Shift

1) Open Shift Cipher Python
2) replace message
3) look for CGA in output

Vigenere

1) run pex2 with cipher text
2) run pex1 with output

ex: most frequent = r = 17 e = 4

r→e : 4→17 = 13 C
f→e : 4→5 = 1 G
i→e: 4→8 = 4 A
l→e: 4→11 = 7
u→e: 4→20 = 16
j→e: 4→9 = 5
m→e 4→12 = 8
z→e 4→25 = 21
x→e 4→23 = 19
g→e 4→6 = 2
e→e 4→4 = 0

Regular Affine

1) open affine.py
2) change message
3) run script

1) open bruteforce
2) run script
3) input message in w/ no spaces
4) look for CGA

RSA & theory

1) run RSAproblem1.py
2) open 7zip
3) open zip file
4) enter pw

WPA2

1) open cmd prompt & type wsl
2) cd into file
3) aircrack-ng -w wifi_passwds.txt traffic_capture1.cap
4) gpg -d readme.txt.gpg

WEP & Linear congruency

1) aircrack-ng traffic_capture2.cap
2) gpg -d readme.txt.gpg
3) ex problem given:

Solve for x. $264 \equiv 428 \pmod{364}$

1) take mod of 428 bc bigger than 364
   - ↳ $= 264 \equiv 64 \pmod{364}$
   - ↳ divide by 4 $\therefore 66 \equiv 16 \pmod{91}$
2) mod inverse in python
   - ↳ pow(66, -1, 91) = 40
3) $16 \cdot 40 \% 91 = 3$
4) for i in range(0,4):
   - print(3 + 91 · i)

$= 3, 94, 185, 276$

Hash + ext euclidean

1) MD5 hash
2) make sure hashcat is in the final folder
3) hashcat --help if you need it
4) hashcat -m 0 -a 1 *hash* rockyou.txt question9.txt
5) go into wsl
6) gpg --import yeation.key
7) gpg -d readme.txt.gpg

Hashcat & treasure pairs

hashcat -m 100 - a 3 value in ctf ?s?d?d?d?d?d?d?l

↳ add --show after its done

unzip file

use torins code

Hash + EC

1) hashcat -m 1400 -a 7 *hash* ?s rockyou.txt
2) gpg -d readme.txt.gpg
3) use ECDH to find key

RSA & CRT

1) put values in wiener attack
2) WSL
3) gpg --import boo.key
4) gpg -d readme.txt.gpg
5) open CRT code
6) in moduli & remainders add all the #s

Openssl + diffe helman + theory

1) openssl pkey -in key.pem
2) copy private key in sublime
   - remove : & spaces
3) paste into DH_theory
4) take prv to unlock file *k*

Assymetric Symetric

EL gamal

RSA

BSGS + el gamal + miller rabbin

1) BSGS el gamal python

2) input p, alpha, beta, t, r

3) use pw to unzip

4) use miller. rabbin code

openssl + rsa theory

1) openssl rsa -pubin -in rsa_key.pem -text

2) use openssl rsa

3) multiply the top 2 #s

4) plug that # into dec2 Ascii

5) run gpg -d readme.txt.gpg

- enter pw