CIS 3362 Homework #2A: Substitution Cipher, Vigenere Solutions

Part A: Written Questions Similar to Quiz/Exam Questions

1) Find 183^{-1} mod 251.

$251 = 183(1) + 68$ $\quad 68 = 251 - 183(1)$
$183 = 68(2) + 47$ $\quad 47 = 183 - 68(2)$
$68 = 47(1) + 21$ $\quad 21 = 68 - 47(1)$
$47 = 21(2) + 5$ $\quad 5 = 47 - 21(2)$
$21 = 5(4) + 1$
$1 = 21 - 5(4)$
$1 = 21 - (47 - 21(2))(4)$
$1 = 21(9) - 47(4)$
$1 = (68 - 47(1))(9) - 47(4)$
$1 = 68(9) - 47(13)$
$1 = 68(9) - (183 - 68(2))(13)$
$1 = 68(35) - 183(13)$
$1 = \big(251 - 183(1)\big)(35) - 183(13)$
$1 = 251(35) - 183(48)$
$1 \equiv 183(-48)\ mod\ 251$
$1 \equiv 183(-48) + 183(251)\ mod\ 251$
$1 \equiv 183(203)\ mod\ 251$

$183^{-1}\ mod\ 251 = 203$

2) For an affine cipher, we know that the ciphertext ‘X’ maps to the plaintext ‘X’ and the ciphertext ‘W’ maps to the plaintext ‘E’. Determine both the decryption AND encryption functions. Both answers must be in the form f(x) = (ax + b) mod 26, where a and b are in between 0 and 25, inclusive.

Decryption

$f(x) \equiv ax + b \ (mod\ 26)$
$23 \equiv a * 23 + b \ (mod\ 26)$
$b \equiv 23 - a * 23 \ (mod\ 26)$
$4 \equiv a * 22 + b \ mod\ 26$
$b \equiv 4 - a * 22 \ (mod\ 26)$
$4 - a * 22 \equiv 23 - a * 23 \ (mod\ 26)$
$4 + a \equiv 23 \ (mod\ 26)$
$a = 19$
$4 \equiv (19 * 22 + b) \ (mod\ 26)$
$4 \equiv 418 + b \ (mod\ 26)$
$4 \equiv 2 + b \ (mod\ 26)$
$b = 2$

$f(x) = (19\text{x} + 2) \bmod 26$

Check:
$(19 * 23 + 2) \ mod\ 26 = 23$
$(19 * 22 + 2) \ mod\ 26 = 4$

Here, we verify that ciphertext 'W' (22) decrypts to plaintext 'E' (4).

Encryption

$f(x) = (19\text{x} + 2) \bmod 26$
$x \equiv 19\big(f(x)\big) + 2 \ (mod\ 26)$
$x + 24 \equiv 19\big(f(x)\big) \ (mod\ 26)$
$19 * 11 \equiv 1 \ (mod\ 26)$
$11 * (x + 24) \equiv 11 * (19\big(f(x)\big) \ (mod\ 26)$
$11x + 264 \equiv f(x) \ (mod\ 26)$

$f(x) = (11x + 4) \bmod 26$

Check:
$(11 * 23 + 4) \ mod\ 26 = 23$
$(11 * 4 + 4) \ mod\ 26 = 22$

Here we verify that plaintext 'E'(4) encrypts to ciphertext 'W' (22)

3) For an alphabet of size 96, how many possible keys would there be to the affine cipher? (Hint: Use logic and the inclusion-exclusion principle to more quickly determine the possible values of a, instead of listing them out one by one!)

Valid keys for this affine cypher consist of all a such that gcd(a, 96) = 1. This means that all a-values cannot share any common factors with 96. The prime factorization of 96 is:

$$96 = 2 * 2 * 2 * 2 * 2 * 3$$

This means that any numbers that are a multiple of 2 or 3 will not work as a-values for our alphabet, and we can exclude them from our possible values.

Let's use the inclusion-exclusion principle to count the number of integers from 1 to 96 that are divisible by 2 or 3. Let A be the set of values divisible by 2 in the range and B be the set of values divisible by 3. There are 96/2 = 48 values divisible by 2. There are 96/3 = 32 values divisible by 3. BUT, there are some numbers divisible by both 2 and 3. These are values divisible by 6. Since we these were added twice, in each of the two previous groups, we must subtract these out. There are 96/6 = 16 integers in the range divisible by 6. Thus, there are

48 + 32 – 16 = 64 integers in between 1 and 96 inclusive that are either divisible by 2 or 3. It follows that there are 96 – 64 = 32 integers in the given range that are relatively prime with 96.

This leaves us with 32 possible working a-values, along with the 96 possible working b-values. Multiply these together to get 32*96 = 3072 possible affine keys.

4) Let x be a positive integer. A set of letters consists of 50 As, 25 Bs, 5 Cs, 45 Ds, and 75 Es. What is the index of coincidence of the set? **Leave your answer as a fraction in lowest terms.**

$$IC = \sum_{i=1}^{5} \frac{f_i(f_i - 1)}{n(n-1)}$$

$$n = 50 + 25 + 5 + 45 + 75 = 200$$

$$IC = \frac{50(49)}{200(199)} + \frac{25(24)}{200(199)} + \frac{5(4)}{200(199)} + \frac{45(44)}{200(199)} + \frac{75(74)}{200(199)}$$

$$IC = \frac{50(49) + 25(24) + 5(4) + 45(44) + 75(74)}{200(199)}$$

$$IC = \frac{2450 + 600 + 20 + 1980 + 5550}{200(199)}$$

$$IC = \frac{10600}{200(199)} = \frac{106\cancel{(100)}}{398\cancel{(100)}} = \frac{53\cancel{(2)}}{199\cancel{(2)}}$$

$$IC = \frac{53}{199}$$

5) The set of letters S consists of 5 As, 15 Bs, 25 Cs, 30 Ds, and 25 Es. The set of letters T consists of 30 As, 26 Bs, 4 Cs, 16 Ds and 24 Es. What is the mutual index of coincidence between sets S and T? **Leave your answer as a fraction in lowest terms.**

$$MIC = \sum_{i=1}^{5} \frac{S_i T_i}{n_S n_T}$$

$$n_S = \sum_{i=1}^{5} S_i = 5 + 15 + 25 + 30 + 25 = 100$$

$$n_T = \sum_{i=1}^{5} T_i = 30 + 26 + 4 + 16 + 24 = 100$$

$$MIC = \frac{5(30)}{100^2} + \frac{15(26)}{100^2} + \frac{25(4)}{100^2} + \frac{30(16)}{100^2} + \frac{25(24)}{100^2}$$

$$MIC = \frac{5(30) + 15(26) + 25(4) + 30(16) + 25(24)}{100^2}$$

$$MIC = \frac{150 + 390 + 100 + 480 + 600}{100^2}$$

$$MIC = \frac{1720}{10000}$$

$$MIC = \frac{172\cancel{(10)}}{1000\cancel{(10)}}$$

$$MIC = \frac{172\cancel{(10)}}{1000\cancel{(10)}}$$

$$MIC = \frac{43\cancel{(4)}}{250\cancel{(4)}}$$

$$MIC = \frac{43\cancel{(4)}}{250\cancel{(4)}}$$

$$MIC = \frac{43}{250}$$