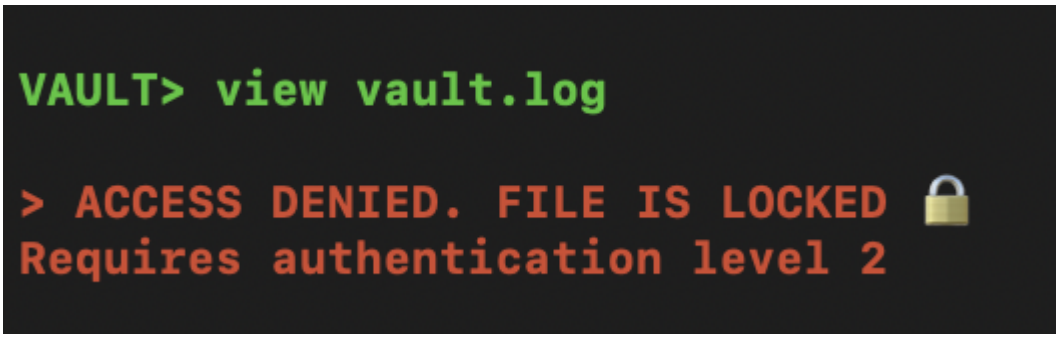
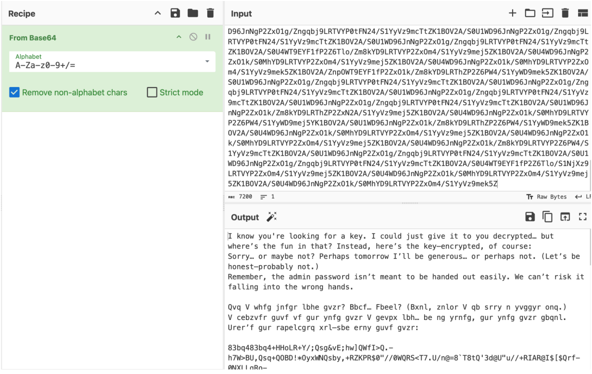
Here is a hint:



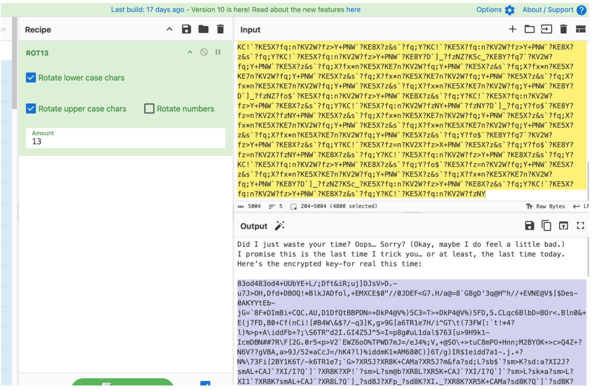
The memdump contains multiple words, but the correct one is just once.

When you run analyze you can see memory corruption(is the same as the memory from the line where the password was)

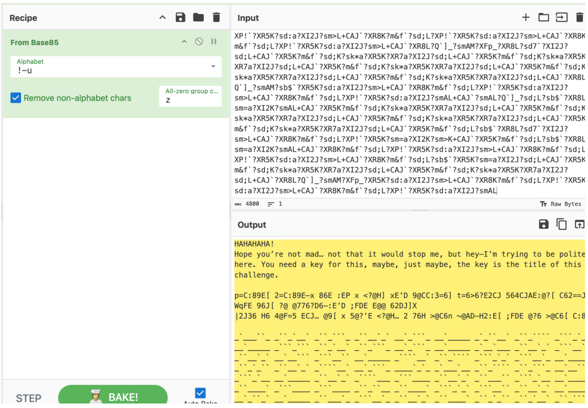
After you unlock vault.log is the key you need for decrypting .emergency_overide. This is how to find the key:



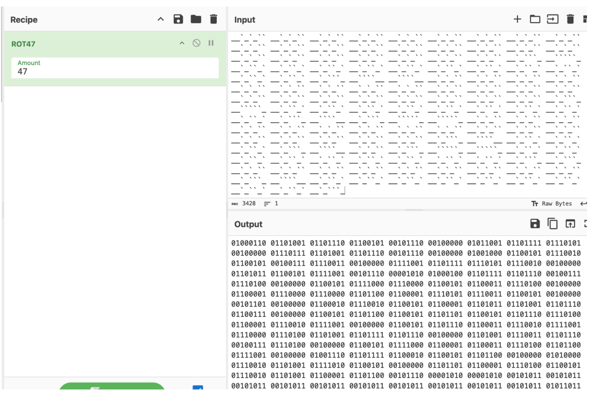
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Input
Output
I know you're looking for a key. I could just give it to you decrypted… but where's the fun in that? Instead, here's the key—encrypted, of course:
Sorry… or maybe not? Perhaps tomorrow I'll be generous… or perhaps not. (Let's be honest—probably not.)
Remember, the admin password isn't meant to be handed out easily. We can't risk it falling into the wrong hands.
Qvq V whfg jnfgr lbhe gvzr? Bbcf… Fbeel? (Bxnl, znlor V qb srry n yvggyr onq.)
V cebzvfr guvf vf gur ynfg gvzr V gevpx lbh… be ng yrnfg, gur ynfg gvzr gbqnl.
Urer'f gur rapelcgrq xrl—sbe erny guvf gvzr:



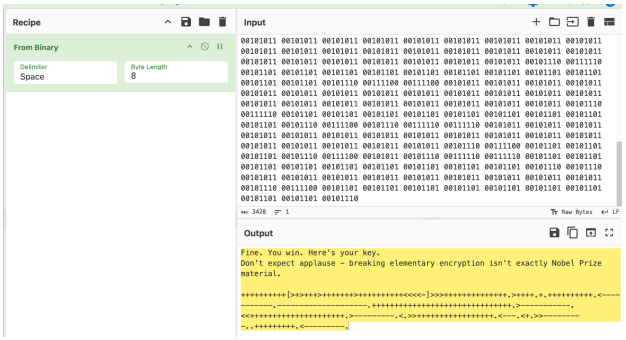
Last build: 17 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
ROT13
Rotate lower case chars
Rotate upper case chars
Rotate numbers
Amount
13
Input
5004
5
204→5004 (4800 selected)
Raw Bytes
Output
Did I just waste your time? Oops… Sorry? (Okay, maybe I do feel a little bad.)
I promise this is the last time I trick you… or at least, the last time today.
Here's the encrypted key—for real this time:

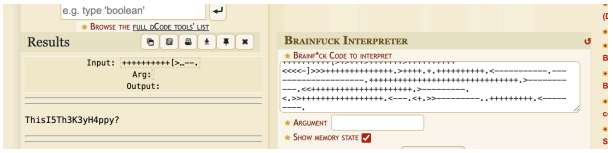


Recipe
From Base85
Alphabet
!-u
Remove non-alphabet chars
All-zero group c…
z
Input
4800
1
Raw Bytes
Output
HAHAHAHA!
Hope you're not mad… not that it would stop me, but hey—I'm trying to be polite here. You need a key for this, maybe, just maybe, the key is the title of this challenge.
STEP
BAKE!



Recipe
ROT47
Amount
47
Input
3420
1
Raw Bytes
Output





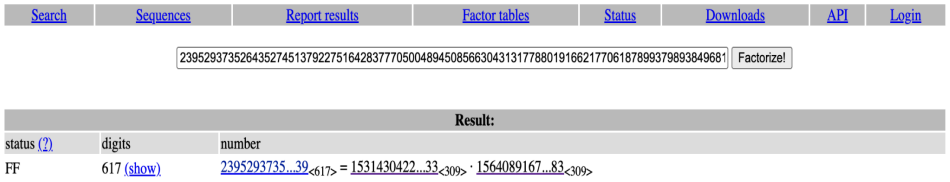
After finding the key you can decrypt .emergency_override

```
AVAILABLE COMMANDS:
LIST              - View visible system files
VIEW <file>       - Display contents of a file
MEMDUMP           - Display memory sectors (warning: restricted)
AUTH              - Attempt authentication
HELP              - Show this help menu
RESTART           - Reboot interface
EXIT              - Close session

LIST -A           - View all system files (requires level 2 access)
DECRYPT           - Decrypt protected files
ANALYZE           - Run memory pattern analysis
UNLOCK <file>     - Attempt to unlock a restricted file (requires level 2 access)
ADMIN             - Log As admin

VAULT> lsit -a
Unrecognized command. Type HELP.

VAULT> list -a

> DIRECTORY: /mnt/sec/
 - system.log
 - auth_records.txt
 - vault.log
 - .memdump_cache
 - .emergency_override

VAULT> view .emergency_override

> FILE IS ENCRYPTED 🔒

VAULT> decode .emergency_override
Unrecognized command. Type HELP.

VAULT> decrypt .emergency_override

> Decryption requires a key:
KEY> ThisI5Th3K3yH4ppy?
> ADDRESS VERIFIED
> DECRYPTING .emergency_override...

> Opening .emergency_override
```

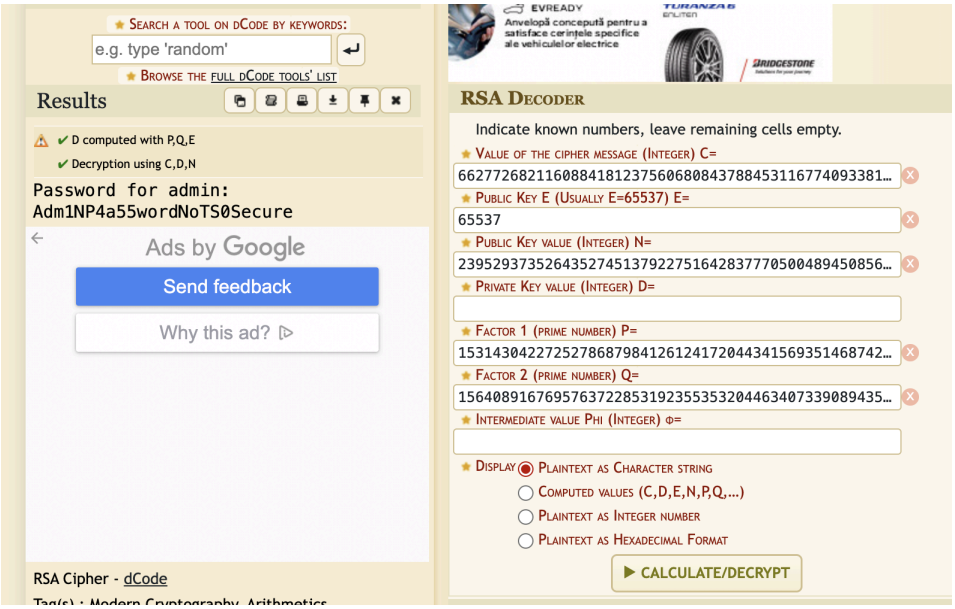
In this file you have a RSA encryption.

```
>> n = 23952937353643527451379227516462837770500409450856630431317788019146217706187899379893849681812990781704953836520667140193826566371235123978523750734131185838362893218308314561469658541192166299207837610399080698925728947259090216745730288819829315333083734504191918095323827886092315374626150075941162029986439515878350953503925971435952673892473695275975350335761493920434089207567616917911245262068773167053490606984596563345574860664906239429328996705934814320660076582002139260827052885623830684919111324135584239632521013235804661631290133798746447379904076227187638903145505164093768174540905724619049879569723 9
>> c = 662772682116088418123756068084378845311677409338181199550536241553038452707936841248885589682225598205297534888070987199414177729640273976618367144256635915429134266095545734250765427514181920335274307345532125237474762986049946677555953182372750002949561497536901991151016113955068561113212057525471918924198465573504637825629556145894790779378852378006180754754338666791377240622900685877558159480707932469104214032171347517179653336150256478222411398098781925738948775453236027603299511118510611031352293046314378878625176076403724603623642634232770110617087495980798644858486781035539297528463795243581420886693960
```

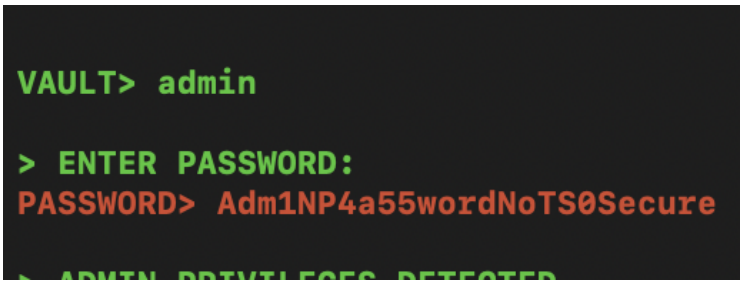
P and Q is easy to find, and e has the most usually value



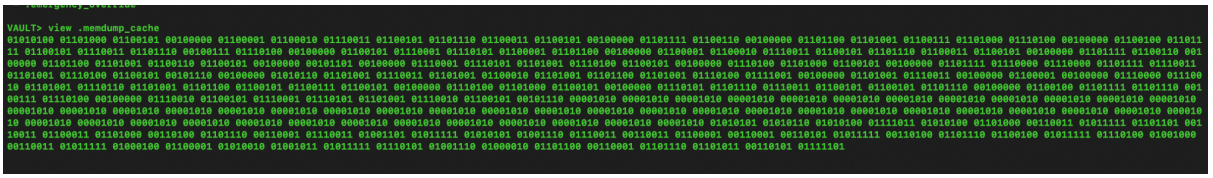
Just decrypt using online RSA decoder



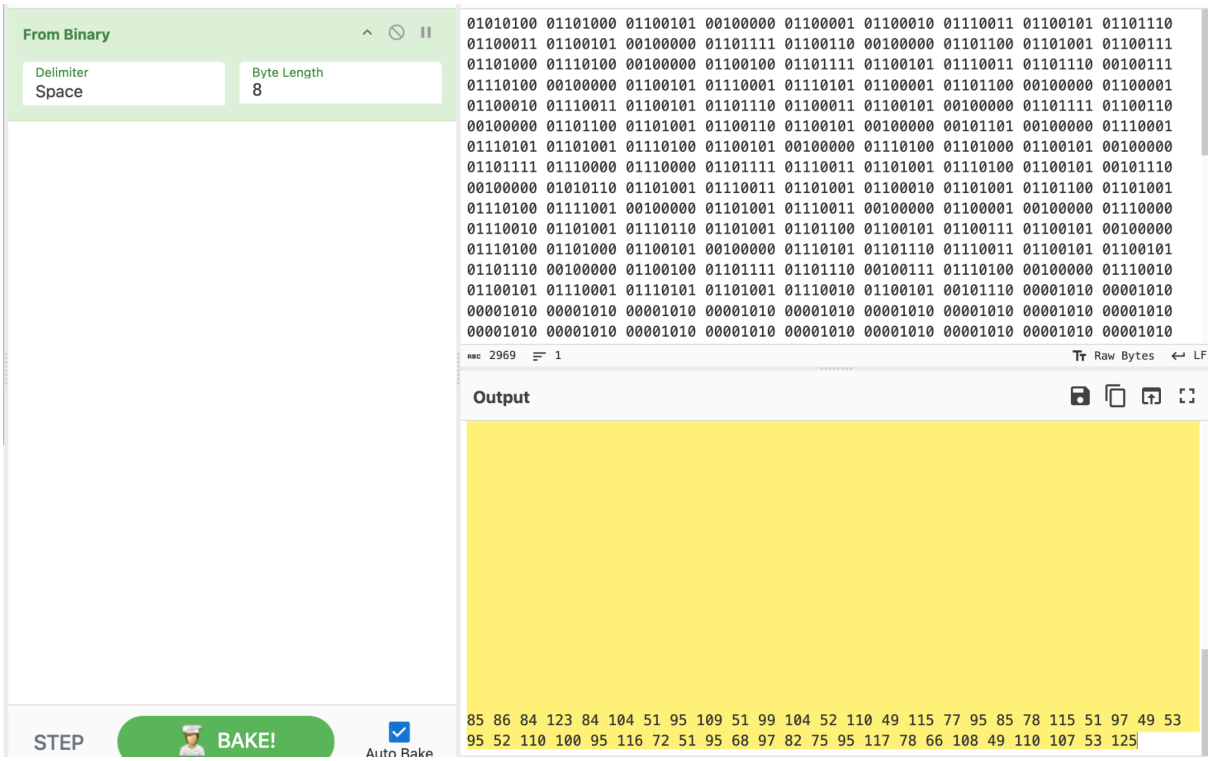
Now you log in as admin and view .memdumo_cache



In .memdumo_cache is the flag encrypted



Decode this from binary



Decode this from decimal and you have the flag