Fall 2020 CIS 3362 Week One Assignment Solutions

(by Thomas Lukas)

1) You can write up a program that can brute force all possible shift values printing their decrypted values. You can see an example of a possible code solution (hmk1-1.c), when 10 is added to the encrypted cipher text we get the output:

```
Welcome to virtual cryptography.
```

The encryption key was k = 16, we get this value because $16 \equiv -10 \pmod{26}$

2) Using the same code from problem 1, when 18 is added to the encrypted cipher text (mod 26) we get the output:

```
Mathematics and considering all possibilities will be important
in this course.
```

The encryption key was k = 8, we get this value because $18 \equiv -8 \pmod{26}$

3) Simplest way to solve this problem is by brute force, since a is restricted to only coprime numbers there are 312 possible keys for the affine cipher. Writing a function that goes through each possible key, see (hmk1-3), we eventually find that the keys a=7 and b=24 decrypt the ciphertext:

```
Though the affine cipher is easy to break with a computer it
allows me to introduce you to quite a few important ideas in
cryptography such as the Extended Euclidean Algorithm.
```

We can find the keys that were used to encrypt the plaintext by finding the mod inverse:

$f(x) = (7x + 24) \bmod 26$
$(x-24) = 7f^{-1}(x) \bmod 26$
$15(x-24) = 15(7f^{-1}(x)) \bmod 26$
$f^{-1}(x) = (15x – 360) \bmod 26$
$f^{-1}(x) = 15x + 4 \bmod 26$

Therefore the encryption keys are a = 15 and b = 4

4) We can create a program that can encrypt the plaintext with the keys a=7 and b=22, so our function would be $f(x) = 7x + 22 \bmod 26$. The program (hmk1-4) gives us the encrypted cipher text:

```
kwjiqgkqcygxuaztwdwregyszaqjqlhqoyztwztwswvvztyvyzzylsajwpqquazt
wfqbmalwffyqlngvzgly
```