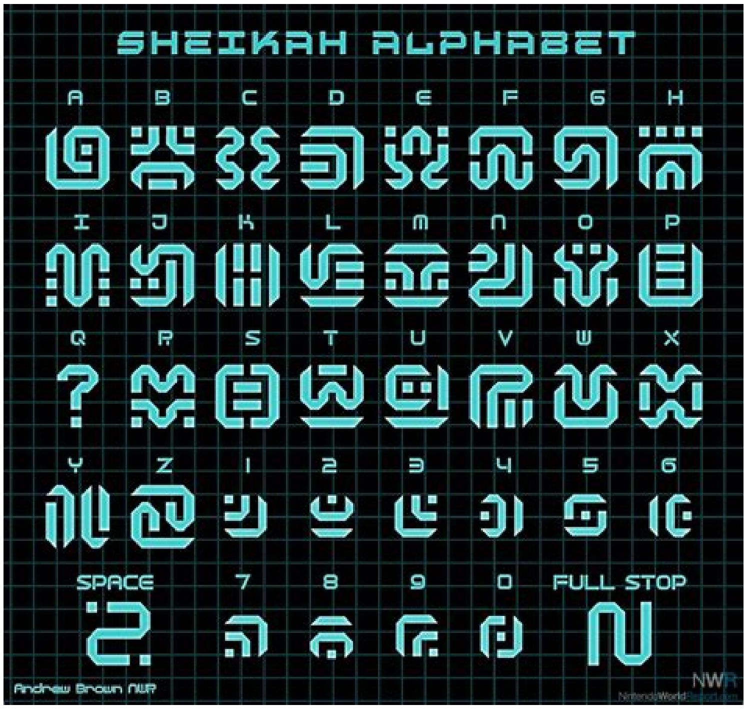
- Hylian Language (Breath of the Wild)

The Hylian language is another silly text-to-image encoder. This is the key, and you can find a decoder on https://www.dcode.fr/hylian-language-breath-of-the-wild.



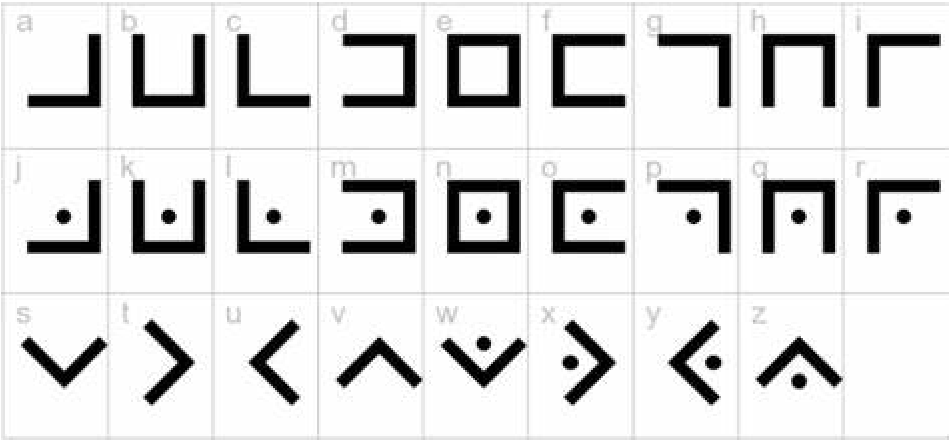
- Sheikah Language (Breathe of the Wild)

The Sheikah language is another silly text-to-image encoder. This is the key, and you can find a decoder on https://www.dcode.fr/sheikah-language.



Pigpen cipher:-

The pigpen cipher is a geometric simple substitution cipher, which exchanges letters for symbols which are fragments of a grid. The example key shows one way the letters can be assigned to the grid.


a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z