Name: _____

Read and take notes on Section 1.7, The Affine Cipher. The first main result in this section can be summarized as follows:

> **Proposition.** Let a and b be integers in the range $0, 1, \ldots 25$ with a relatively prime to 26 (guaranteeing the existence of a multiplicative inverse mod 26.) The affine cipher with key (a, b) can be described by the affine encryption function
>
> $$E_{a,b}(x) = (ax + b) \ \%26$$
>
> This function has an inverse, the decryption function with decryption key (c, d), given by the following formula:
>
> $$D_{a,b}(x) = (cx + d) \ \%26\,, \quad \text{where} \quad c = a^{-1} \ \text{ and } \ d = -a^{-1}b$$

Reading Questions

1. Look again at the example in the second paragraph, encrypting 'hello how are you.'

   (a) What is the key for this affine cipher? What is the affine encryption function?

   (b) Encode first word of the plaintext, 'hello,' using the assignment 'a' is 0, 'b' is 1, etc. This will give you the encoded plaintext for the first word, as a series of five numbers.

   (c) Encrypt the encoded plaintext using the affine cipher function $E_{3,11}(x)$, i.e. for each number in your code from 1b, multiply by 3, add 11, and reduce modulo 26.

(d) Decode the ciphertext using the assignment 0 is 'A', 1 is 'B,' etc. You should get the first word of the ciphertext given in the example, 'GXSSB.'

(e) According to the proposition, the decryption function is $D_{3,11}(x) = (cx + d)$ %26, where c is the inverse of 3 mod 26 and d is $-11c$ %26. Check that $c = 9$ and $d = 5$.

(f) Decrypt your encoded ciphertext (the list of numbers from 1c) by applying the function $D_{3,11}(x) = (9x + 5)$ %26 to each number. You should recover the encoded plaintext from 1b.

2. (a) Why is a brute-force ciphertext-only attack harder for the affine cipher than for the shift cipher?

(b) What kind of attack is likely to succeed against an affine cipher?

3. What struck you in this reading? What is still unclear? What remaining questions do you have?