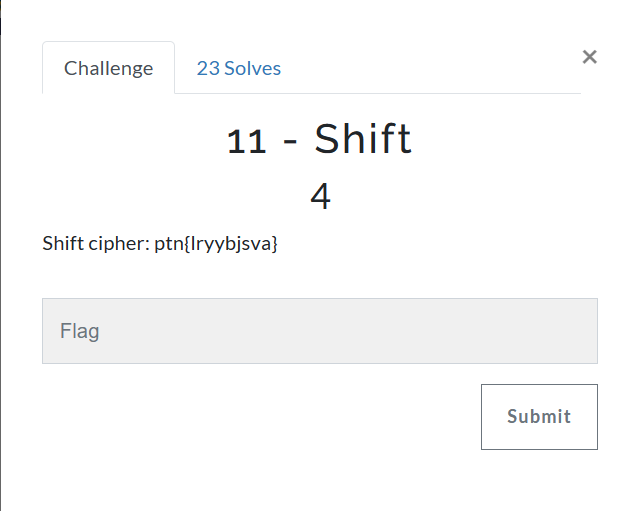
Hash + Ext Euclidean

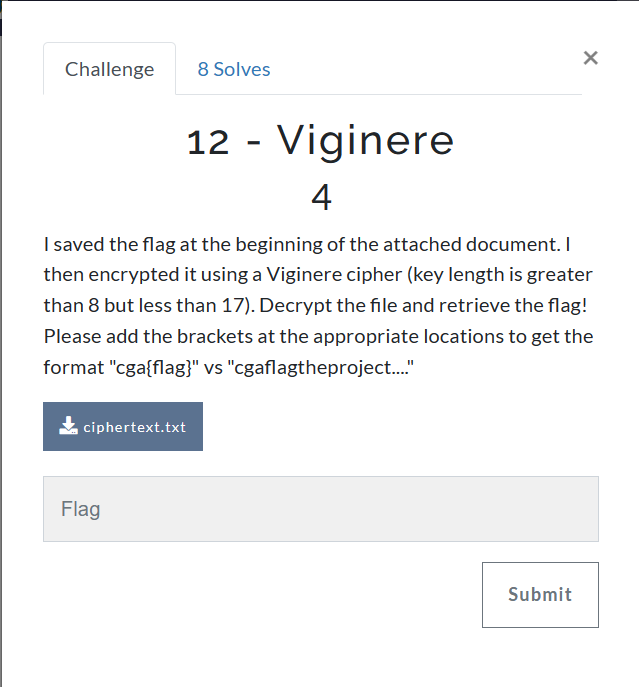


A close up of a note

Description automatically generated

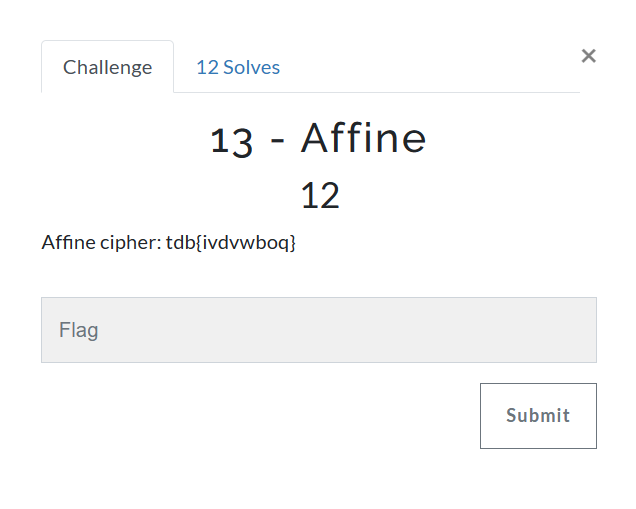


* Open shift cipher in python
* Replace message
* Look for cga in output

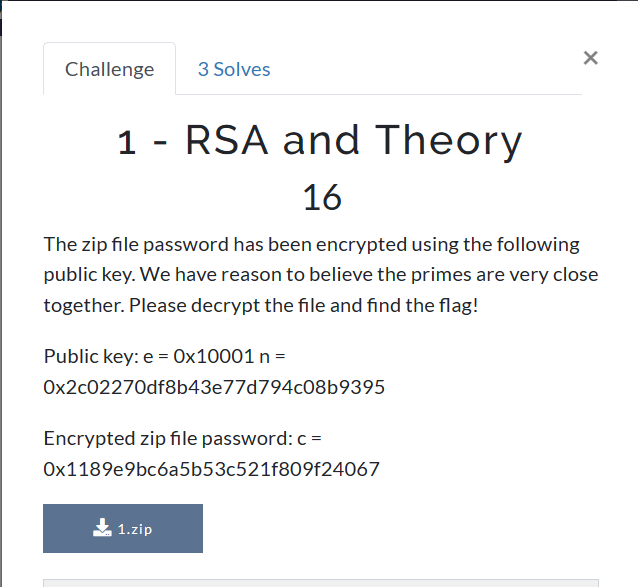


* Run pex2 with the ciphertext
* Run pex1 with all the output files

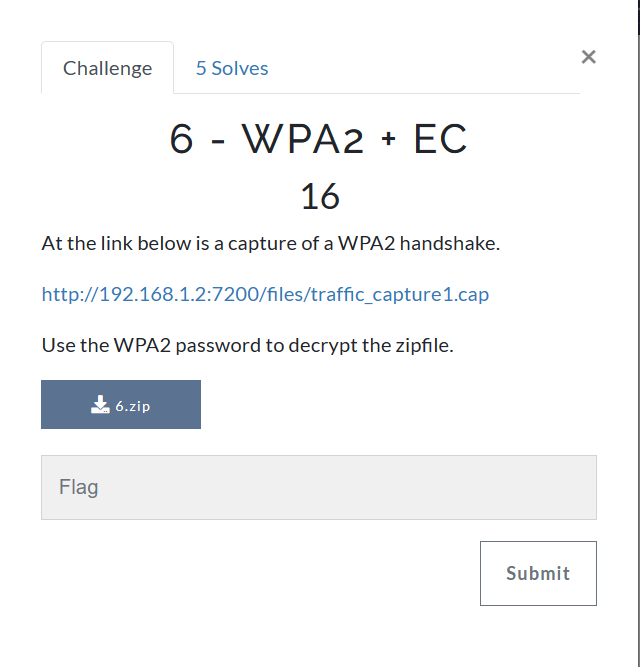
OR – run the vigenere code

Affine

* Put message into affine.py
* Change message
* Look for cga

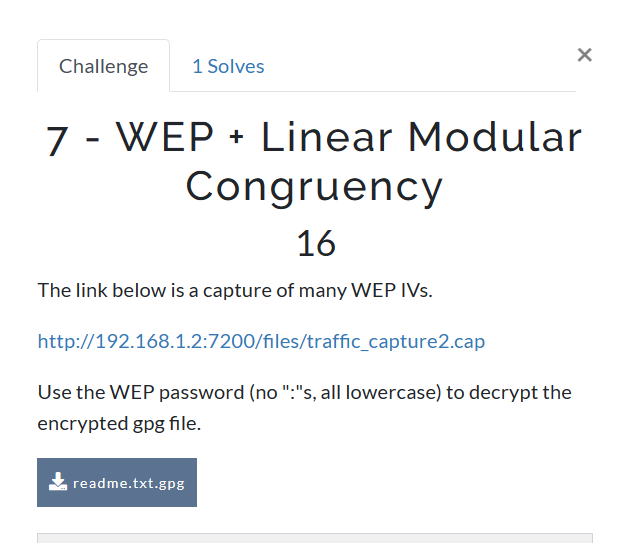


1. Download 1.zip
2. 7-Zip -> 7zFM -> select 1.zip from downloaded location
3. Run rsa1 python program with given e, n, c
4. Open zip file
5. Use ASCII string output as prompted pswd

WPA2 + EC

\*FOR WPA2 ALWAYS USE WIFI\_PASSWDS.TXT\*

* Open terminal in final prep folder type wsl
* Type aircrack-ng -w wifi\_passwds.txt traffic\_capture1.cap and get a key
* Type gpg -d readme.txt.gpg



* WEP + Linear Modular Congruency
* Aircrack-ng traffic\_capture2.cap
* Gpg -d readme.txt.gpg
* Use linear mod congruency pyhton script
* IF SOLVING FOR x EXAMPLE

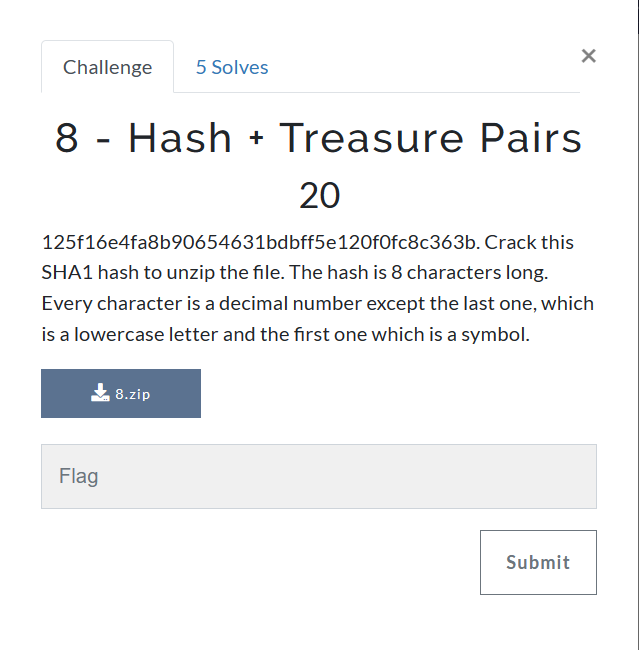
A paper with writing on it

Description automatically generated

Hash + extended Euclidean

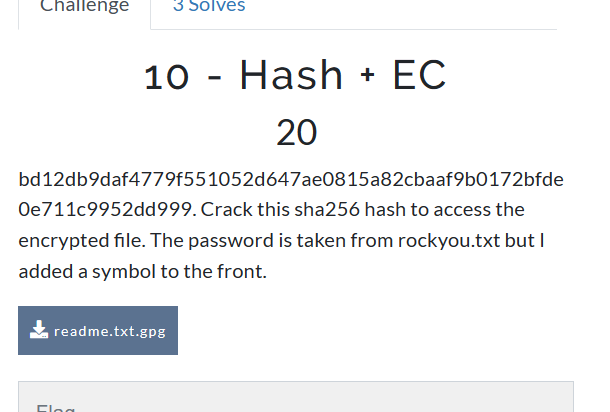
* MD5
* MD5 hash
* Hashcat -m 0 -a 1 \*HASH\* rockyou.txt question9.txt
* Go into wsl
* Gpg –import yeaton.key
* Gpg -d readme.txt.gpg

Hash + treasure pairs



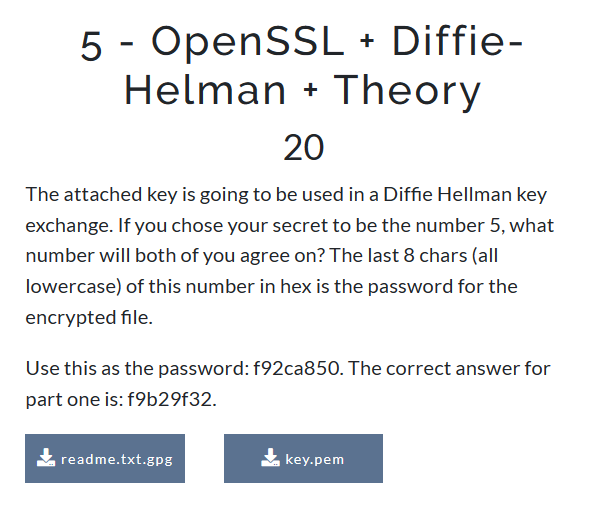
* Hashcat -m -100 -a 3 \*HASH\* ?s?d?d?d?d?d?d?l
  + Repeat and add –show once this command is done
  + M is the type of cipher and a is the attack
* Unzip file
* use the TreasurePairFinding code to solve

Hashcat + EC



* hashcat -m 1400 -a 7 \*HASH\* ?s rockyou.txt
* gpg -d readme.txt.gpg
* use ECDH to find key

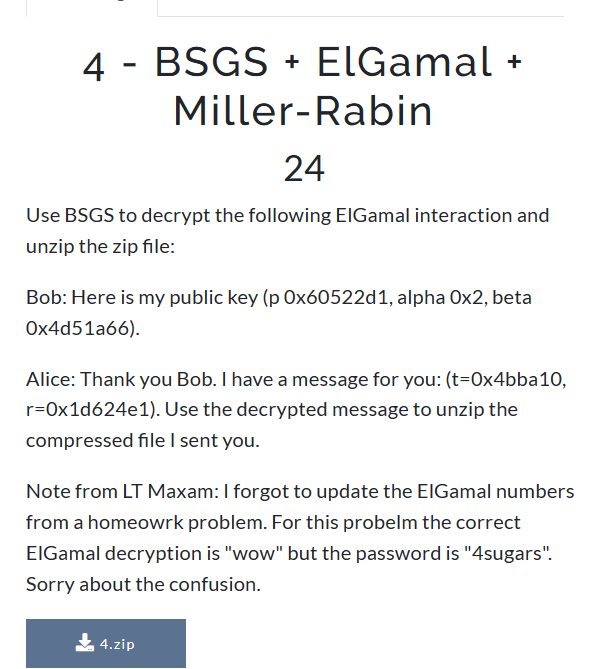
OpenSSL + DiffieHelman



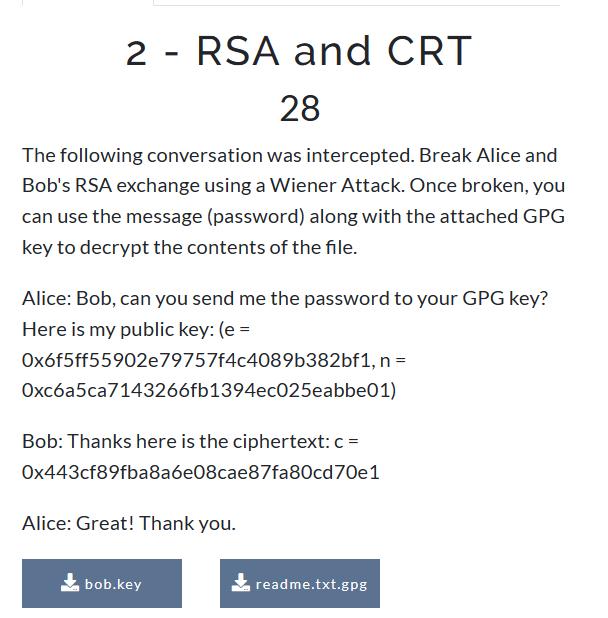
* Open terminal in final prep folder
* openssl pkey -in key.pem to get a private key
* copy private key in sublime and remove the colons and make it all one line
* paste into DH\_Theory
* take pw to unlock the file and this value will be k in the output



* openssl rsa -pubin -in rsa\_key.pem -text
* gpg -d readme.txt.gpg (will be prompted for passphrase)
* use opensslrsatheory.py, input n, e from terminal output and c from given problem
* multiply top two number by each other
* plug that number into dec2ascii, plug that number into prompted passphrase
* cga{OTP}



* open 7-zip file folder, 7zFM open 4zip (will be prompted for password) password is 4sugars
* brings up notepad gives # to test w miller rabin and witness
* use millerrabin.py
* flag is cga{6556, 3161, composite}
* OR  
  - BSGS elgamal python 🡪 input p,alpha, beta,t,r 🡪 use pw to unzip file 🡪 use miller rabbin code



* put e, n, c into littleweinerprogram.py
* open terminal type:
* wsl
* gpg - -import bob.key (will be prompted for password put in answer from program)
* gpg -d readme.txt.gpg
* open CRT code
* in moduli and remainders add the values