CHRISTOPHER MORCOM
A20385~~7~~64

CS458-01/02/03 - Fall 2018
Problem Set 1
Due in Blackboard on Wednesday, September 5 (11:59pm)

I would always assume that a math professor's very favorite dessert is pi.

Problem 1

Given the ciphertext:

get R=W, H=L   get X=U

I WOULD ALWAYS ASSUME THAT A MATH
D RNXHT VHRVCK VKKXOW FYVF V OVFY

→ Must be a school subject → get O=M, Y=H
→ T=D

GENBWKKNE'K PWEC BVPNEDFW TWKKWEF DK GD.
PROFESSOR S VERY FAVORITE DESSERT IS PI

must be a posessive → Professors
get C=Y
→ get P=V

- The method used for encrypting it was simple substitution.
- No letter is encrypted as itself.
  - For example, in this message we know that 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~~ ← Most freq cipher chars: ~~D~~FKN~~V~~WEF → freq most used vowel : E
   - Ciphertext frequencies

Plain		F	Y	I	R	T	P	L			S			O	M	V		W		D		A	E	U	H	
Cipher	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
freq	0	2	2	4	5	5	2	2	0	0	9	0	0	4	2	2	0	2	0	2	0	7	6	2	2	0

2. - 1-letter English words: a i
   - One letter word in ciphertext: D, V   D = A doesn't work..
3. - Most frequently doubled letters in English: s e t f l m o
   - Double letters in ciphertext: KK
4. - Most frequent 2-letter words in English: an, at, as, he, be, in, is, it, on, or, to, of, do, go, no, so, my
   - Two-letter words in ciphertext: DK, GD
5. - Most frequent 3-letter words in English: the, and, for, was, his, not, but, you, are, her
   - Three-letter words in ciphertext: N/A
6. - Most frequent initial letters in English: t a s o i
   - Initial letters in ciphertext: R, V, F, O, G, P, B, T, D, G
7. - Most frequent final letters in English: e s d n t
   - Final letters in ciphertext: T, K, W, F, Y, C, D
8. - Plaintext letters used: abcdefghijklmnopqrstuvwxyz

RH
↓
Unused letters:
~~B, C, G, J, K~~ L ~~N, Q~~ W ~~X, Z~~
↓
WOULD   NO VOWE
ALWAYS

Words that end in "I": ai, bi, di, gi, hi, ki, li, mi, oi, pi, si, ti, xi
I know none of the other ones...