CS458 - Spring 2022
Class Activity 1
Due in Blackboard on Sunday, February 6th (11:59pm)

Given the ciphertext:
met ge fyegakg dezyhajb ciq egmayh:

fyegakg zinckklicgaq bcpljd paprayh: Hepa faefja li dezy bcpljd iaaq ge keigliza ge gcxa hgafh ge fyegakg gmaphajnah byep kenlq, likjzqliv cideia ieg bzjjd nckklicgaq, likjzqliv kmljqyai ziqay gtajna dacyh tme kciieg ra nckklicgaq dag. faefja tlgm tacxaiaq lppzia hdhgaph ey ziqayjdliv paqlkcj keiqlgleih.

vag nckklicgaq: czgmeylsaq kenlq nckkliah kci majf fyegakg dez byep kenlq. dez hmezjq vag c kenlq nckklia ch heei ch dez kci. eika dez cya bzjjd nckklicgaq, dez pcd ra crja ge hgcyg qeliv hepa gmlivh gmcg dez mcq hgeffaq qeliv rakczha eb gma fciqaplk.

tacy c pchx: Lb dez cya ieg bzjjd nckklicgaq ciq cvaq gte ey ejqay, dez hmezjq tacy c pchx li liqeey fzrjlk fjckah.

cnelq kyetqh ciq feeyjd naigljcgaq hfckah: raliv li kyetqh jlxa li kjchhyeeph, yahgczycigh, rcyh, blgiahh kaigayh, ey penla gmacgayh fzgh dez cg mlvmay ylhx bey kenlq. cnelq liqeey hfckah gmcg qe ieg ebbay byahm cly byep gma ezgqeeyh ch pzkm ch fehhlrja. lb liqeeyh, ryliv li byahm cly rd efailiv tliqeth ciq qeeyh, lb fehhlrja.

tchm dezy mciqh ebgai tlgm hecf ciq tcgay bey cg jachg gtaigd hakeiqh ahfaklcjjd cbgay dez mcna raai li c fzrjlk fjcka, ey cbgay rjetliv dezy ieha, kezvmliv, ey hiaasliv.

kjaci ciq qlhlibakg: kjaci mlvm gezkm hzybckah qcljd. gmlh likjzqah gcrjah, qeeyxierh, jlvmg htlgkmah, kezigaygefh, mciqjah, qahxh, fmeiah, xadrecyqh, geljagh, bczkagh, ciq hlixh.

Vyacg oer vzdh.

- The method used for encrypting it was simple substitution.
- No letter is encrypted as itself.
  - For example, PWEC cannot be the ciphertext for when.
- Analyze this message using the form below

Cryptanalysis Form

1. • Most frequent English letters: **e t a o i n s**
   • Ciphertext frequencies

unused: Q X, they can be U or V

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	A	Y	O	P	T	S	N	L	C	I	H	V	J	M	D	B	Z	W	Q	X	G	K	R	U

The above analysis is read as the letter taken from the ciphertext and finding the letter in the decoder. Eg: 'MET' becomes 'HOW'

2. • 1-letter English words: **a i**
   • One letter word in ciphertext: A, I

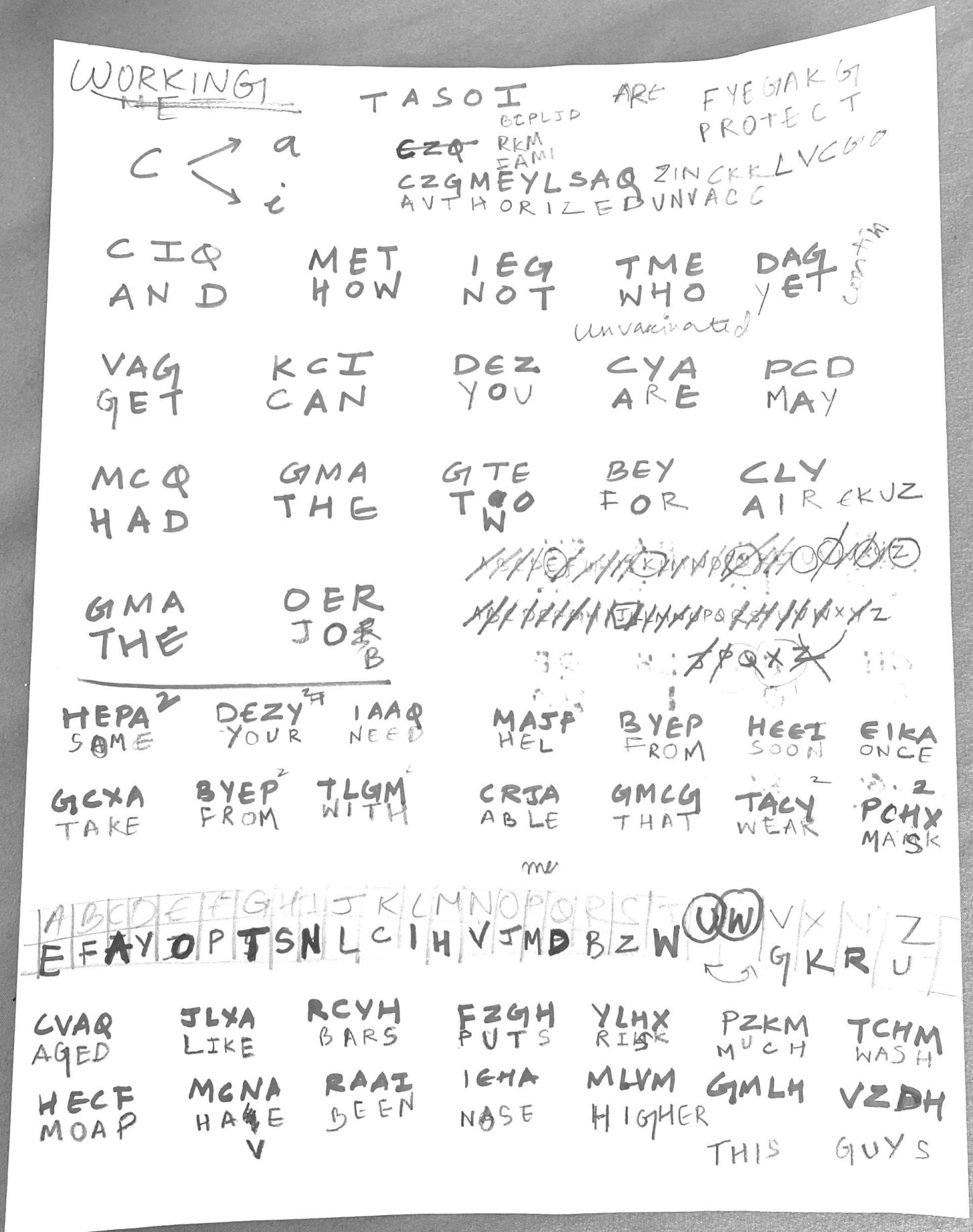
3. • Most frequently doubled letters in English: **s e t f l m o**
   • Double letters in ciphertext: C, E, L, N, M, P, O, S, F

→ Two-letter words in ciphertext:
TO, IN, BE, OR, AS, OF, IF, DO, AT, BY

→ THREE-letter words in ciphertext:
AND, HOW, NOT, WHO, YET, GET, CAN, YOU, ARE, MAY, HAD, THE, TWO,
FOR, AIR, THE, JOB

→ INITIAL letters in ciphertext:
A, H, N, W, Y, G, C, M, T, F, J, S, O, L, B, P, R, I, D, V

→ FINAL letters in ciphertext:
C, D, E, F, G, H, K, L, M, N, O, P, R, S, T, W, Y


WORKING
TASOI
ARE
FYEGIAKG
PROTECT
C
a
i
CIQ AND
MET HOW
IEG NOT
TME WHO
DAG YET
Unvaccinated
VAG GET
KCI CAN
DEZ YOU
CYA ARE
PCD MAY
MCQ HAD
GMA THE
GTE TWO
BEY FOR
CLY AIR
GMA THE
OER JOB
HEPA SOME
DEZY YOUR
IAAQ NEED
MAJF HEL
BYEP FROM
HEEI SOON
EIKA ONCE
GCXA TAKE
BYEP FROM
TLGM WITH
CRJA ABLE
GMCG THAT
TACY WEAR
PCHX MASK
me
E F A Y O P T S N L C I H V J M D B Z W U W V X N Z
G K R U
CVAQ AGED
JLXA LIKE
RCYH BARS
FZGH PUTS
YLHX RISK
PZKM MUCH
TCHM WASH
HECF MOAP
MCNA HAVE
RAAI BEEN
IEMA NOSE
MLVM HIGHER
GMLH
VZDH
THIS
GUYS