CIS 3362 Homework #2: Classical Ciphers - Written Problems

Due: Check WebCourses for the due date.

Directions: To be done individually. (Sorry, I just realized it would be a bit silly to assign this in groups...it would short change students the opportunity to practice for the first exam since these are questions extremely similar to exam questions...)

1) Prove that encrypting a plaintext with two successive affine cipher keys is no more secure than encrypting a plaintext with a single set of affine cipher keys.

2) Find 148^{-1} mod 327.

3) For an alphabet of size 79, a set of affine encryption keys is a = 46, b = 22. (Thus the encryption function is f(x) = (46x + 22) % 79.) Determine the corresponding set of decryption keys.

4) A set of letters consists of 20 As, 35 Bs, 40 Cs, 5 Ds, 10 Es, and 50 Fs. What is the index of coincidence of the set?

5) The set of letters S consists of 15 As, 25 Bs, 35 Cs, 15 Ds, and 10 Es. The set of letters T consists of 60 As, 25 Bs, 15 Cs, 20 Ds and 40 Es. What is the mutual index of coincidence between sets S and T? **Leave your answer as a fraction in lowest terms.**

6) Encrypt the plaintext "FOOTBALLGAMEONTHURSDAY" using the Vigenere cipher and the keyword "KNIGHTS". (For practice for the first exam, do this by hand with a chart with the values of the letters.)

7) Encrypt the message, "WHENWALLSCOMEDOWNEVERYONEWINS" using the Playfair cipher with the key "BRICKS" and the padding character "X". (Please do NOT use a program to do this.)

8) Decrypt the message, "ABEPCLCFWNAMNX", which was enciphered using the Playfair cipher with the key "TURTLES". Note: The padding character used was "Q". (Please do NOT use a program to do this.)