CIS 3362 Homework #2
Monoalphabetic Ciphers
Due: Check WebCourses for the due date.

Note: This is a group assignment. Each group should have two students. When you select your group, please let me know the composition of your group. I will collect these on August 29th and September 3rd. Any unassigned students will be put into groups of my choosing after that date. You must submit all assignments in WebCourses as groups – only one submission for group. (WebCourses will enforce this rule.)

1) Given that the encryption function for an affine cipher in a language with 45 alphabet characters is f(x) = (26x + 42) % 45, determine the corresponding decryption function. Please show all of your work.

2) Encrypt the following message below using the affine cipher function, f(x) = (17x + 23) % 26.

```
THISISOURFIRSTINVOLVEDHOMEWORKASSIGNMENT
```

3) Consider a language with an alphabet size of 200. How many possible affine cipher keys could there be for this language? (Note: You may write a program to answer this question. If you don't see if there's a short-cut to count the number of values from 1 to 200 that do share a common factor with 200.)

4) You are attempting to break an affine cipher (in English). You believe that the ciphertext 'W' maps to the plaintext letter 'e' and that the ciphertext 'R' maps to the plaintext 't'. Determine the **decryption** function used based on these two pieces of information.

5) Prove that composing two valid affine cipher functions produces another valid affine cipher function.

Decode the following ciphertexts. Please use the tools that I have provided off the course webpage and any tools you may create yourself. In your write-up, describe the steps you took and why you took them in decrypting the ciphertext. After your description, reveal the plaintext.

6) (shift)

```
mxudydhecuteqijxuhecqdite
```

7) (affine)

```
crayuhqpwezqjzwbayujhyiwkyjswqjnamjwqzckcnnnwzayucdydqnczznwewgj
wzcdzhwqdekwjryjouwezcydwcmhz
```

8) (affine)

```
zxqoqudqziozxyzigippxifqyhdinqwlbdifycykmkozzgqlzclilzx
```

9) (substitution)

```
zowdsbqsenviohsoozxsngmnazwsmnrnfflsdnmngxzbqnyswdssuzawfvazwnvg
vkwdzwbqnysazgvgftlsmswsqhngsmrnwdwdsngkvqhzwnvgngwdnohsoozxszgm
wdskvffvrngxvgsngsoosgasvgsdzowvovfeszffvkwdsmsaqtbwnvgbqvlfshok
nqowwvafznhwdsbqnyslsowvkfiajwvtvizffngvqmsqwvxswwdnobqnystvihio
wxvwvwdswdnqmkfvvqvkwdsdsalinfmngxenzwdsasgwqzfsfsezwvqwdsgsuwhs
oozxsrnffwsfftvihvqs
```

10) (substitution)

```
qfvjpbyxkkwbhbrqkjukpulhbgkkqcbkwubboqibfkpuluxswkkqcbkbloqibfkw
bubzxhhebqejyxlgujlkjgvjpujpswhvqkbvbhbrbhjoblxkbrblxgvjpqublkwp
ukzwblvjpnjvjpzxhhfbbfjababnxiqhfpoohxbfqfvjpfzxlskwbijrbujoblhj
jcqkkwbxlfxnbjgxkxkfubnzxkwfbrbuqhohqfkxiojpiwbfjlbjgkwjfbojpiwb
fzxhhwqrbqlblrbhjobzxkwkzjgubbfajjkwxbiqunfkqcbxkvjpzjl
```