Fall 2026 CIS 3362 Homework #1 Solutions

1) For this question and the following question, I wrote some C++ code that takes in a string and for each possible decryption key for the shift cipher (0 to 25), applies it and prints out what the plaintext would be if the key were that value. The code is attached as the file h1code.cpp. When I ran the function q12() and inputted the string given for this question, the output produced was as follows:

```
0:   hvwgvogpssbobwbqfsrwpzvchgiaasfzshgvcdsksrcbhaszh
1:   guvfunforanavaperqvoyubgfhzzreyrgfubcrjrqbagzryg
2:   ftuetmenqqzmzuzodqpunxtafegyyqdxqfetabqiqpazfyqxf
3:   estdsldmppylytyncpotmwszedfxxpcwpedszaphpozyexpwe
4:   drscrkclooxkxsxmbonslvrydcewwobvodcryzogonyxdwovd
5:   cqrbqjbknnwjwrwlanmrkuqxcbdvvnauncbqxynfnmxwcvnuc
6:   bpqapiajmmvivqvkzmlqjtpwbacuumztmbapwxmemlwvbumtb
7:   aopzohzilluhupujylkpisovazbttlyslazovwldlkvuatlsa
8:   znoyngyhkktgtotixkjohrnuzyasskxrkzynuvkckjutzskrz
9:   ymnxmfxgjjsfsnshwjingqmtyxzrrjwqjyxmtujbjitsyrjqy
10:  xlmwlewfiirermrgvihmfplsxwyqqivpixwlstiaihsrxqipx
11:  wklvkdvehhqdqlqfuhgleokrwvxpphuohwvkrshzhgrqwphow
12:  vjkujcudggpcpkpetgfkdnjqvuwoogtngvujqrgygfqpvognv
13:  uijtibtcffobojodsfejcmiputvnnfsmfutipqfxfepounfmu
14:  thishasbeenanincrediblhotsummerletshopewedontmelt
15:  sghrgzraddmzmhmbqdchakgnsrtlldqkdsrgnodvdcnmsldks
16:  rfgqfyqzcclylglapcbgzjfmrqskkcpjcrqfmncucbmlrkcjr
17:  qefpexpybbkxkfkzobafyielqprjjboibqpelmbtbalkqjbiq
18:  pdeodwoxaajwjejynazexhdkpoqiianhapodklasazkjpiahp
19:  ocdncvnwzzividixmzydwgcjonphhzmgzoncjkzrzyjiohzgo
20:  nbcmbumvyyhuhchwlyxcvfbinmoggylfynmbijyqyxihngyfn
21:  mablatluxxgtgbgvkxwbueahmlnffxkexmlahixpxwhgmfxem
22:  lzakzsktwwfsfafujwvatdzglkmeewjdwlkzghwowvgflewdl
23:  kyzjyrjsvverezetivuzscyfkjlddvicvkjyfgvnvufekdvck
24:  jxyixqiruudqdydshutyrbxejikccuhbujixefumutedjcubj
25:  iwxhwphqttcpcxcrgtsxqawdihjbbtgatihwdetltsdcibtai
```

It's interesting to note that one of the wrong shifts spuriously produced two consecutive words. On occasion this happens, but of course, the rest of the text is garbage, so 1 wasn't the correct encryption key. Instead, the correct encryption key was 14, so to decrypt, we subtract 14 (or add 12), revealing the following plaintext:

This has been an incredibl hot summer. Let's hope we don't melt.

You'll notice that incredible was misspelled. In this case, it wasn't intentional, just some fast, inaccurate typing. But a common strategy for those encrypting messages is to intentionally misspell lots of words so as to thwart those trying to break the code looking for patterns that match regular English letter combinations. One can misspell quite a bit, but the intended recipient can still make out the message.

2) For this question I chose to first run my code on a small prefix of the given ciphertext, producing the following output:

```
0:   grrngorzugrsgsgzkxcnuykhgtt
1:   fqqmfnqytfqrfrfyjwbmtxjgfss
2:   epplempxsepqeqexivalswiferr
3:   dookdlowrdopdpdwhuzkrvhedqq
4:   cnnjcknvqcnococvgtyjqugdcpp
5:   bmmibjmupbmnbnbufsxiptfcboo
6:   allhailtoalmamaterwhosebann
7:   zkkgzhksnzklzlzsdqvgnrdazmm
8:   yjjfygjrmyjkykyrcpufmqczyll
9:   xiiexfiqlxijxjxqbotelpbyxkk
10:  whhdwehpkwhiwiwpansdkoaxwjj
11:  vggcvdgojvghvhvozmrcjnzwvii
12:  uffbucfniufgugunylqbimyvuhh
13:  teeatbemhteftftmxkpahlxutgg
14:  sddzsadlgsdeseslwjozgkwtsff
15:  rccyrzckfrcdrdrkvinyfjvsree
16:  qbbxqybjeqbcqcqjuhmxeiurqdd
17:  paawpxaidpabpbpitglwdhtqpcc
18:  ozzvowzhcozaoaohsfkvcgspobb
19:  nyyunvygbnyznzngrejubfronaa
20:  mxxtmuxfamxymymfqditaeqnmzz
21:  lwwsltwezlwxlxlepchszdpmlyy
22:  kvvrksvdykvwkwkdobgrycolkxx
23:  juuqjrucxjuvjvjcnafqxbnkjww
24:  ittpiqtbwituiuibmzepwamjivv
25:  hssohpsavhsththalydovzlihuu
```

The only potential option is an encryption key of 6, so I then applied that to the whole text with the function decryptShift:

All Hail to Alma Mater
whose banner Black and Gold
will wave in fame and splendor
as the passing years unfold.
May loyalty and friendship
within our hearts unite
and light the star to guide us
ever upward in our flight
With honor and affection
our frendship will renew
we sing of thee our Alma Mater ever true!

This is UCF's Alma Mater!

3) There are 312 possible keys for this cipher, so it would be best if we didn't have to print out the corresponding decryption for each possible encryption key. Instead, what we can do is search for a few words or maybe even one word, and only print out the decryptions that contain that word (say "the") or maybe the decryptions that have a high percentage of both e's and t's, and then manually sort out the answer from there.

Let's do a first stab at it by only printing out the decryptions with the word "the". The corresponding code is also in the file h1code.cpp (ran function q3()). Here is the output:

```
270 3 5
gyjlcpcdxhlbejzspwpgdhchogyjgydwgjjclcdgjebgpgjbhopxjwdzpvyjcdcg
yjzhlwbjhoylxpcjqjcgbdgujzhxjbcjzjbbpwfohwhcjmjhmsjghedbbhsqjgyj
mhsdgdzpsupcebvydzyypqjzhccjzgjegyjxvdgypchgyjwpceghpbblxjpxhctg
yjmhvjwbhogyjjpwgygyjbjmpwpgjpcejrlpsbgpgdhcghvydzygyjspvbhocpgl
wjpcehocpglwjbthejcgdgsjgyjxpejzjcgwjbmjzgghgyjhmdcdhcbhoxpcndce
wjrldwjbgypggyjfbyhlseejzspwjgyjzplbjbvydzydxmjsgyjxghgyjbjmpwpg
dhc
122 5 6
zdeqbobuksqinewtorozusbsvzdezdurzeebqbuzenizozeisvokeruwoydebubz
dewsqriesvdqkobehebziuzfewskeibeweiiorgvsrsbejesjtezsnuiisthezde
jstuzuwotfobniyduwddohewsbbewzenzdekyuzdobszderobnzsoiiqkeoksbmz
dejsyerisvzdeeorzdzdeiejorozeobneaqotizozusbzsyduwdzdetoyisvbozq
reobnsvbozqreimsnebzuztezdekonewebzreijewzzszdesjubusbisvkobcubn
reaqureizdozzdegidsqtnnewtorezdewoqieiyduwdukjetzdekzszdeiejoroz
usb
144 9 25
celrqdqtbfrnwlhmdydctfqfacelcetycllqrqtclwncdclnfadblythdvelqtqc
elhfrynlfaerbdqlglqcntcslhfblnqlhlnndyzafyfqlulfumlcfwtnnfmglcel
ufmtcthdmsdqwnvetheedglhfqqlhclwcelbvtcedqfcelydqwcfdnnrbldbfqpc
elufvlynfacelldycecelnludydcldqwljrdmncdctfqcfvethecelmdvnfaqdcr
yldqwfaqdcrylnpfwlqctcmlcelbdwlhlqcylnulhccfcelfutqtfqnfabdqxtqw
yljrtylncedccelznefrmwwlhmdylcelhdrnlnvethetbulmcelbcfcelnludydc
tfq
292 11 13
iwtjcpcxbdjhstrapgpixdcduiwtiwxgittcjcxitshipithdupbtgxrplwtcxci
wtrdjghtduwjbpctktcihxiqtrdbthctrthhpgnudgdctetdeatidsxhhdaktiwt
edaxixrpaqpcshlwxrwwpktrdcctritsiwtblxiwpcdiwtgpcsidphhjbtpbdcvi
wtedltghduiwttpgiwiwthtepgpitpcstfjpahipixdcidlwxrwiwtaplhducpij
gtpcsducpijgthvdstcixiatiwtbpstrtcigthetriidiwtdexcxdchdubpczxcs
gtfjxgthiwpiiwtnhwdjasstrapgtiwtrpjhthlwxrwxbetaiwtbidiwthtepgpi
xdc
0 11 24
theunanimousdeclarationofthethirteenunitedstatesofamericawhenint
hecourseofhumaneventsitbecomesnecessaryforonepeopletodissolvethe
politicalbandswhichhaveconnectedthemwithanotherandtoassumeamongt
hepowersoftheearththeseparateandequalstationtowhichthelawsofnatu
reandofnaturesgodentitlethemadecentrespecttotheopinionsofmankind
```

```
requiresthattheyshoulddeclarethecauseswhichimpelthemtotheseparat
ion
235 17 10
hfystgtqieswnycxglghqetejhfyhfqlhyytstqhynwhghywejgiylqcgofytqth
fyceslwyejfsigtydythwqhryceiywtycywwglkjeletypyepxyhenqwwexdyhfy
pexqhqcgxrgtnwofqcffgdycettychynhfyioqhfgtehfylgtnhegwwsiygietuh
fypeoylwejhfyyglhfhfywypglghygtnyasgxwhghqetheofqcfhfyxgowejtghs
lygtnejtghslywuenythqhxyhfyignycythlywpychhehfyepqtqetwejigtmqtn
lyasqlywhfghhfykwfesxnnycxglyhfycgswywofqcfqipyxhfyihehfywypglgh
qet
```

The output consists of the integer index at which "the" was found in the string, and the corresponding decryption keys of a and b that generated that output.

It follows that the correct decryption keys were a = 11 and b = 24 with the following plaintext:

The unanimous Declaration of the thirteen United States of America,

When in the course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation.

This, of course, is the beginning of the United States Declaration of Independence. (I thought it would be fun to put it in here as we're celebrating 250 years since the Declaration.)

As an exercise, let's compute the corresponding encryption keys that were used:

We're solving for y:

x = (11y + 24) (mod 26)

11y = (x – 24) (mod 26)

$19(11y) \equiv 19(x + 2)(mod\ 26)$

$209y \equiv (19x + 38)(mod\ 26)$

$y \equiv (19x + 12)(mod\ 26)$

Thus, the original encryption keys used were a = 19 and b = 12.
We decrypted using a = 11 and b = 24.

Note: I used the look up chart on the given Reference Sheet posted for the course (https://www.cs.ucf.edu/courses/cis3362/fall2026/refsheets/ReferenceSheet.pdf) for the inverse of 11 mod 26.

4) The affine cipher for a language with 45 letters has the encryption keys a = 28 and b = 16. What are the corresponding decryption keys?

The encryption function is:

f(x) = (28x + 16) (mod 45)

Let's switch x and y and solve for y:

$x \equiv (28y + 16)(mod\ 46)$

$(x - 16) \equiv 28y(mod\ 45)$, now we need to find 28^{-1} mod 45.

45 = 1 x 28 + 17
28 = 1 x 17 + 11
17 = 1 x 11 + 6
11 = 1 x 6 + 5
6 = 1 x 5 + 1, gcd = 1

6 – 1 x 5 = 1
6 – (11 – 6) = 1
2x6 – 1 x11 = 1
2(17 – 11) – 1 x 11 = 1
2 x 17 – 3 x 11 = 1
2 x 17 – 3(28 – 17) = 1
2 x 17 – 3 x 28 + 3 x 17 = 1
5 x 17 – 3 x 28 = 1
5(45 – 28) – 3 x 28 = 1
5 x 45 – 5 x 28 – 3 x 28 = 1
5 x 45 – 8 x 28 = 1

Taking this equation mod 45, we find that $-8(28) \equiv 1\ (mod\ 45)$.
It follows that $28^{-1} \equiv -8 \equiv 37\ (mod\ 45)$.
So, we'll multiply the equation we have through by 37:

$(37)28y \equiv 37(x - 16)(mod\ 45)$
$y \equiv (37x - 37 \times 16)(mod\ 45)$
$y \equiv (37x + 8 \times 16)(mod\ 45)$
$y \equiv (37x + 128)(mod\ 45)$
$y \equiv (37x + 38)(mod\ 45)$

It follows that the corresponding decryption keys are **a = 37 and b = 38.**

A relatively simple way to double check this is to compute $f(f^{-1}(x))$, which should return x under mod 45:

$$f\left(f^{-1}(x)\right) = (28(37x + 38) + 16)\ (mod\ 45)$$

$$= (1036x + 1064 + 16)\ (mod\ 45)$$

$$\equiv (x + 1080)\ (mod\ 45)$$

$$\equiv x\ (mod\ 45)$$

This proves that the corresponding decryption keys we found are indeed correct!