Fall 2018 CIS 3362 Week One Assignment Solutions

For questions 1 - 3 decode each message. The techniques used to encrypt the messages are either similar to methods used in the day 1 activity or the affine cipher. 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) `jruxhijgcxcvuxuinntpghdas`

Solution

A utility program was written to try each shift. This program is included at the end of this document. When a shift of +11 was applied to the ciphertext, the message:

```
UCF IS TURNING FIFTY YEARS OLD
```

is obtained. Note that this means that the encryption key was a shift of 15.

2) (shift) `lmkwlqvoumaaiomazmittgqavbawjil`

Solution

The use of the same utility program yields the following plaintext with a shift of +18 applied to the ciphertext. Thus the encryption key was 8.

```
DECODING MESSAGES REALLY ISN'T SO BAD
```

3) (affine) `jbdeaxeadzeixkxdfszkbzvazvfxmkvaxszkhxmvadsbzvircjzkxhd`
`uixkaxgabzvhzvocyvfavfxskxpvxehbrerobfdf`

Solution

Using the second utility program attached, we can sift through 312 possible decryptions to discover the cipher text. After a couple minutes of looking here is what we find:

```
MY INTENTION HERE IS FOR YOU TO USE BRUTE FORCE BUT IF YOU HAD
MORE CIPHERTEXT YOU COULD JUST USE FREQUENCY ANALYSIS
```

The corresponding decryption keys turn out to be a = 5, b = 19. Perhaps a quicker way to find this instead of scanning would be to use the "search" feature in notepad and look for common three letter words ("you" might be a good guess!).

4) Using the affine cipher with the encryption keys a = 9 and b = 6, encrypt the following plaintext:

```
packmyboxwithfivedozenliquorjugs
```

Note: If you write a program to perform the encryption, please include the text of that program in your write-up.

Solution

A simple edit can be made to any utility program for #3 to just print out the given affine operation only for a = 9 and b = 6. Here is the corresponding ciphertext:

```
lgyskopcfwavrzanqhcxqtbauecdjeim
```

Program for Questions 1, 2

```
#include <stdio.h>
#include <string.h>

int main() {

    char cipher[1000];
    scanf("%s", cipher);

    int i, j;

    // Try each shift.
    for (i=0; i<26; i++) {
        printf("%d\t", i);
        for (j=0; j<strlen(cipher); j++)
            printf("%c", (cipher[j]-'a'+i)%26 + 'a');
        printf("\n");
    }
    printf("\n");
    return 0;
}
```

Program for Question 3

```
#include <stdio.h>
#include <string.h>

const int ALIST[] = {1,3,5,7,9,11,15,17,19,21,23,25};

int main() {

    char cipher[1000];
    scanf("%s", cipher);

    int a, b, i, j;

    // Try each key.
    for (i=0; i<12; i++) {
      for (b=0; b<26; b++) {
        printf("%d %d\t", ALIST[i], b);
        for (j=0; j<strlen(cipher); j++)
          printf("%c", (ALIST[i]*(cipher[j]-'a')+b)%26 + 'a');
        printf("\n");
      }
    }
    printf("\n");
    return 0;
}
```

Program to solve question 4

```
#include <stdio.h>
#include <string.h>

int main() {
    char cipher[1000];
    scanf("%s", cipher);
    int i;

    for (i=0; i<strlen(cipher); i++) {
        printf("%c", (9*(cipher[i]-'a')+6)%26 + 'a');
    }
    printf("\n");

    return 0;
}
```