Fall 2025 CIS 3362 Homework 1 Solution

1) (shift)

```
kivgwcjmtqmdmqiulzqvsqvoixatzqopbvwe
```

Solution

I ran my program breakshift.py that is attached and here is the output it produced:

```
1 jhufvbilsplclphtkypurpunhwzsypnoauvd
2 igteuahkrokbkogsjxotqotmgvyrxomnztuc
3 hfsdtzgjqnjajnfriwnspnslfuxqwnlmystb
4 gercsyfipmizimeqhvmromrketwpvmklxrsa
5 fdqbrxeholhyhldpgulqnlqjdsvouljkwqrz
6 ecpaqwdgnkgxgkcoftkpmkpicruntkijvpqy
7 dbozpvcfmjfwfjbnesjoljohbqtmsjhiuopx
8 canyoubelieveiamdrinkingapslrightnow
9 bzmxntadkhdudhzlcqhmjhmfzorkqhfgsmnv
10 aylwmszcjgctcgykbpgligleynqjpgefrlmu
11 zxkvlrybifbsbfxjaofkhfkdxmpiofdeqklt
12 ywjukqxahearaewiznejgejcwlohnecdpjks
13 xvitjpwzgdzqzdvhymdifdibvkngmdbcoijr
14 wuhsiovyfcypycugxlchechaujmflcabnhiq
15 vtgrhnuxebxoxbtfwkbgdbgztilekbzamghp
16 usfqgmtwdawnwasevjafcafyshkdjayzlfgo
17 trepflsvczvmvzrduizebzexrgjcizxykefn
18 sqdoekrubyuluyqcthydaydwqfibhywxjdem
19 rpcndjqtaxtktxpbsgxczxcvpehagxvwicdl
20 qobmcipszwsjswoarfwbywbuodgzfwuvhbck
21 pnalbhoryvrirvnzqevaxvatncfyevtugabj
22 omzkagnqxuqhqumypduzwuzsmbexdustfzai
23 nlyjzfmpwtpgptlxoctyvtyrladwctrseyzh
24 mkxiyelovsofoskwnbsxusxqkzcvbsqrdxyg
25 ljwhxdknurnenrjvmarwtrwpjybuarpqcwxf
```

Looks like the key was 8 and the original plaintext (with spaces, capitalization and punctuation added) is:

Can you believe I am drinking a PSL right now?

2) (shift)

```
amzsqhifscbdzomtowfkwzzpsuwjsbcbnccapsqoigswkwzzpshfojszwbuk
whvhvsdfcufoaawbuhsoawbhvspsuwbbwbuctgsdhsapsfkwgvigziqy
```

Solution

I ran my program inputting this ciphertext and will not include the whole output because it line wraps and won't look great. But with a visual inspection, I found that the key = 14 and here is the corresponding plaintext, again with capitalization, punctuation, etc. added:

My lecture on Playfair will be given on Zoom because I will be traveling with the programming team in the beginning of September. Wish us luck!

3) (affine)

```
rozcrrpagodrpivimovxaqsmcvvidrhuviqxadeqboowqbocrbhirmphuzqv
wadrpipozigrpqramqdadmovzovqriaradrosuhimrcviodidaesqrpaguiq
vapqnirvaixqdxtqahixroxorpagadrpiryozqgruiqvgbcraqspozadebuz
crraderpagadyvaradeadqdqggaedsidrayahhtiihroobqxdorroxoar
```

Solution

I ran my program, breakaffine.py on this ciphertext. This program tries all 312 affine decryption keys and searches for three words in the supposed decryption: "the", "and" and "prize". Luckily the program only spit out 12 possibilities and the last one is the correct plaintext. Here is everything it spit out:

```
1 16
hepshhfqwethfylycelnqgicsllythxklygnqtugreemgreshrxyhcfxkpglmqth
fyfepywhfghqcgtqtcelpelghyqhqtheikxychslyetytquighfqwkyglqfgdyhl
qyngtnjgqxynhenehfqwqthfyhoepgwhkyglwrshqgifepqturkpshhqtuhfqwqt
olqhqtuqtgtgwwqutiythqoqxxjyyxheergntehheneqh
1 23
olwzoomxdlaomfsfjlsuxnpjzssfaoersfnuxabnylltnylzoyefojmerwnstxao
mfmlwfdomnoxjnaxajlswlsnofxoxaolprefjozsflafaxbpnomxdrfnsxmnkfos
xfunauqnxefuolulomxdxaomfovlwndorfnsdyzoxnpmlwxabyrwzooxabomxdxa
vsxoxabxananddxbapfaoxvxeeqffeollynualoolulxo
3 23
wnudwwqxpngwqvivhnioxtzhdiivgwsfivtoxgjtannltandwasvwhqsfutilxgw
qvqnuvpwqtwxhtgxghniunitwvxwxgwnzfsvhwdivngvgxjztwqxpfvtixqtkvwi
xvotgoctxsvownonwqxpxgwqvwrnutpwfvtipadwxtzqnuxgjafudwwxgjwqxpxg
rixwxgjxgtgtppxjgzvgwxrxsscvvswnnatognwwnonxw
5 6
nybqnndgkyvnduhuoyhrgisoqhhuvnpchuirgvailyymilyqnlpunodpcbihmgvn
dudybukndingoivgvoyhbyhinugngvnyscpuonqhuyvuvgasindgkcuihgditunh
gurivrxigpurnyryndgkgvndunwybiknciuihklqngisdybgvalcbqnngvandgkgv
whgngvagvivikkgavsuvngwgppxuupnyylirvynnyrygn
5 15
whkzwwmpthewmdqdxhqaprbxzqqdewylqdrapejruhhvruhzwuydwxmylkrqvpew
mdmhkdtwmrwpxrepexhqkhqrwdpwpewhblydxwzqdhedepjbrwmptldrqpmrcdwq
pdareagrpydawhahwmptpewmdwfhkrtwldrqtuzwprbmhkpejulkzwwpejwmptpe
fqpwpejpererttpjebdewpfpyygddywhhuraehwwhahpw
5 19
alodaaqtxliaqhuhbluetvfbduuhiacpuhvetinvyllzvyldaychabqcpovuztia
```

```
qhqlohxaqvatbvitibluoluvahtatialfpchbaduhlihitnfvaqtxphvutqvghau
theviekvtchealelaqtxtiaqhajlovxaphvuxydatvfqlotinypodaatinaqtxti
jutatintivivxxtnifhiatjtcckhhcallyveilaalelta
7 7
wbavwwihxbcwilylnbymhpdnvyylcwerylpmhcjpobbfpobvwoelwnierapyfhcw
ilibalxwipwhnpchcnbyabypwlhwhcwbdrelnwvylbclchjdpwihxrlpyhipulwy
hlmpcmkphelmwbmbwihxhcwilwtbapxwrlpyxovwhpdibahcjoravwwhcjwihxhc
tyhwhcjhcpcpxxhjcdlcwhtheekllewbbopmcbwwbmbhw
7 9
ydcxyykjzdeyknanpdaojrfpxaaneygtanrojelrqddhrqdxyqgnypkgtcrahjey
knkdcnzykryjprejepdacdarynjyjeydftgnpyxandenejlfrykjztnrajkrwnya
jnoreomrjgnoydodykjzjeyknyvdcrzytnrazqxyjrfkdcjelqtcxyyjelykjzje
vajyjeljererzzjlefneyjvjggmnngyddqroedyydodjy
7 13
chgbccondhicorerthesnvjtbeerickxervsnipvuhhlvuhbcukrctokxgvelnic
orohgrdcovcntvinitheghevcrncnichjxkrtcberhirinpjvcondxrvenovarce
nrsvisqvnkrschshcondnicorczhgvdcxrvedubcnvjohgnipuxgbccnipcondni
zencnipnivivddnpijricnznkkqrrkchhuvsihcchshnc
15 23
szibssoxjzqsonanvzaexdhvbaanqsylandexqfdmzzpdmzbsmynsvoylidapxqs
onozinjsodsxvdqxqvzaizadsnxsxqszhlynvsbanzqnqxfhdsoxjlndaxodknsa
xnedqewdxyneszezsoxjxqsonstzidjslndajmbsxdhozixqfmlibssxqfsoxjxq
taxsxqfxqdqdjjxfqhnqsxtxyywnnyszzmdeqzsszezxs
17 7
klqpkkchflgkcnandlaihtbdpaangkwjantihgxtyllrtylpkywnkdcwjqtarhgk
cnclqnfkctkhdtghgdlaqlatknhkhgklbjwndkpanlgnghxbtkchfjntahctunka
hnitgisthwniklilkchfhgkcnkzlqtfkjntafypkhtbclqhgxyjqpkkhgxkchfhg
zahkhgxhgtgtffhxgbngkhzhwwsnnwkllytiglkklilhk
19 8
toputthisontherecordiamcurrentlyreadingabookaboutbletchlyparkint
hehopesthaticanincorporateitintomylectureonenigmathisyearihavetr
iedandfailedtodothisinthetwopastyearsbutiamhopingbyputtingthisin
writinginanassignmentiwillfeeltoobadnottodoit
19 8
toputthisontherecordiamcurrentlyreadingabookaboutbletchlyparkint
hehopesthaticanincorporateitintomylectureonenigmathisyearihavetr
iedandfailedtodothisinthetwopastyearsbutiamhopingbyputtingthisin
writinginanassignmentiwillfeeltoobadnottodoit
```

It follows that the decryption keys were a = 19, b = 8. Here is the work for the corresponding encryption keys (not necessary):

$x = 19y + 8 \pmod{26}$
$19y = (x - 8) \pmod{26}$
$11(19y) = 11(x - 8) \bmod 26$
$y = 11x - 88 = 11x + 16 \pmod{26}$
So this message was encrypted with the keys a = 11, b = 16.

Here is the plaintext with the normal formatting added:

To put this on the record I am currently reading a book about Bletchly Park in the hopes that I can incorporate it into my lecture on Enigma this year. I have tried and failed to do this in the two past years but I am hoping by putting this in writing in an assignment I will feel too bad not to do it.

Incidentally, I have been trying to read the book when I go to lunch. So far I have read 104 pages. I will say that it's a compilation of first hand sources (people who were actually there), and combing through these sorts of sources is not easy. (People say a lot of random, non-relevant things. So when historians take those first hand accounts and write them up, they do a great deal of work cleaning up the writing and presenting what occurred in a more objective way, removing lots of irrelevant commentary.)

4) Using the affine cipher with **encryption keys** a = 9 and b = 4, encrypt a message (a nice one) for the course TAs!

Solution

I ran my program printaffine.py which has a message hard-coded and then I encrypted it with the keys above to yield the following ciphertext:

```
tperqkxabgbefyrgimekkygriort
```