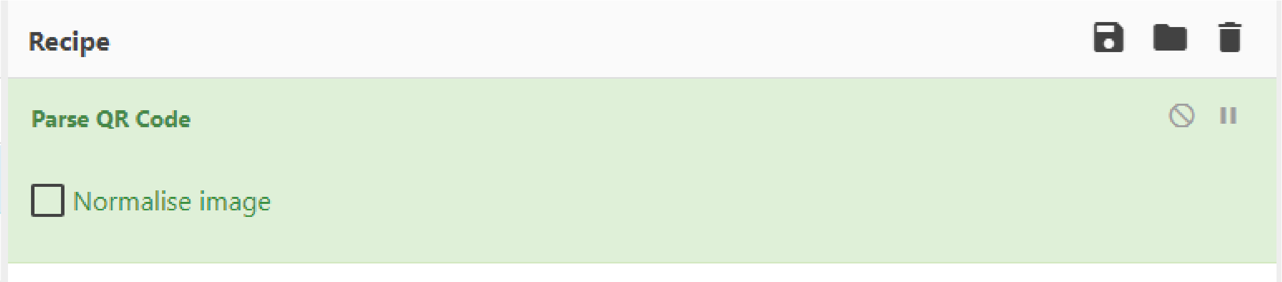
Challenge1: Hello World

Part 1: The QR code

At first we can see that Taguar has supplied us with a QR code and a Base64 encoded string. Lets have a closer look at the QR code. As most steps, needed to solve this challenge, are doable with cyberchef, we will download the QR code and for now drag the file into the input box from cyberchef. Now set the recipe to Parse QR code and hit cook!

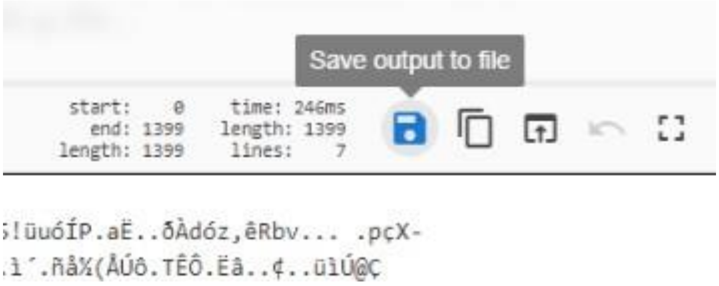


This is the output that we get....

output.txt

output.txt - 2KB

Now to the normal eye this might look like a lot of nonesense, but it is actually very important...go ahead and download the file from cyberchef with the `Save output to file` **button. Do not copy and paste the output, this is very important!!**



```
  start:    0    time: 246ms
    end: 1399  length: 1399
 length: 1399   lines:    7
```

```
5!üuóÍP.aË..ðÀdóz,êRbv... .pçX-
.ì´.ñå%(ÅÚô.TÊÔ.Ëâ..¢..üìÚ@Ç
```

Now navigate to the location where you saved the output and check what type of file it is with the following command:

```
file filename.dat
```

Output:

```
download.dat: gzip compressed data, has CRC, last modified: Sun Jul 18
21:30:14 2021, original size modulo 2^32 3222
```

Perfect! It is a gzip file. Let's extract the content! Add the extension from gz to the file with the following command:

```
mv filename.dat filename.dat.gz
```

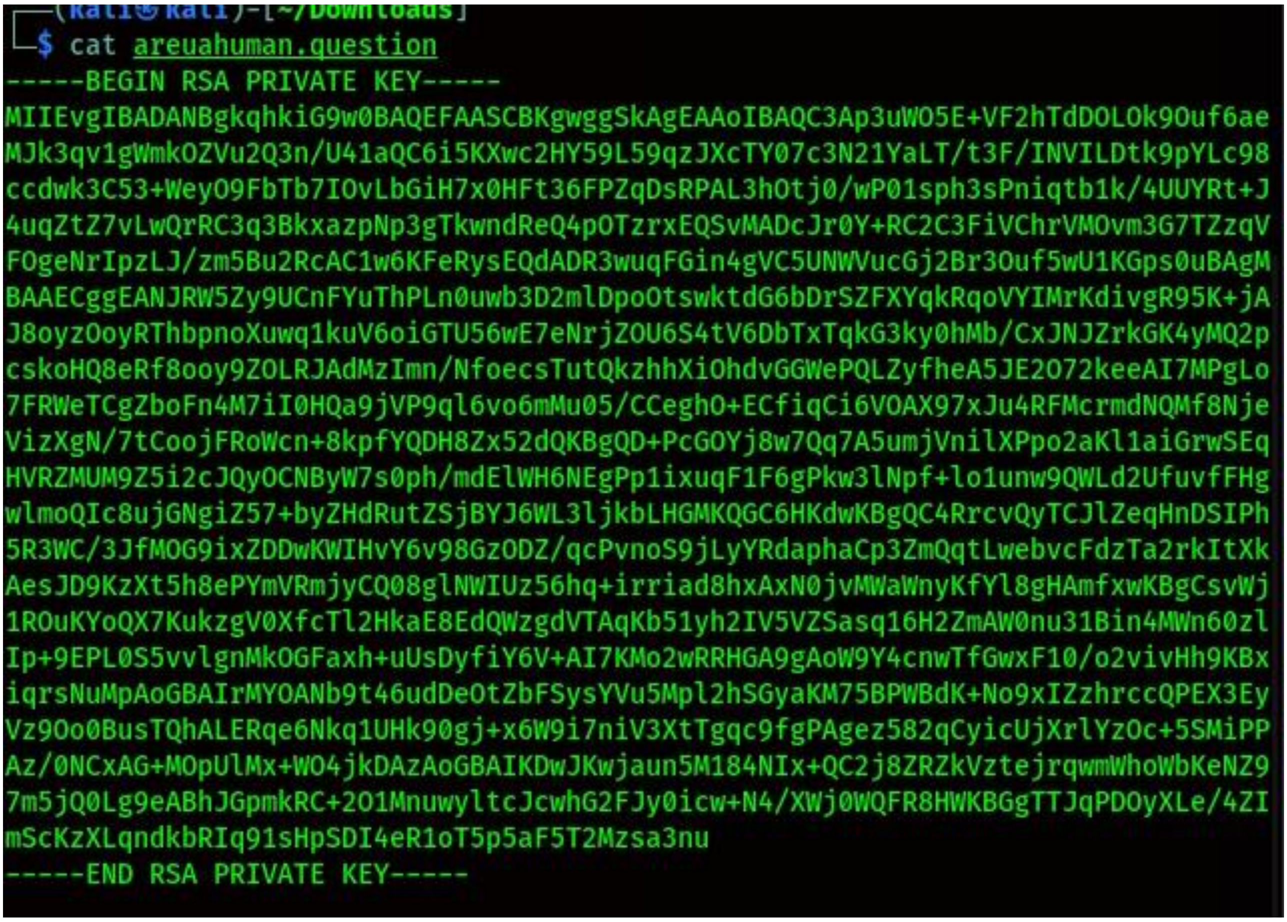
And extract it:

```
gzip -d filename.dat.gz
```

After this we get a tar archive...let's extract this one!:

```
tar -xvf filename.dat
```

Now we get a file named areuahuman.question. If we view the contents of that file we get an RSA private key! Super!

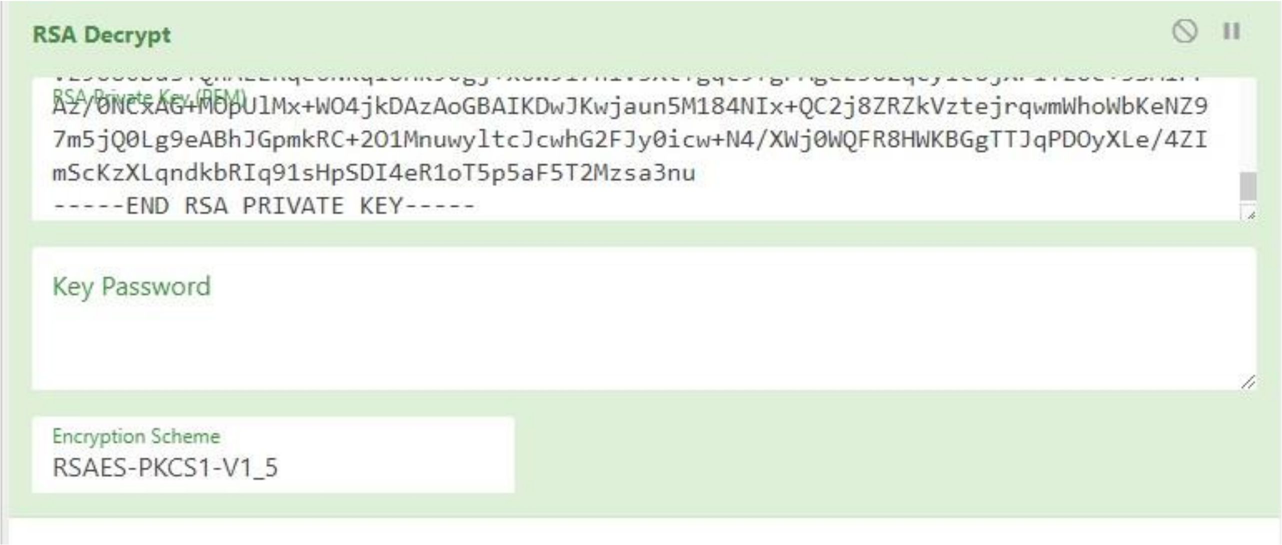


```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat areuahuman.question
-----BEGIN RSA PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC3Ap3uWO5E+VF2hTdDOLOk9Ouf6ae
MJk3qv1gWmkOZVu2Q3n/U41aQC6i5KXwc2HY59L59qzJXcTY07c3N21YaLT/t3F/INVILDtk9pYLc98
ccdwk3C53+WeyO9FbTb7IOvLbGiH7x0HFt36FPZqDsRPAL3hOtj0/wP01sph3sPniqtb1k/4UUYRt+J
4uqZtZ7vLwQrRC3q3BkxazpNp3gTkwndReQ4pOTzrxEQSvMADcJr0Y+RC2C3FiVChrVMOvm3G7TZzqV
FOgeNrIpzLJ/zm5Bu2RcAC1w6KFeRysEQdADR3wuqFGin4gVC5UNWVucGj2Br3Ouf5wU1KGps0uBAgM
BAAECggEANJRW5Zy9UCnFYuThPLn0uwb3D2mlDpoOtswktdG6bDrSZFXYqkRqoVYIMrKdivgR95K+jA
J8oyzOoyRThbpnoXuwq1kuV6oiGTU56wE7eNrjZOU6S4tV6DbTxTqkG3ky0hMb/CxJNJZrkGK4yMQ2p
cskoHQ8eRf8ooy9ZOLRJAdMzImn/NfoecsTutQkzhhXiOhdvGGWePQLZyfheA5JE2O72keeAI7MPgLo
7FRWeTCgZboFn4M7iI0HQa9jVP9ql6vo6mMu05/CCeghO+ECfiqCi6VOAX97xJu4RFMcrmdNQMf8Nje
VizXgN/7tCoojFRoWcn+8kpfYQDH8Zx52dQKBgQD+PcGOYj8w7Qq7A5umjVnilXPpo2aKl1aiGrwSEq
HVRZMUM9Z5i2cJQyOCNByW7s0ph/mdElWH6NEgPp1ixuqF1F6gPkw3lNpf+lo1unw9QWLd2UfuvfFHg
wlmoQIc8ujGNgiZ57+byZHdRutZSjBYJ6WL3ljkbLHGMKQGC6HKdwKBgQC4RrcvQyTCJlZeqHnDSIPh
5R3WC/3JfMOG9ixZDDwKWIHvY6v98GzODZ/qcPvnoS9jLyYRdaphaCp3ZmQqtLwebvcFdzTa2rkItXk
AesJD9KzXt5h8ePYmVRmjyCQ08glNWIUz56hq+irriad8hxAxN0jvMWaWnyKfYl8gHAmfxwKBgCsvWj
1ROuKYoQX7KukzgV0XfcTl2HkaE8EdQWzgdVTAqKb51yh2IV5VZSasq16H2ZmAW0nu31Bin4MWn60zl
Ip+9EPL0S5vvlgnMkOGFaxh+uUsDyfiY6V+AI7KMo2wRRHGA9gAoW9Y4cnwTfGwxF10/o2vivHh9KBx
iqrsNuMpAoGBAIrMYOANb9t46udDeOtZbFSysYVu5Mpl2hSGyaKM75BPWBdK+No9xIZzhrccQPEX3Ey
Vz9Oo0BusTQhALERqe6Nkq1UHk90gj+x6W9i7niV3XtTgqc9fgPAgez582qCyicUjXrlYzOc+5SMiPP
Az/0NCxAG+MOpUlMx+WO4jkDAzAoGBAIKDwJKwjaun5M184NIx+QC2j8ZRZkVztejrqwmWhoWbKeNZ9
7m5jQ0Lg9eABhJGpmkRC+2O1MnuwyltcJcwhG2FJy0icw+N4/XWj0WQFR8HWKBGgTTJqPDOyXLe/4ZI
mScKzXLqndkbRIq91sHpSDI4eR1oT5p5aF5T2Mzsa3nu
-----END RSA PRIVATE KEY-----
```

Part 2: RSA

First we have to decode the base64 string. This is pretty easy. Just set the recipe to From Base64 and paste the encoded string into the input window(*Again download the output do not copy paste as it can lead to errors!*). And then you are set to decrypt the message! :D

On cyberchef set the recipe to RSA decrypt. It will ask you for the Key, the password for the key and an encryption scheme. Paste the private key into the RSA Private Key field, set the encryption scheme to the second one! You can leave the password field empty, because the key hasn't got one set. Now all you have to do is put a message, which in our case is the decoded base64 string(the output you downloaded), into the input window and hit cook!



RSA Private Key (PEM)

```
Az/0NCxAG+M0pU1Mx+WO4jkDAzAoGBAIKDwJKwjaun5M184NIx+QC2j8ZRZkVztejrqwmWhoWbKeNZ9
7m5jQ0Lg9eABhJGpmkRC+2O1MnuwyltcJcwhG2FJy0icw+N4/XWj0WQFR8HWKBGgTTJqPDOyXLe/4ZI
mScKzXLqndkbRIq91sHpSDI4eR1oT5p5aF5T2Mzsa3nu
-----END RSA PRIVATE KEY-----
```

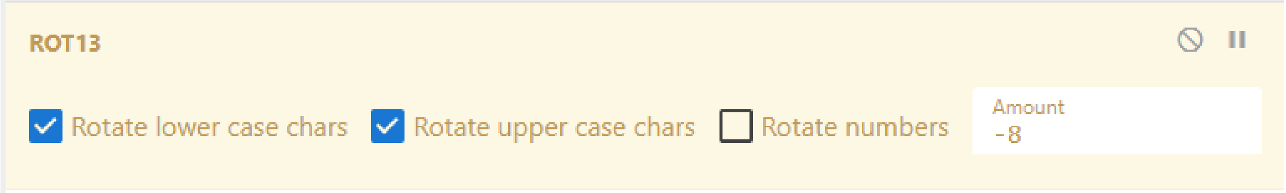
Key Password

Encryption Scheme: RSAES-PKCS1-V1_5

Nice! We got it! The decoded key seems to be a Base85 encoded string. This is also no problem! Just download the output, set the recipe to From Base85 and put the file into the input window.

Part 3: The finale

Now after all of this...we finally are at the last step! The base85 output seems to be a ROT 8 encoded string! This is easy! Set the recipe to ROT of any choice and make sure that the amout is set to -8.



ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars □ Rotate numbers

Amount
-8

Take the ROT 8 encrypted string and paste it into the input window! The output you get is the solution! :)
Thank you very much for reading this writeup! :D