Name: Kajol Tanesh Shah
A20496724

CS458 - Fall 2022
Class Activity 1
Due in Blackboard on Saturday, September 10$^{\text{th}}$ (11:59pm)

Given the ciphertext:

Qrm fpq hd jpvqvib lmwpmq xmllfbml, viqmkkvbvskm qh qrhlm jrh fpm vi ehllmllvhi hd qrm gma fit ziviqmkkvbvskm qh fkk hqrmpl, rfl smmi lqztvmt dhp wmiqzpvml. Qrm zlmdzkimll hd lzwr xmllfbml, mlemwvfkka vi qvxm hd jfp, vl hsuvhzl; hi qrm hqrmp rfit, qrmvp lhkzqvhi xfa sm f xfqqmp hd bpmfq vxehpqfiwm qh qrhlm dphx jrhx qrm gma vl whiwmfkmt. Szq qrm phxfiwm whiimwqmt jvqr qrm lzsymwq, qrm ihq ziwhxxhi tmlvpm qh tvlwhump f lmwpmq, fit qrm vxekvmt wrfkkmibm qh qrm vibmizvqa hd fkk dphx jrh vq vl rvttmi rfum fqqpfwqmt qh qrm lzsymwq qrm fqqmiqvhi hd xfia qh jrhx vql zqvkvqa vl f xfqqmp hd vitvddmpmiwm. Lmwpmq whtm vl "WL458 dfkk lmxmlqmp". Bhht yhs.

- The method used for encrypting it was simple substitution.

- No letter is encrypted as itself.

  - For example, PW**E**C cannot be the ciphertext for wh**e**n.

- Analyze this message using the form below

Cryptanalysis Form

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

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
7	9	0	15	4	29	2	46	32	7	21	39	75	0	0	24	59	28	9	16	3	39	21	17	3	14

2. - 1-letter English words: **a i**
   - One letter word in ciphertext: f

3. - Most frequently doubled letters in English: s e t f l m o
   - Double letters in ciphertext: d, h, i, k, l, m, q, t, x

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: hd, qh, vi, vl, hi, sm, vq

5. - Most frequent 3-letter words in English: **the, and, for, was, his, not, but, you, are, her**
   - Three-letter words in ciphertext: qrm, fpq, jrh, fpm, gma, fit, fkk, rfl, dhp, jfp, xfa, szq, ihq, vql, yhs

6. - Most frequent initial letters in English: **t a s o i**
   - Initial letters in ciphertext: q, f, h, j, l, x, v, e, g, z, r, s, d, w, m, b, p, t, y

7. • Most frequent final letters in English: **e s d n t**

   • Final letters in ciphertext: m, q, d, b, l, h, i, a, t, k, p, r, x, s

8. • Plaintext letters used: abcdefghijklmnopqrstuvwxyz

   Cipher:- FSWTMDBRVYGKXIHENPLQZUJCAO

9. Secret Code is:

   CS458 fall semester

10. Plaintext: The art of writing secret messages,
    intelligible to those who are in
    possession of the key and unintelligible
    to all others, has been studied for
    centuries. The usefulness of such
    messages, especially in time of war,
    is obvious; on the other hand,
    their solution may be a matter of
    great importance to those from
    whom the key is concealed. But
    the romance connected with the
    subject, the not uncommon desire
    to discover a secret, and the implied
    challenge to the ingenuity of all
    from who it is hidden have attracted
    to the subject the attention of many
    to whom its utility is a matter of
    indifference. Secret code is
    "CS458 fall semester". Good job.