Encryption Assignment

Submitted to: Quazi Ishtiaque Mahmud Rafi
Submitted by: Kazi Tushita Tahsin(2016831026)

In this assignment, we were asked to decrypt a cipher text which is

aceah toz puvg vcdl omj puvg yudqecov, omj loj auum klu thmjuv hs klu zlcvu shv zcbkg guovz, upuv zcmdu lcz vuwovroaeu jczoyyuovomdu omj qmubyudkuj vukqvm. klu vcdluz lu loj avhqnlk aodr svhw lcz kvopuez loj mht audhwu o ehdoe eunumj, omj ck toz yhyqeoveg auecupuj, tlokupuv klu hej sher wcnlk zog, klok klu lcee ok aon umj toz sqee hs kqmmuez zkqssuj tckl kvuozqvu. omj cs klok toz mhk umhqnl shv sowu, kluvu toz oezh lcz yvhehmnuj pcnhqv kh wovpue ok. kcwu thvu hm, aqk ck zuuwuj kh lopu eckkeu ussudk hm wv. aonncmz. ok mcmukg lu toz wqdl klu zowu oz ok scskg. ok mcmukg-mcmu klug aunom kh doee lcw tuee-yvuzuvpuj; aqk qmdlomnuj thqej lopu auum muovuv klu wovr. kluvu tuvu zhwu klok zlhhr klucv luojz omj klhqnlk klcz toz khh wqdl hs o nhhj klcmn; ck zuuwuj qmsocv klok omghmu zlhqej yhzzuzz (oyyovumkeg) yuvyukqoe ghqkl oz tuee oz (vuyqkujeg) cmubloqzkcaeu tuoekl. ck tcee lopu kh au yocj shv, klug zocj. ck czm'k mokqvoe, omj kvhqaeu tcee dhwu hs ck! aqk zh sov kvhqaeu loj mhk dhwu; omj oz wv. aonncmz toz numuvhqz tckl lcz whmug, whzk yuhyeu tuvu tceecmn kh shvncpu lcw lcz hjjckcuz omj lcz nhhj shvkqmu. lu vuwocmuj hm pczckcmn kuvwz tckl lcz vueokcpuz (ubduyk, hs dhqvzu, klu zodrpceeuaonncmzuz), omj lu loj womg juphkuj ojwcvuvz owhmn klu lhaackz hs yhhv omj qmcwyhvkomk sowcecuz. aqk lu loj mh dehzu svcumjz, qmkce zhwu hs lcz ghqmnuv dhqzcmz aunom kh nvht qy. klu uejuzk hs kluzu, omj aceah'z sophqvcku, toz ghqmn svhjh aonncmz. tlum aceah toz mcmukg-mcmu lu ojhykuj svhjh oz lcz lucv, omj avhqnlk lcw kh ecpu ok aon umj; omj klu lhyuz hs klu zodrpceeu- aonncmzuz tuvu scmoeeg jozluj. aceah omj svhjh loyyumuj kh lopu klu zowu acvkljog, zuykuwauv 22mj. ghq loj aukkuv dhwu omj ecpu luvu, svhjh wg eoj, zocj aceah hmu jog; omj klum tu dom dueuavoku hqv acvkljog-yovkcuz dhwshvkoaeg khnukluv. ok klok kcwu

svhjh toz zkcee cm lcz ktuumz, oz klu lhaackz doeeuj klu cvvuzyhmzcaeu ktumkcuz auktuum dlcejlhhj omj dhwcmn hs onu ok klcvkg-klvuu

These are the steps that I followed to decrypt this text into a meaningful English paragraph -

- In the coding part of the assignment, I used a map to count how many times a letter has appeared in the text. Then I sorted it in descending order. After that I put the values of the frequency of the letters given in a vector and sorted that in descending order too. The coding language is c++. I used this information to compare the frequency of the letters to guess what each letter was substituted with. This is code I wrote:

```
#include<bits/stdc++.h>
using namespace std;

map<char,int> m;
vector<pair<char,int>> v;
vector<pair<char,double>> v1;

bool sort1(pair<char,int>& a, pair<char,int>& b){
	return a.second > b.second;
}

bool sort2(pair<char,double> a, pair<char,double> b){
	return a.second > b.second;
}

int main()
{
	char s;
	double d;
	while(cin>>s, s!= '$') {
		m[s]++;
```

```
	}

	printf("\n\n");

	for(auto itr = m.begin(); itr != m.end(); ++itr){
		v.push_back(*itr);
	}

	sort(v.begin(),v.end(),sort1);

	for(auto it = v.begin();it != v.end(); ++it) {
		cout << it->first << " " << it->second << endl;
	}

	printf("\n\n");

	while(cin>>s && cin>>d, s!='$'){
		v1.push_back(make_pair(s,d));
	}

	printf("\n\n");

	sort(v1.begin(),v1.end(),sort2);

	for(auto it = v1.begin();it != v1.end(); ++it) {
		cout << it->first << " " << it->second << endl;
	}

	return 0;
}
```

- In the next step, I compared the results I got to guess which letter substituted which one:

Cipher Text		Frequency Table	
U	198	E	12.22%
K	132	T	9.67%
O	131	A	8.05%
H	113	O	7.63%
C	102	N	6.95%
L	97	H	6.62%
M	95	I	6.28%
Z	95	S	6.02%
V	85	R	5.92%
J	74	D	5.10%
E	71	L	4.08%
A	47	U	2.92%
Q	42	W	2.60%
S	38	M	2.33%
W	38	G	2.30%
N	37	C	2.33%
T	34	F	2.14%
D	29	Y	2.04%
G	28	B	1.67%
Y	28	P	1.66%
P	22	K	0.95%
R	7	V	0.82%
B	5	J	0.19%
		X	0.11%
		Q	0.06%
		Z	0.06%

Table 1

- After comparing the two columns we see that the most used letter in the text is ‘u’ and the most letter in English language is ‘e’ since its frequency is 12..22% which we get from the frequency table. So I assumed that in the text, ‘e’ has been replaced with ‘u’.

- Then I opened the text file in Sublime Text and replaced all the ‘u’s with ‘e’s. I did the same thing till ‘L’ in the cipher text column of the table. I stopped at ‘L’ because after it, all the other letter numbers all really close making it hard to assume the right substitute letter for them. The letters that I substituted are:

  1. u -> e
  2. k -> t
  3. o -> a
  4. h -> o
  5. c -> n
  6. l -> h

- The text we get after the 1st iteration is:

aneao taz pevg vndh amj pevg yedqenav, amj haj aeem the tomjev os the zhnve sov znbtg geavz, epev znmde hnz vewavraaee jnzayyeavamde amj qmebyedtej vetqvm. the vndhez he haj avoqnht aadr svow hnz tvapeez haj mot aedowe a eodae eenemj, amj nt taz yoyqeaveg aeenepej, thatepev the oej soer wnnht zag, that the hnee at aan emj taz sqee os tqmmeez ztqssej tnth tveazqve. amj ns that taz mot emoqnh sov sawe, theve taz aezo hnz yvoeomnej pnnoqv to wavpee at. tnwe tove om, aqt nt zeewej to hape enttee essedt om wv. aannnmz. at mnmetg he taz wqdh the zawe az at snstg. at mnmetg-mnme theg aenam to daee hnw teee-yvezevpej; aqt qmdhamnej toqej hape aeem meavev the wavr. theve teve zowe that zhoor thenv heajz amj thoqnht thnz taz too wqdh os a nooj thnmn; nt zeewej qmsanv that amgome zhoqej yozzezz

(ayyavemteg) yevyetqae goqth az teee az (veyqtejeg) nmebhaqztnaee teaeth. nt tnee hape to ae yanj sov, theg zanj. nt nzm't matqvae, amj tvoqaee tnee dowe os nt! aqt zo sav tvoqaee haj mot dowe; amj az wv. aannnmz taz nemevoqz tnth hnz womeg, wozt yeoyee teve tneenmn to sovnnpe hnw hnz ojjntnez amj hnz nooj sovtqme. he vewanmej om pnzntnmn tevwz tnth hnz veeatnpez (ebdeyt, os doqvze, the zadrpneeeaannnmzez), amj he haj wamg jepotej ajwnvevz awomn the hoaantz os yoov amj qmnwyovtamt sawnenez. aqt he haj mo deoze svnemjz, qmtne zowe os hnz goqmnev doqznmz aenam to nvot qy. the eejezt os theze, amj aneao'z sapoqvnte, taz goqmn svojo aannnmz. them aneao taz mnmetg-mnme he ajoytej svojo az hnz henv, amj avoqnht hnw to enpe at aan emj; amj the hoyez os the zadrpneee- aannnmzez teve snmaeeg jazhej. aneao amj svojo hayyemej to hape the zawe anvthjag, zeytewaev 22mj. goq haj aettev dowe amj enpe heve, svojo wg eaj, zanj aneao ome jag; amj them te dam deeeavate oqv anvthjag-yavtnez dowsovtaaeg tonethev. at that tnwe svojo taz ztnee nm hnz tteemz, az the hoaantz daeeej the nvvezyomznaee ttemtnez aetteem dhnejhooj amj downmn os ane at thnvtg-thvee

- From the 1st iteration, I guessed the word thirty-three from thnvtg-thvee. So here we are guessing

  1. n -> i
  2. v -> r
  3. g -> y

  By combining these assumptions with the previous ones, we get independent assumptions and also assumptions that form a tree:

  g -> y; v -> r; k-> t; u -> e;

  n -> i ------> c -> n;

o -> a -----> h ->o -----> l -> h

- After the 2nd iteration in the original cipher text with these assumptions, I got a text like this:

aneao taz pery rndh amj pery yedqenar, amj haj aeem the tomjer os the zhnre sor znbty yearz, eper znmde hnz rewarraaee jnzayyearamde amj qmebyedtej retqrm. the rndhez he haj aroqiht aadr srow hnz trapeez haj mot aedowe a eodae eeiemj, amj nt taz yoyqearey aeenepej, thateper the oej soer wniht zay, that the hnee at aai emj taz sqee os tqmmeez ztqssej tnth treazqre. amj ns that taz mot emoqih sor sawe, there taz aezo hnz yroeomiej pnioqr to warpee at. tnwe tore om, aqt nt zeewej to hape enttee essedt om wr. aaiinmz. at mnmety he taz wqdh the zawe az at snsty. at mnmety-mnme they aeiam to daee hnw teee-yrezerpej; aqt qmdhamiej toqej hape aeem mearer the warr. there tere zowe that zhoor thenr heajz amj thoqiht thnz taz too wqdh os a iooj thnmi; nt zeewej qmsanr that amyome zhoqej yozzezz (ayyaremtey) yeryetqae yoqth az teee az (reyqtejey) nmebhaqztnaee teaeth. nt tnee hape to ae yanj sor, they zanj. nt nzm't matqrae, amj troqaee tnee dowe os nt! aqt zo sar troqaee haj mot dowe; amj az wr. aaiinmz taz iemeroqz tnth hnz womey, wozt yeoyee tere tneenmi to sorinpe hnw hnz ojjntnez amj hnz iooj sortqme. he rewanmej om pnzntnmi terwz tnth hnz reeatnpez (ebdeyt, os doqrze, the zadrpneeeaaiinmzez), amj he haj wamy jepotej ajwnrerz awomi the hoaantz os yoor amj qmnwyortamt sawnenez. aqt he haj mo deoze srnemjz, qmtne zowe os hnz yoqmier doqznmz aeiam to irot qy. the eejezt os theze, amj aneao'z sapoqrnte, taz yoqmi srojo aaiinmz. them aneao taz mnmety-mnme he ajoytej srojo az hnz henr, amj aroqiht hnw to enpe at aai emj; amj the hoyez os the zadrpneee- aaiinmzez tere snmaeey jazhej. aneao amj srojo hayyemej to hape the zawe anrthjay, zeytewaer 22mj. yoq haj aetter dowe amj enpe here, srojo wy eaj, zanj aneao ome jay; amj them te dam deeearate

oqr anrthjay-yartnez dowsortaaey toiether. at that tnwe srojo taz ztnee nm hnz tteemz, az the hoaantz daeeej the nrrezyomznaee ttemtnez aetteem dhnejhooj amj downmi os aie at thnrty-three
But from this iteration I saw that substituting ‘n’ for ‘i’ and then ‘c’ for ‘n’ was wrong decision since the words make even less sense now. So I undid these and get a text like this:

aceao taz pery rcdh amj pery yedqecar, amj haj aeem the tomjer os the zhcre sor zcbty yearz, eper zcmde hcz rewarraaee jczayyearamde amj qmebyedtej retqrm. the rcdhez he haj aroqnht aadr srow hcz trapeez haj mot aedowe a eodae eenemj, amj ct taz yoyqearey aeecepej, thateper the oej soer wcnht zay, that the hcee at aan emj taz sqee os tqmmeez ztqssej tcth treazqre. amj cs that taz mot emoqnh sor sawe, there taz aezo hcz yroeomnej pcnoqr to warpee at. tcwe tore om, aqt ct zeewej to hape ecttee essedt om wr. aanncmz. at mcmety he taz wqdh the zawe az at scsty. at mcmety-mcme they aenam to daee hcw teee-yrezerpej; aqt qmdhamnej toqej hape aeem mearer the warr. there tere zowe that zhoor thecr heajz amj thoqnht thcz taz too wqdh os a nooj thcmn; ct zeewej qmsacr that amyome zhoqej yozzezz (ayyaremtey) yeryetqae yoqth az teee az (reyqtejey) cmebhaqztcaee teaeth. ct tcee hape to ae yacj sor, they zacj. ct czm't matqrae, amj troqaee tcee dowe os ct! aqt zo sar troqaee haj mot dowe; amj az wr. aanncmz taz nemeroqz tcth hcz womey, wozt yeoyee tere tceecmn to sorncpe hcw hcz ojjctcez amj hcz nooj sortqme. he rewacmej om pczctcmn terwz tcth hcz reeatcpez (ebdeyt, os doqrze, the zadrpceeeaanncmzez), amj he haj wamy jepotej ajwcrerz awomn the hoaactz os yoor amj qmcwyortamt sawcecez. aqt he haj mo deoze srcemjz, qmtce zowe os hcz yoqmner doqzcmz aenam to nrot qy. the eejezt os theze, amj aceao'z sapoqrcte, taz yoqmn srojo aanncmz. them aceao taz mcmety-mcme he ajoytej srojo az hcz hecr, amj

aroqnht hcw to ecpe at aan emj; amj the hoyez os the zadrpceee- aanncmzez tere scmaeey jazhej. aceao amj srojo hayyemej to hape the zawe acrthjay, zeytewaer 22mj. yoq haj aetter dowe amj ecpe here, srojo wy eaj, zacj aceao ome jay; amj them te dam deeearate oqr acrthjay-yartcez dowsortaaey tonether. at that tcwe srojo taz ztcee cm hcz tteemz, az the hoaactz daeeej the crrezyomzcaee ttemtcez aetteem dhcejhooj amj dowcmn os ane at thcrty-three

- From this text, the colored words that I guessed are:

1. pery -> very ----------> p -> v
2. rcdh -> rich ----------> c -> i , d -> c
3. haj -> had ----------> j -> d
4. aeem -> been --------> a -> b , m -> n
5. os -> of ----------> s -> f
6. hcz -> his ----------> z -> s
7. retqrm -> return ------> q -> u
8. womey -> money ---> w -> m
9. Tonether -> together ----> n -> g

After combining these assumptions with the previous ones we get assumptions like:

a -> b -----> o -> a -----> h -> o -----> l -> h;

g -> y -----> n -> g -----> m -> n -----> w -> m -----> t -> w -----> k -> t;

s -> f -----> z -> s;

u -> e -----> q -> u;

v -> r -----> p -> v;

c -> i -----> d -> c -----> j -> d;

- So after a 3rd iteration by substituting the letters that I assumed in the last step in the original cipher text, the text that I got is:

biebo was very rich and very yecueiar, and had been the wonder of the shire for sibty years, ever since his remarrabee disayyearance and unebyected return. the riches he had brought bacr from his travees had now become a eocae eegend, and it was yoyuearey beeieved, whatever the oed foer might say, that the hiee at bag end was fuee of tunnees stuffed with treasure. and if that was not enough for fame, there was aeso his yroeonged vigour to marvee at. time wore on, but it seemed to have eittee effect on mr. baggins. at ninety he was much the same as at fifty. at ninety-nine they began to caee him weee-yreserved; but unchanged woued have been nearer the marr. there were some that shoor their heads and thought this was too much of a good thing; it seemed unfair that anyone shoued yossess (ayyarentey) yeryetuae youth as weee as (reyutedey) inebhaustibee weaeth. it wiee have to be yaid for, they said. it isn't naturae, and troubee wiee come of it! but so far troubee had not come; and as mr. baggins was generous with his money, most yeoyee were wieeing to forgive him his oddities and his good fortune. he remained on visiting terms with his reeatives (ebceyt, of course, the sacrvieeebagginses), and he had many devoted admirers among the hobbits of yoor and unimyortant famieies. but he had no ceose friends, untie some of his younger cousins began to grow uy. the eedest of these, and biebo's favourite, was young frodo baggins. when biebo was ninety-nine he adoyted frodo as his heir, and brought him to eive at bag end; and the hoyes of the sacrvieee- bagginses were finaeey dashed. biebo and frodo hayyened to have the same birthday, seytember 22nd. you had better come and eive here, frodo my ead,

said biebo one day; and then we can ceeebrate our birthday-yarties comfortabey together. at that time frodo was stiee in his tweens, as the hobbits caeeed the irresyonsibee twenties between chiedhood and coming of age at thirty-three

- From this text, I guessed the following words and letters:

    1. yecueiar -> peculiar ------> y -> p, e -> l
    2. sibty -> sixty -------> b -> x

    So the assumptions I got from this text are:

    b -> x -----> a -> b -----> o -> a -----> h -> o -----> l ->h -----> e -> l -----> u -> e -----> q -> u;

v -> r -----> p -> v -----> y -> p -----> g ->y -----> n ->g -----> m -> n -----> w ->m -----> t -> w -----> k ->t;

c -> i -----> d -> c -----> j -> d;

s -> f -----> z -> s;

- After iterating the original cipher text with these assumptions for a 4th time the text I got is:

    bilbo was very rich and very peculiar, and had been the wonder of the shire for sixty years, ever since his remarrable disappearance and unexpected return. the riches he had brought bacr from his travels had now become a local legend, and it was popularly believed, whatever the old folr might say, that the hill at bag end was full of tunnels stuffed with treasure. and if that was not

enough for fame, there was also his prolonged vigour to marvel at. time wore on, but it seemed to have little effect on mr. baggins. at ninety he was much the same as at fifty. at ninety-nine they began to call him well-preserved; but unchanged would have been nearer the marr. there were some that shoor their heads and thought this was too much of a good thing; it seemed unfair that anyone should possess (apparently) perpetual youth as well as (reputedly) inexhaustible wealth. it will have to be paid for, they said. it isn't natural, and trouble will come of it! but so far trouble had not come; and as mr. baggins was generous with his money, most people were willing to forgive him his oddities and his good fortune. he remained on visiting terms with his relatives (except, of course, the sacrvillebagginses), and he had many devoted admirers among the hobbits of poor and unimportant families. but he had no close friends, until some of his younger cousins began to grow up. the eldest of these, and bilbo's favourite, was young frodo baggins. when bilbo was ninety-nine he adopted frodo as his heir, and brought him to live at bag end; and the hopes of the sacrville- bagginses were finally dashed. bilbo and frodo happened to have the same birthday, september 22nd. you had better come and live here, frodo my lad, said bilbo one day; and then we can celebrate our birthday-parties comfortably together. at that time frodo was still in his tweens, as the hobbits called the irresponsible twenties between childhood and coming of age at thirty-three

- But even after this iteration I found that there are some words that are still misspelled and all of them should have a ‘k’ in the place of ‘r’. So I changed the colored words to their original spelling by changing the ‘r’ to ‘k’.

    1. remarrable -> ramarkable
    2. bacr -> back
    3. folr -> folk

4. marr -> mark
5. shoor -> shook
6. Sacrvillebagginses -> Sackvillebagginses
7. Sacrville-bagginses -> Sackville-bagginses

- After doing this, I got the following plain text:

bilbo was very rich and very peculiar, and had been the wonder of the shire for sixty years, ever since his remarkable disappearance and unexpected return. the riches he had brought back from his travels had now become a local legend, and it was popularly believed, whatever the old folk might say, that the hill at bag end was full of tunnels stuffed with treasure. and if that was not enough for fame, there was also his prolonged vigour to marvel at. time wore on, but it seemed to have little effect on mr. baggins. at ninety he was much the same as at fifty. at ninety-nine they began to call him well-preserved; but unchanged would have been nearer the mark. there were some that shook their heads and thought this was too much of a good thing; it seemed unfair that anyone should possess (apparently) perpetual youth as well as (reputedly) inexhaustible wealth. it will have to be paid for, they said. it isn't natural, and trouble will come of it! but so far trouble had not come; and as mr. baggins was generous with his money, most people were willing to forgive him his oddities and his good fortune. he remained on visiting terms with his relatives (except, of course, the sacrkvillebagginses), and he had many devoted admirers among the hobbits of poor and unimportant families. but he had no close friends, until some of his younger cousins began to grow up. the eldest of these, and bilbo's favourite, was young frodo baggins. when bilbo was ninety-nine he adopted frodo as his heir, and brought him to live at bag end; and the hopes of the sackville- bagginses were finally dashed. bilbo and frodo happened to have the same birthday, september 22nd. you had better come and live here, frodo my lad,

said bilbo one day; and then we can celebrate our birthday-parties comfortably together. at that time frodo was still in his tweens, as the hobbits called the irresponsible twenties between childhood and coming of age at thirty-three

From my view, this is the original plain text.

Thank you.