Fall 2021 CIS 3362 Week One Homework Solutions

For questions 1 - 3 decode each message. The techniques used to encrypt the messages are given in parentheses right before the cipher text. In your write-up, explain the process you used to decrypt and include any code you might have used as an aid. Please do not use websites that automatically solve ciphers as most of your grade will be based on your description of the decryption process and **original code** you include in your write up.

1) (shift)

`hspytyczxpozldespczxldoz`

Solution

I wrote an attached program (shift_dec.c) that tries each decryption key and prints out possible plain text trying all 26 decryption keys. To run the program, just run it on the command line and pipe in a file with just the input string (which is above). Here is the output generated:

Dec Key 1: groxsxbywonykcdrobywkcny
Dec Key 2: fqnwrwaxvnmxjbcqnaxvjbmx
Dec Key 3: epmvqvzwumlwiabpmzwuialw
Dec Key 4: dolupuyvtlkvhzaolyvthzkv
Dec Key 5: cnktotxuskjugyznkxusgyju
Dec Key 6: bmjsnswtrjitfxymjwtrfxit
Dec Key 7: alirmrvsqihsewxlivsqewhs
Dec Key 8: zkhqlqurphgrdvwkhurpdvgr
Dec Key 9: yjgpkptqogfqcuvjgtqocufq
Dec Key 10: xifojospnfepbtuifspnbtep
Dec Key 11: wheninromedoastheromasdo
Dec Key 12: vgdmhmqnldcnzrsgdqnlzrcn
Dec Key 13: ufclglpmkcbmyqrfcpmkyqbm
Dec Key 14: tebkfkoljbalxpqeboljxpal
Dec Key 15: sdajejnkiazkwopdankiwozk
Dec Key 16: rczidimjhzyjvnoczmjhvnyj
Dec Key 17: qbyhchligyxiumnbyligumxi
Dec Key 18: paxgbgkhfxwhtlmaxkhftlwh
Dec Key 19: ozwfafjgewvgsklzwjgeskvg
Dec Key 20: nyvezeifdvufrjkyvifdrjuf
Dec Key 21: mxudydhecuteqijxuhecqite
Dec Key 22: lwtcxcgdbtsdphiwtgdbphsd
Dec Key 23: kvsbwbfcasrcoghvsfcaogrc
Dec Key 24: juravaebzrqbnfgurebznfqb
Dec Key 25: itqzuzdayqpameftqdaymepa

The only message that makes sense uses a decryption key of 11. The message is:

When in rome do as the romas do.

As you can see, there's a typo in the plaintext. (Full credit will be given for fixing the typo or not fixing it…)

2) (shift)

```
yvmuqhuqbbsqkjyekiisxeebmybbdejweedbyduqdtmumybbqbbxqluqrujj
uhunfuhyudsu
```

Solution
Running the same program on a different file leads to the following answer (not including the full output to save space…) which was encrypted using a key of 16:

Dec Key 16: ifweareallcautiousschoolwillnotgoonlineandwewillallhaveabetterexperience

Putting spaces, we get:

If we are all cautious, school will not go online and we will all have a better experience.

3) (affine)

```
fxgksxfxcayclxivoawgviwofxfxobfxiaxcnfgbreovirofcpirewcbgvyx
obsixoafgtiollrcidfgfxiygdifglvcbfgkforrlgaactcrcfcia
```

Solution
I created a new program and tried all 312 possible keys. To avoid looking through them, I searched for a few common words and only printed out strings that had at least one of the common words to reduce the brute force work of looking through many possible plaintexts. Note that the program loops through decryption keys, not encryption keys. I also just pipe the input to the program on the command line just like the first two programs.

I decided to check for the following words: "the", "with" and "for". Using just these three words, here are the possibilities I got:

Dec Key 1 0:
fxgksxfxcayclxivoawgviwofxfxobfxiaxcnfgbreovirofcpirewcbgvyxobsixoafgtiollrcidfgfxiygdifgl
vcbfgkforrlgaactcrcfcia

Dec Key 11 23:
aqldnqaqtxbtoqhuvxfluhfvaqaqviaqhxqtkalicpvuhcvatghcpftilubqvinhqvxalyhvoocthealaqhbleha
loutialdavccolxxtytctathx

Dec Key 17 13:
uolbhouovnfvsotgrnxlgtxruouoreuotnovauleqdrgtqruvitqdxvelgforehtornulytrssqvtmuluotflmtuls
gveulburqqslnnvyvqvuvtn

Dec Key 21 18:
thoughthiscipherasmoremaththantheshiftonlyarelativelyminorchangehastobeappliedtothecodetoprintoutallpossibilities

Dec Key 23 22:
hfesufhfqwcqpfylgwielyighfhfgthfywfqjhetxkglyxghqdyxkiqtelcfgtuyfgwherygppxqynhehfycenyheplqtheshgxxpewwqrqxqhqyw

Dec Key 25 19:
ownjbwowrtvriwlyftxnylxfowowfsowltwrgonscpfylcforelcpxrsnyvwfsblwftonalfiicrlqonowlvnqloniyrsonjofccinttrarcrorlt

Pretty clearly, the decryption keys are a = 21, b = 18. Here's the work to get the encryption keys:

$f(x) = (21x + 18) \bmod 26$

Put x where f(x) is and $f^{-1}(x)$ where x is and we get:

$x = (21f^{-1}(x) + 18) \bmod 26$

$(x - 18) = 21f^{-1}(x) \bmod 26$
$5(x - 18) = 5(21)f^{-1}(x) \bmod 26$

$f^{-1}(x) = 5(x - 18) \bmod 26$

$f^{-1}(x) = (5x - 90) \bmod 26$

$f^{-1}(x) = (5x + 14) \bmod 26$, so the encryption keys were a = 5, b = 14.

Here is the plaintext:

Though this cipher as more math than the shift, only a relatively minor change has to be applied to the code to print out all possibilities.

Note: we can see this has another typo "as" was supposed to be "has".

4) Using the affine cipher with the encryption keys a = 15 and b = 6, encrypt the following plaintext:

```
tyingforsixteenthwithcornelluniversityinusnewsandworldreportspub
licationmostinnovativeschoolscategoryucfisfloridastoprankedschoo
lforinnovation
```

Solution

We can just take the code for #3, remove the loops and the word searches and produce the following ciphertext:

```
fcwtsdibqwnfootfhywfhkibtopputwjobqwfcwtuqtoyqgtzyibpzboxibfqxuv
pwkgfwiteiqfwttijgfwjoqkhiipqkgfosibcukdwqdpibwzgqfixbgtaozqkhii
pdibwttijgfwit
```

The code is attached in the file affine_q4.c.