# Exercise

- Please write a program to:

1. determine the keyword length of these two encrypted messages using I.C.
2. Then solve the encryption keyword letters
3. Finally, break this ciphertext and recover the plaintext.

- You should hand in a README for the description of the program.
  - Use HackMD to write a README and provide a **readable** public URL in file url.txt

- Note: The programs will need to read the message from stdin and output the result followed by a newline to stdout. The answer should be saved in a text file named message1_out.txt and message2_out.txt

Reference https://macs4200.org/chapters/08/5/determining-keyword.html

# Encrypted message 1

- ZQQTK PQUWD PGMWD BQTXY LFQWL SHAJB UCIPV KUQEJ RBAAC LRSIZ ZCRWT LDFMT PGYXF ISOSE ASZXN PHTAY HHIIR ADDIJ LBFO
E VKUWW VFFLV TCEXG HFFXF ZVGXF BFQEI ZOSEZ UGFGF UJUGK PCZWZ UQQJI VAFLV CSDCX YOPYR SQTEI HQFII VTAYI LRGGR AWAR
N LAGWK JCZXZ UIMPC FTAVX LHMRU LAMRT PDMXV VIDWV SJQWW YCYOE VKXIU NSBVV CWAYJ SMMGH BWDIU DSYYJ AGQXR ZWP
IF SRZSK PCZWR URQQS YOOIW YSELF USEEE KOEAV SSMVE DSYYJ APQHR PZKYE SSMVE PBSWF TSFLZ UUILZ JVUXY HGOSJ AIERF ZAMP
C SONSL YOZHR ULUIK FHAET XIUVV HBPXY PGPMW MWOYC AMMXK HQTIJ PHEIC MAAVV JZAWV SMFSR UOSIZ UKTMT ODDSX YSEW
Y HGSEZ USPEJ AFARX HGOIE KSZGP VJQVG YSVYU PQQEE KWZAY PQTTV YGARJ HBPXY PBSWR YSPEP IMPEP MWZHZ UUFLV PFDIR SZQ
ZV SWZPZ LIAJK OSUVT VBHIE AWARR SJMPL LHTIJ HAQTI PBOMG SSEAY PQTLR CSEAV WHMAR FHDEU PHUSE HZMFL ZSEEE KKTMT O
ODID HYURX YOBMU OOHST HAARX AVQVV CSZYV ZCRWZ USOYI PGFWR UREXI PDBME NHTIK OWZXR DRDCM LWXJI VAMXK YOOXZ C
SEYG LFEXZ AWARJ HFQAF YYURX HGMGK PJQPP PBXMK LFMXL YSMWZ UGAGZ LHKXY LQDIU BZUXP VTARV DFUXV YCDXY LDMVK POX
MK FCREE VHTII MWZHJ HGBSN LFRYC HHAYT OGFSE LOZHR ZKTSC LGAQV HQTEJ AWEID LBFME AVQLV HZFLP ZQQTK PQUWD VTMXV
TDQVR ASOPR ZGAJR UHMKF UWEXJ HGFLV KFQED ZCRGF UGQVM HHUWD VFFLV PABSJ AIDIJ VTBPL YOXMJ AGURV JIDIJ PBFLV JVGVT
OVUWK VFKEE KHDEU PHUSE DVQXY LFAJR UQUIE ACDGF TDMVR AWHIC FFQGV UHFMD LGMVV ZINNV JHQHK VJQVP KWRJV YSZXY
HBPPZ UURVF THTEK DVUGY AVQME KIXKV UQQSI JFQHL SWFCF MTAVD LFMKV ZQAYC KOXPF DAQVV ZHMXV TSZXJ HFQNV HZAYJ SM
IEK JVQHR URFLV TCFMM LGAJK OSIVZ ASDJF YAMWZ TDAVK HBFEE PBSVV KWQRK PBFLV HBMPP ZWESW OWELZ ZHAVP HGFLV MOO
XJ OSDIT VFPWG YCNES PZUXP PGMTF DSDJL SOZHK YCGFC LGAQV ASEXR URUXZ ZPKXY PGFVF BPXIJ VAQWK HBPEI KHTEK HZMVX LD
AVK PCZSW OWEXF YWOEC LJUHV UQQMJ ZWRXV KQARJ PGFIE JMUWE VZQWJ WSDXZ UOOMF BGMRU LLMGK PBSME PHEHV TOZHJ
PBNVZ LTFSN YWFIR OWEXF YMIID BGFOE VKYSI LHTEE TSDIW HQFWY BAMRE HHGVV CWQAV KIZHV YOZME KIOXZ VBAJV EHQRU LRQ
BG LFUIE JSUWK OSNIJ AVQPG ACFLV JFUXZ JWEQF MVGQR UVUWK VFKLZ ZHAVZ JOXGY HFMGK LFEGR UCZPP ISQWK PAMXV KPKXY L
GFEE KODHN OWOLY BAMRV EDQVZ LBOIN OSFLV YOOXL HZAVK YOPMK PCZEI FVMWW BFZMJ OSPXF MCDQT VFDIT AJUIN ZCRME K
WHMU BOXWN LAGWK YSSEI KHTID HGRSI TWZKG HFFWF MOSVV HHILF SSIID BGFQV HGGVV AVQQS FHTIZ YFQPR AWARK VHTID HGE
SW ISURX ZPKAY VAFLV FODIJ BFDSL URQHR URURT VBFID WZMXZ UUFLV PBOMU LBFWZ UHTIZ YZUZV ZCDGF URUXZ VBILZ JVFVR KW
FMF UVMWY HBPIU KCIRK VIEAV TIEXI HHTII JCZWZ KSDXY LUQRV YOXFV HFURX VTFLV DVAPV UODVR AWHIK OOZXY LFQWG LQFMM
LDDSS HPUPZ AMAJZ AGPIK HWXW

# Encrypted message 2 **HINT key length could be 5 or 6**

- IVIKDKDQMJGLPWLZGMPFBJIIDBBYSLJDXFGBIWWEHAPHEYSGNCCYOOTSTZABCOBVRTAZEYWVWWAZAIDGAZ
  PETHPVBPWOBVJXGFMDOBCGPFKXKSZZAIGCJRPETACJHUTHPVHKJHPZHFPMEVZEQSBYOMHSDVFTASFGZTC
  OBZCGHFMDOBCWVNVBRVKRGXDBMKFBTGBVGMPTBVFMTGBLBMXZWESHGCBYSKDTBYSFWOARQHCJQEQBC
  UIDCNCHWWGNEDWIHPTKQCZGDKIGDENHPZGIGWVTWIASBFHATQIJSBCDWZBMPGQKKTHTQIGMEFMJSGISLK
  CFTHPVFXLSZVHAGSMGCLHWJCSXMDTRBTIWWEGHUHPVGXRZCJWHCCZZBVPFKVFTIWWECYIVQJUXCHTVAT
  CWVRBHJHPFILTCNYWLUOBYSKHAIEGBDBBYSKTKIJHATSFGZTCOBZCGIVIKVXLOAZBAXRQEUYDFITFBBSWIHA
  PHPVKTHAIUOGSHPRHMWSGNWLWSLKCTKCQUOGPGGCIFDFBYOMWSPRRLDAMUWLTOAVKAXQPTONHSLYWL
  HSOISZPHQFBBRCCCRMWWVBCYCCWKVXGOLVENPHMJCEJHQFBLIVMJSMWSVYOWICJVGBUHMUOGSPICOGR
  SLRUTXBAKSTRVWKVXG

# Bonus Exercise 1

1. Building an elementary MD5 hash cracker program via Python Programming to recover the two hash values.

   5f4dcc3b5aa765d61d8327deb882cf99

   5a105e8b9d40e1329780d62ea2265d8a

**Reference**

https://nicholasmordecai.co.uk/programming/creating-simple-python-md5-cracker/

https://s1.nordcdn.com/nord/misc/0.55.0/nordpass/200-most-common-passwords-en.pdf

# An asymmetric ciphers (RSA) Example

Choose **p = 3** and **q = 11** (secret)

Compute n = p * q = 3 * 11 = 33

Compute ϕ(n) = (p - 1) * (q - 1) = 2 * 10 = 20

Choose e such that 1 < e < ϕ(n) and e and n are coprime.

Let e = 7

**Compute a value for d such that (d * e) mod ϕ(n) = 1.**

One solution is **d = 3** [(3 * 7) mod 20 = 1]

Public key is (e, n) => (7, 33)

Private key is (d, n) => (3, 33)

The encryption of $m = 2$ is $c = \mathbf{2}^{7}$ mod $33 = 29$

**The decryption of $c = 29$ is $m = 29^{3}$ mod $33 =2$**

# Proof for the RSA Algorithm

- $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi(n)} \equiv M^1\ M^{k\phi(n)}$ (mod n)
- $\equiv M^1\ \mathbf{M^{\phi(n)}}\ {}^{k}$ (mod n)

- By Euler's theorem $M^{\phi(n)}$ (mod n)=1 ⇒
- ed≡1 (mod ϕ (n)) ed=1+kϕ(n)

- Another Example
- p=885320963, q=238855417,
- n=p · q=211463707796206571
- Let e=9007, ∴ d=116402471153538991
- M="cat"=30120, C=113535859035722866

# Bonus Exercise 2
# Perfect secrecy achieved with RSA?

Give your answer and reasons in README by creating a separated subdirectory apart from the program code explanation