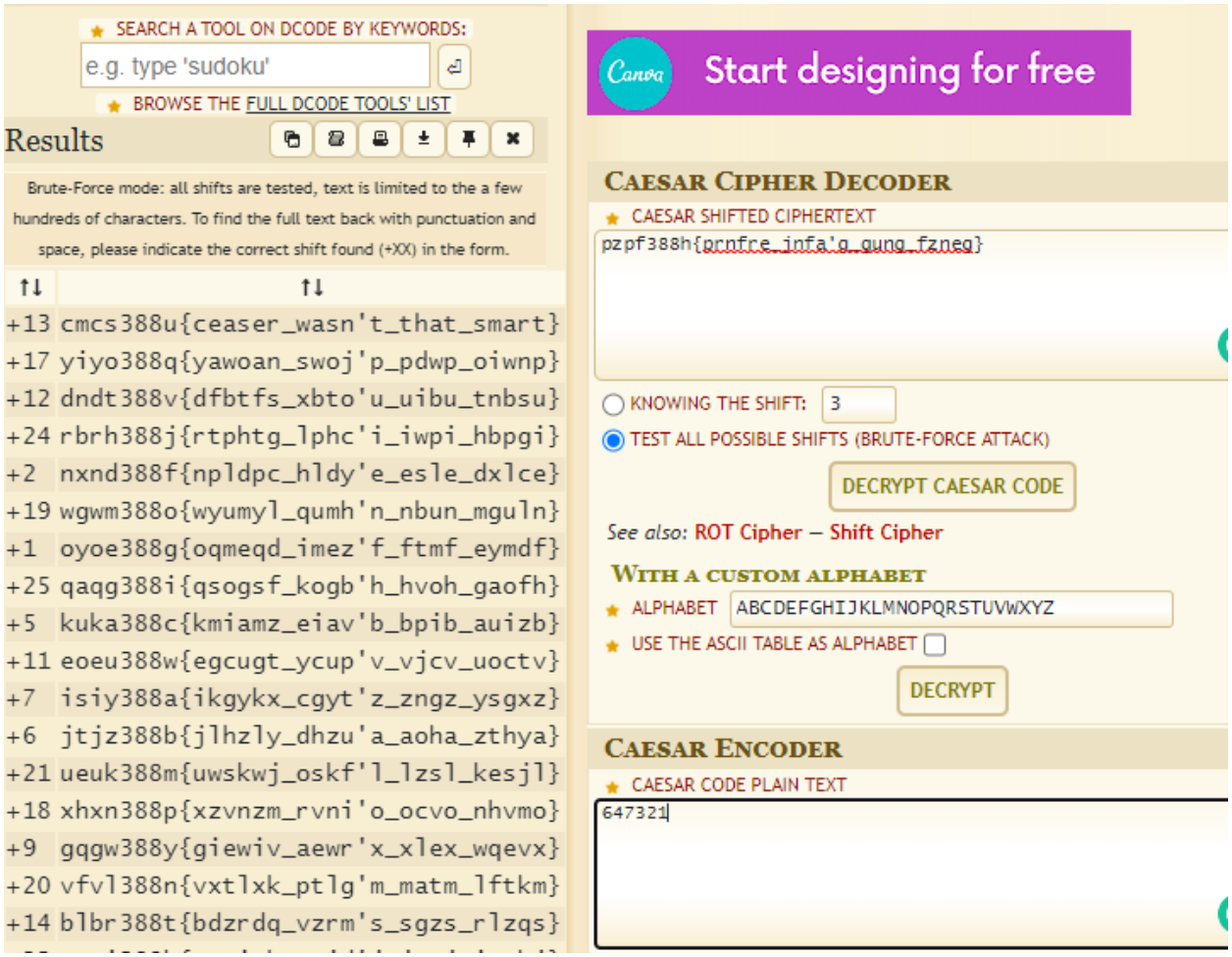
Homework #9 Crypto

Honor Pledge: I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

1. a. The text
   `Y21zYzM4OHV7ZW5jb2RpbmchPWVuY3J5cHRpb24tcmlnaHQ/fQ`
   Is in Base64 so using the command
   `echo "Y21zYzM4OHV7ZW5jb2RpbmchPWVuY3J5cHRpb24tcmlnaHQ/fQ" | base64 -d`
   We get

   The plaintext is thus:
   `cmsc388u{encoding!=encryption-right?}`

   b. The text
   `Pzpf388h{prnfre_jnfa'g_gung_fzneg}`
   Is in the format of CMSC388U{text}. Since the numbers aren't changed, this must be a simple shift or replacement encoding.
   I decided to try a caesar cipher first.Using https://www.dcode.fr/caesar-cipher



We get a shift of +13, and the plaintext is
`Cmcs388u{ceaser_wasn't_that_smart}`

2. Yes, the email thanos@sna.pp was compromised in the data breach. The hash associated with it is `c010b29fb22c2d79ce9402f72a4987f5`

First I decided to try and determine what type of hash it is. I ran `hashid 'c010b29fb22c2d79ce9402f72a4987f5'`

```
┌──(kali㉿kali)-[~]
└─$ hashid 'c010b29fb22c2d79ce9402f72a4987f5'
Analyzing 'c010b29fb22c2d79ce9402f72a4987f5'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Next, I loaded the hash into a text file called 'hash.txt'. Next, I decided to use MD5 as the encoding since it is commonly used. Next, I ran the commands

```
sudo unshadow rockyou.txt hash.txt > passwd
john --show passwd
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo unshadow rockyou.txt hash.txt > passwd

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show passwd
bobe89!:NO PASSWORD
:NO PASSWORD:::::
LLll:NO PASSWORD:;;
:NO PASSWORD:magick::
:NO PASSWORD::@@@~~~
[illegible] :NO PASSWORD
zincntido:NO PASSWORD
zAIYUMI:NO PASSWORD

182 password hashes cracked, 554 left
```

Then i typed

```
john  --wordlist=rockyou.txt --format=Raw-MD5 hash.txt
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john  --wordlist=rockyou.txt --format=Raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 50 password hashes with no different salts (Raw-MD5 [MD5 32/32])
Remaining 28 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
ordnance1        (nas123@sna.pp)
adik91           (kopink5@sna.pp)
vkikpdkovt       (ocean24712@sna.pp)
pablomanuel      (chloelowie@sna.pp)
OSITOPANDA       (conniecute@sna.pp)
d3ath            (023173624@sna.pp)
Jamaal1          (darylkrystel@sna.pp)
y.w@k@786        (linger3@sna.pp)
tori027          (32868254@sna.pp)
pass2630259      (mydangiu@sna.pp)
obeliks          (07080520@sna.pp)
marcshecanapish  (issac0812@sna.pp)
```

I then ran `john  --show --format=Raw-MD5 hash.txt` to see all of the cracked passwords in a readable format.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john  --show --format=Raw-MD5 hash.txt
0843089856@sna.pp:3655848
09265481511@sna.pp:lysabug17
camilaniky@sna.pp:330084
60985bucaneros15@sna.pp:canoramos
iloveang*@sna.pp:0851902709
va40ni@sna.pp:muephy
nayeliscarlett@sna.pp:5261192
PORelmundo8@sna.pp:mindy_
thanos@sna.pp:decieann07
raremen@sna.pp:boing08
lanikque@sna.pp:lufalufa
NOT4USE@sna.pp:marshii05
culobonito@sna.pp:ianosalina1991
Falcons!@sna.pp:smfintotihakeri
CIPHERUS@sna.pp:0826365647
doobie4@sna.pp:flaboi99
supercalypso@sna.pp:032406133
0815383375@sna.pp:sofimcevoy
sorryjose@sna.pp:ni1994
```

The plaintext password for thanos@sna.pp is `decieann07`