Network Security Lab1

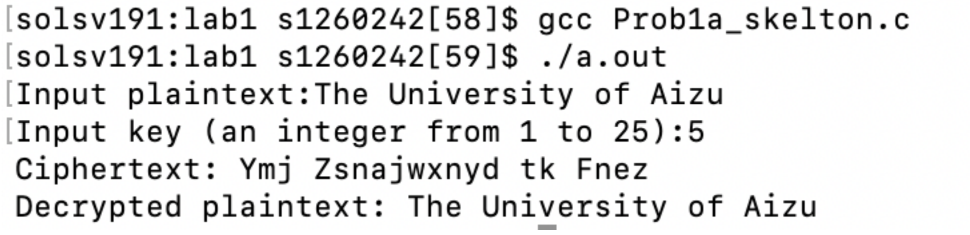
S1260242

Ryusei Takahashi

Problem1

a)

(1)



```
[solsv191:lab1 s1260242[58]$ gcc Prob1a_skelton.c
[solsv191:lab1 s1260242[59]$ ./a.out
[Input plaintext:The University of Aizu
[Input key (an integer from 1 to 25):5
 Ciphertext: Ymj Zsnajwxnyd tk Fnez
 Decrypted plaintext: The University of Aizu
```

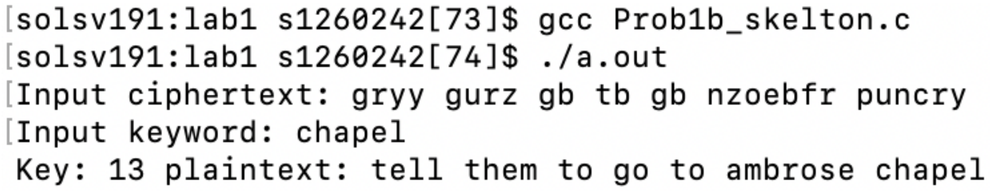
Input “The University of Aizu” as a plaintext and key=5.

the codes are included in C files

b)

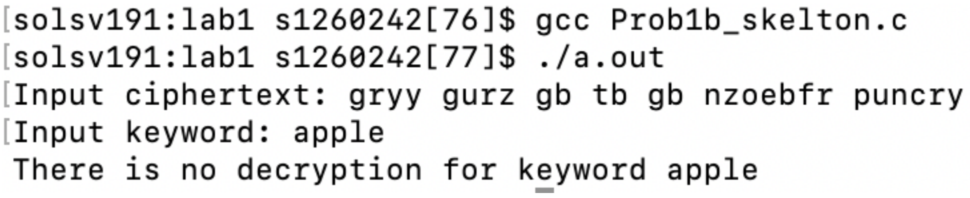
(1)

With keyword:



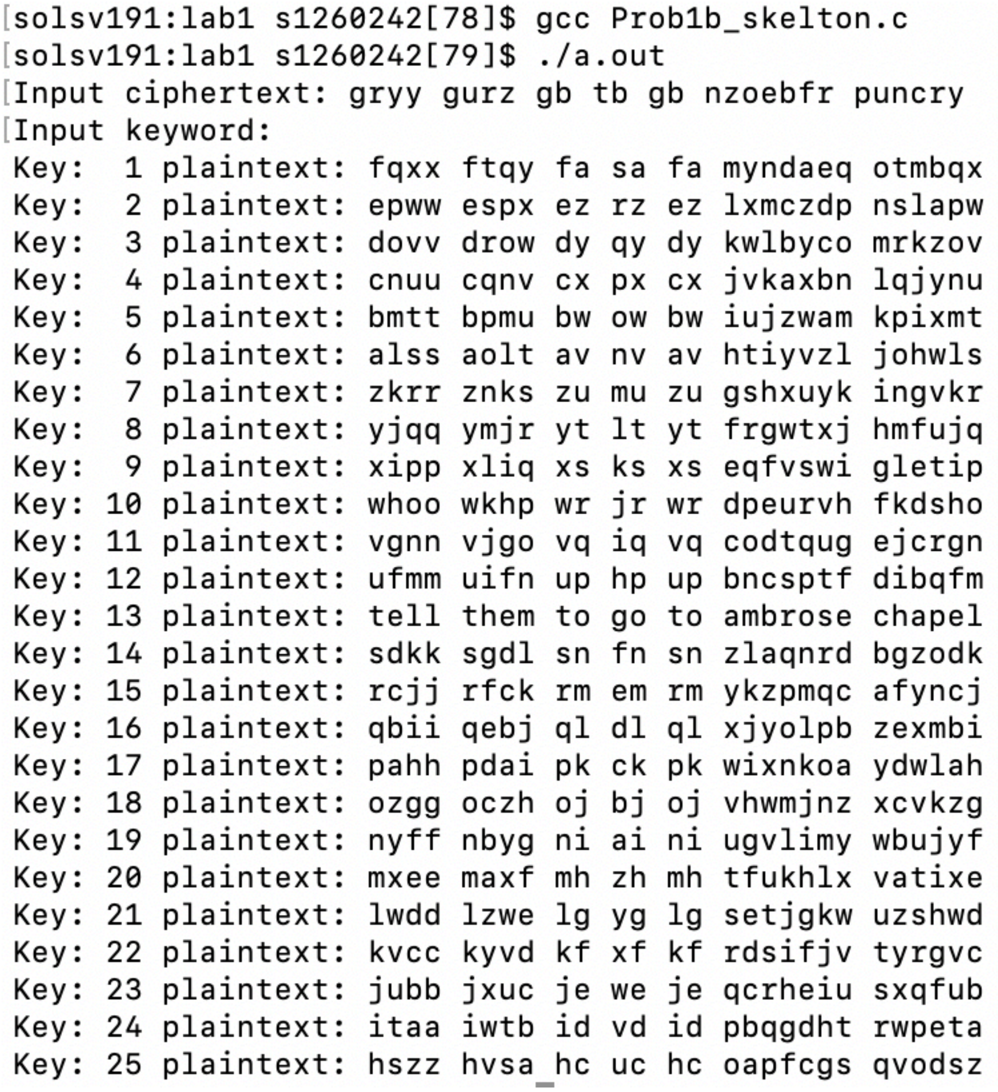
```
[solsv191:lab1 s1260242[73]$ gcc Prob1b_skelton.c
[solsv191:lab1 s1260242[74]$ ./a.out
[Input ciphertext: gryy gurz gb tb gb nzoebfr puncry
[Input keyword: chapel
 Key: 13 plaintext: tell them to go to ambrose chapel
```

Keyword is nothing:



```
[solsv191:lab1 s1260242[76]$ gcc Prob1b_skelton.c
[solsv191:lab1 s1260242[77]$ ./a.out
[Input ciphertext: gryy gurz gb tb gb nzoebfr puncry
[Input keyword: apple
 There is no decryption for keyword apple
```

Without keyword:



```
[solsv191:lab1 s1260242[78]$ gcc Prob1b_skelton.c
[solsv191:lab1 s1260242[79]$ ./a.out
[Input ciphertext: gryy gurz gb tb gb nzoebfr puncry
[Input keyword:
 Key:  1 plaintext: fqxx ftqy fa sa fa myndaeq otmbqx
 Key:  2 plaintext: epww espx ez rz ez lxmczdp nslapw
 Key:  3 plaintext: dovv drow dy qy dy kwlbyco mrkzov
 Key:  4 plaintext: cnuu cqnv cx px cx jvkaxbn lqjynu
 Key:  5 plaintext: bmtt bpmu bw ow bw iujzwam kpixmt
 Key:  6 plaintext: alss aolt av nv av htiyvzl johwls
 Key:  7 plaintext: zkrr znks zu mu zu gshxuyk ingvkr
 Key:  8 plaintext: yjqq ymjr yt lt yt frgwtxj hmfujq
 Key:  9 plaintext: xipp xliq xs ks xs eqfvswi gletip
 Key: 10 plaintext: whoo wkhp wr jr wr dpeurvh fkdsho
 Key: 11 plaintext: vgnn vjgo vq iq vq codtqug ejcrgn
 Key: 12 plaintext: ufmm uifn up hp up bncsptf dibqfm
 Key: 13 plaintext: tell them to go to ambrose chapel
 Key: 14 plaintext: sdkk sgdl sn fn sn zlaqnrd bgzodk
 Key: 15 plaintext: rcjj rfck rm em rm ykzpmqc afyncj
 Key: 16 plaintext: qbii qebj ql dl ql xjyolpb zexmbi
 Key: 17 plaintext: pahh pdai pk ck pk wixnkoa ydwlah
 Key: 18 plaintext: ozgg oczh oj bj oj vhwmjnz xcvkzg
 Key: 19 plaintext: nyff nbyg ni ai ni ugvlimy wbujyf
 Key: 20 plaintext: mxee maxf mh zh mh tfukhlx vatixe
 Key: 21 plaintext: lwdd lzwe lg yg lg setjgkw uzshwd
 Key: 22 plaintext: kvcc kyvd kf xf kf rdsifjv tyrgvc
 Key: 23 plaintext: jubb jxuc je we je qcrheiu sxqfub
 Key: 24 plaintext: itaa iwtb id vd id pbqgdht rwpeta
 Key: 25 plaintext: hszz hvsa hc uc hc oapfcgs qvodsz
```

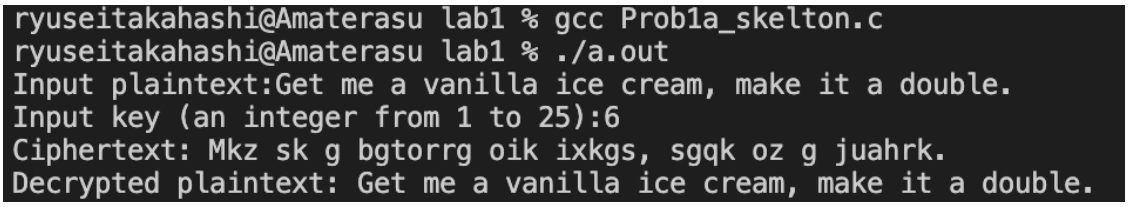
the codes are included in C files

c)

(1)

k=6, plaintext=”Get me a vanilla ice cream, make it a double.”

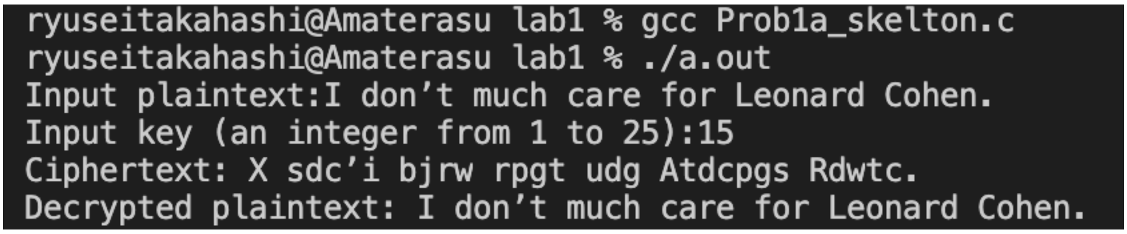
Result:



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1a_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input plaintext:Get me a vanilla ice cream, make it a double.
Input key (an integer from 1 to 25):6
Ciphertext: Mkz sk g bgtorrg oik ixkgs, sgqk oz g juahrk.
Decrypted plaintext: Get me a vanilla ice cream, make it a double.
```

k=15, plaintext=”I don’t much care for Leonard Cohen.”

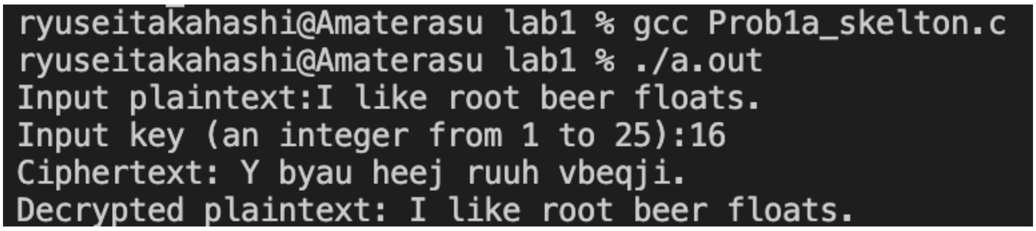
Result:



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1a_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input plaintext:I don’t much care for Leonard Cohen.
Input key (an integer from 1 to 25):15
Ciphertext: X sdc’i bjrw rpgt udg Atdcpgs Rdwtc.
Decrypted plaintext: I don’t much care for Leonard Cohen.
```

k＝16, plaintext=”I like root beer floats.”

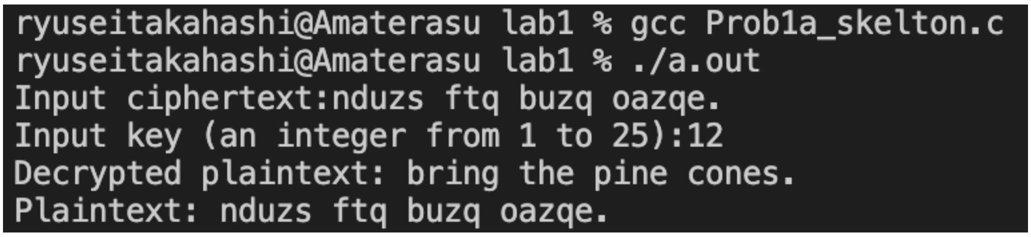
Result:



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1a_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input plaintext:I like root beer floats.
Input key (an integer from 1 to 25):16
Ciphertext: Y byau heej ruuh vbeqji.
Decrypted plaintext: I like root beer floats.
```

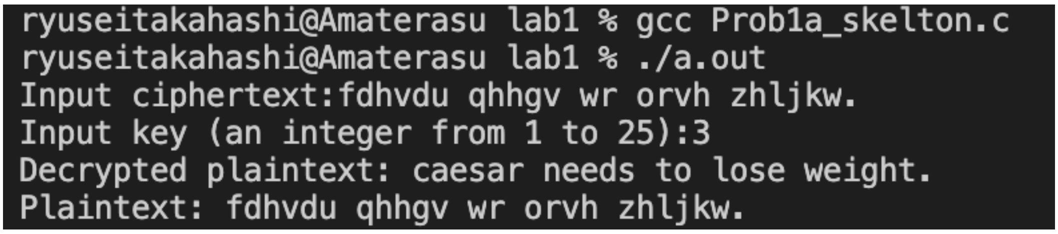
d)

k=12, ciphertext=” nduzs ftq buzq oazqe.”



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1a_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input ciphertext:nduzs ftq buzq oazqe.
Input key (an integer from 1 to 25):12
Decrypted plaintext: bring the pine cones.
Plaintext: nduzs ftq buzq oazqe.
```

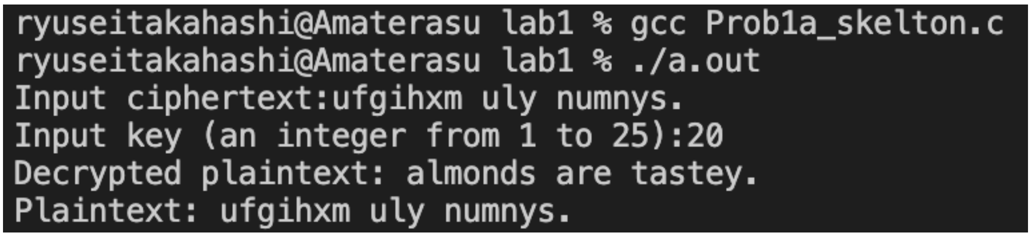
k=3, ciphertext= “fdhvdu qhhgv wr orvh zhljkw.”



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1a_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input ciphertext:fdhvdu qhhgv wr orvh zhljkw.
Input key (an integer from 1 to 25):3
Decrypted plaintext: caesar needs to lose weight.
Plaintext: fdhvdu qhhgv wr orvh zhljkw.
```

k=20, ciphertext=” ufgihxm uly numnys.

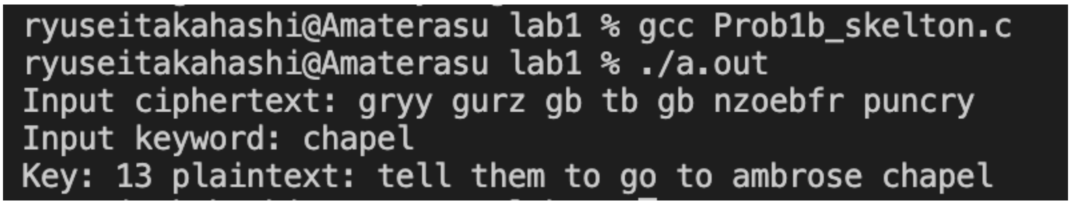
In C file, I change the from encrypt to decrypt and from decrypt to encrypt for using comment out.



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1a_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input ciphertext:ufgihxm uly numnys.
Input key (an integer from 1 to 25):20
Decrypted plaintext: almonds are tastey.
Plaintext: ufgihxm uly numnys.
```

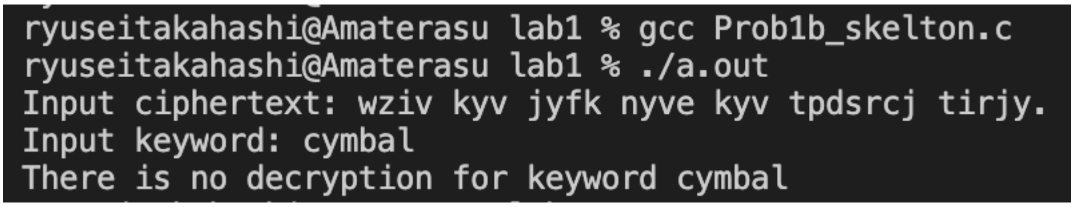
e)

ciphertext=” gryy gurz gb tb gb nzoebfr puncry”, keyword=”chapel”



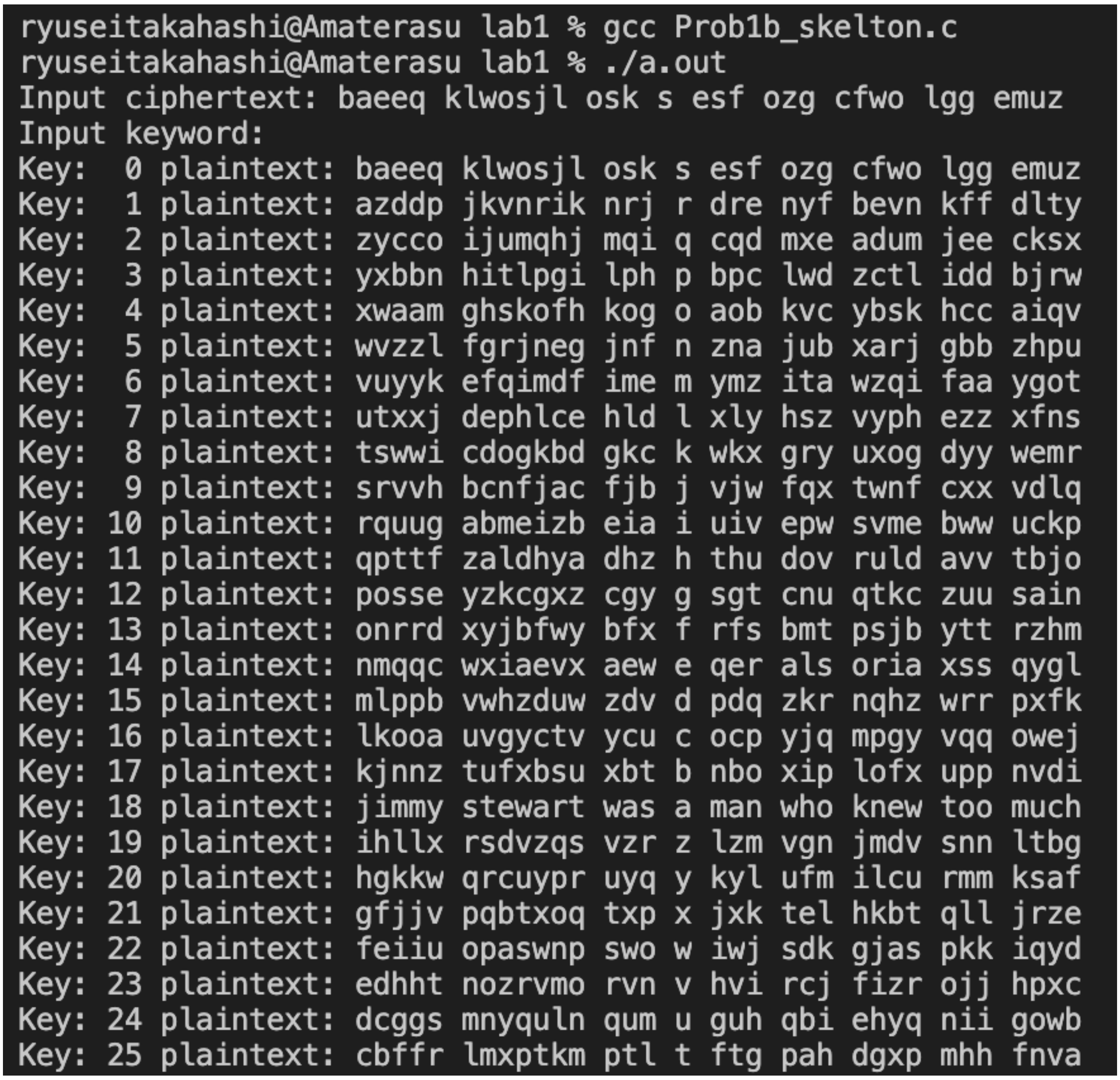
```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1b_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input ciphertext: gryy gurz gb tb gb nzoebfr puncry
Input keyword: chapel
Key: 13 plaintext: tell them to go to ambrose chapel
```

ciphertext=” wziv kyv jyfk nyve kyv tpdsrcj tirjy.”, keyword=”symbal”



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1b_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input ciphertext: wziv kyv jyfk nyve kyv tpdsrcj tirjy.
Input keyword: cymbal
There is no decryption for keyword cymbal
```

cipheretxt=” baeeq klwosjl osk s esf ozg cfwo lgg emuz”, no keyword



```
ryuseitakahashi@Amaterasu lab1 % gcc Prob1b_skelton.c
ryuseitakahashi@Amaterasu lab1 % ./a.out
Input ciphertext: baeeq klwosjl osk s esf ozg cfwo lgg emuz
Input keyword:
Key:  0 plaintext: baeeq klwosjl osk s esf ozg cfwo lgg emuz
Key:  1 plaintext: azddp jkvnrik nrj r dre nyf bevn kff dlty
Key:  2 plaintext: zycco ijumqhj mqi q cqd mxe adum jee cksx
Key:  3 plaintext: yxbbn hitlpgi lph p bpc lwd zctl idd bjrw
Key:  4 plaintext: xwaam ghskofh kog o aob kvc ybsk hcc aiqv
Key:  5 plaintext: wvzzl fgrjneg jnf n zna jub xarj gbb zhpu
Key:  6 plaintext: vuyyk efqimdf ime m ymz ita wzqi faa ygot
Key:  7 plaintext: utxxj dephlce hld l xly hsz vyph ezz xfns
Key:  8 plaintext: tswwi cdogkbd gkc k wkx gry uxog dyy wemr
Key:  9 plaintext: srvvh bcnfjac fjb j vjw fqx twnf cxx vdlq
Key: 10 plaintext: rquug abmeizb eia i uiv epw svme bww uckp
Key: 11 plaintext: qpttf zaldhya dhz h thu dov ruld avv tbjo
Key: 12 plaintext: posse yzkcgxz cgy g sgt cnu qtkc zuu sain
Key: 13 plaintext: onrrd xyjbfwy bfx f rfs bmt psjb ytt rzhm
Key: 14 plaintext: nmqqc wxiaevx aew e qer als oria xss qygl
Key: 15 plaintext: mlppb vwhzduw zdv d pdq zkr nqhz wrr pxfk
Key: 16 plaintext: lkooa uvgyctv ycu c ocp yjq mpgy vqq owej
Key: 17 plaintext: kjnnz tufxbsu xbt b nbo xip lofx upp nvdi
Key: 18 plaintext: jimmy stewart was a man who knew too much
Key: 19 plaintext: ihllx rsdvzqs vzr z lzm vgn jmdv snn ltbg
Key: 20 plaintext: hgkkw qrcuypr uyq y kyl ufm ilcu rmm ksaf
Key: 21 plaintext: gfjjv pqbtxoq txp x jxk tel hkbt qll jrze
Key: 22 plaintext: feiiu opaswnp swo w iwj sdk gjas pkk iqyd
Key: 23 plaintext: edhht nozrvmo rvn v hvi rcj fizr ojj hpxc
Key: 24 plaintext: dcggs mnyquln qum u guh qbi ehyq nii gowb
Key: 25 plaintext: cbffr lmxptkm ptl t ftg pah dgxp mhh fnva
```

Problem2

1） I confirmed it.

2） bgepsonm_lk_ihy_at_uwfrdvc

Problem3

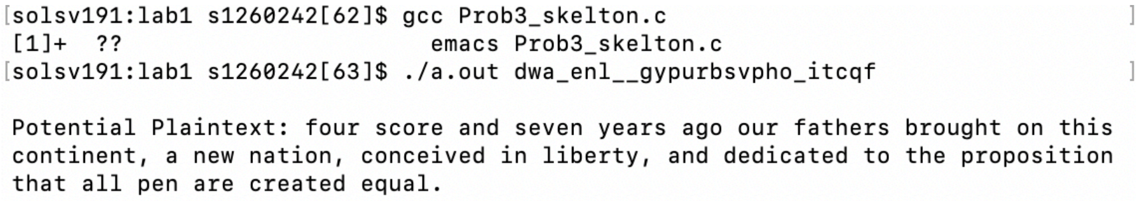
a) Implement a C function that performs frequency attacks on a mono-alphabetic substitution ciphers.

the codes are included in C files

b) Implement a C function that takes a partial mono-alphabetic substitution (i.e., subs in Problem 2) and a ciphertext and returns a potential plaintext.

the codes are included in C files

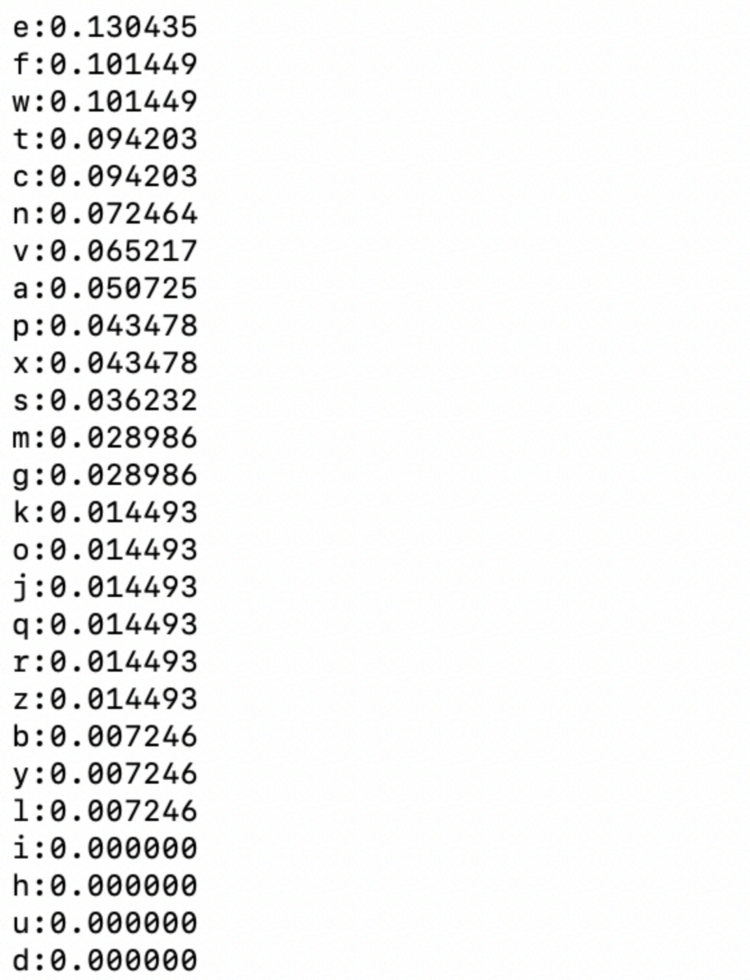
c) Use your functions from (a) and (b) to decrypt the following cipher text:
"ztmn pxtne cfa peqef kecnp cjt tmn zcwsenp ontmjsw ztnws tf wsvp xtfwvfefw, c feb fcwvtf, xtfxevqea vf gvoenwk, cfa aeavxcwea wt wse rntrtpvwvtf wscw cgg lef cne xnecwea eymcg."



```
[solsv191:lab1 s1260242[62]$ gcc Prob3_skelton.c                              ]
 [1]+  ??                        emacs Prob3_skelton.c
[solsv191:lab1 s1260242[63]$ ./a.out dwa_enl__gypurbsvpho_itcqf              ]

 Potential Plaintext: four score and seven years ago our fathers brought on this
 continent, a new nation, conceived in liberty, and dedicated to the proposition
 that all pen are created equal.
```

The key is dwa_enl__gypurbsvpho_itcqf .



```
e:0.130435
f:0.101449
w:0.101449
t:0.094203
c:0.094203
n:0.072464
v:0.065217
a:0.050725
p:0.043478
x:0.043478
s:0.036232
m:0.028986
g:0.028986
k:0.014493
o:0.014493
j:0.014493
q:0.014493
r:0.014493
z:0.014493
b:0.007246
y:0.007246
l:0.007246
i:0.000000
h:0.000000
u:0.000000
d:0.000000
```

Based on the incidence of the letters above, we find out from the most used letters.