Fall 2020 CIS 3362 Quiz #1 Part A: Shift, Affine, Extended Euclidean Algorithm Solutions

Date: 9/9/2020

1) (9 pts) Encrypt the plaintext "HOWAREYOU" using the shift cipher with the key = 11.

Solution
H = 7 + 11 = 18 = S
O = 14 + 11 = 25 = Z
W = 22 + 11 = 33 % 26 = 7 = H
A = 0 + 11 = 11 = L
R = 17 + 11 = 28 % 26 = 2 C
E = 4 + 11 = 15 = P
Y = 24 + 11 = 35 % 26 = 9 J
O = 14 + 11 = 25 = Z
U = 20 + 11 = 31 % 26 = 5 F

Ciphertext is **SZHLCPJZF.** **(Grading: 1 pt per letter.)**

2) (5 pts) Consider an Affine cipher for an alphabet with 42 symbols. How many possible encryption keys would there be for the Affine cipher on an alphabet of this size?

Solution
There are 42 possible values for b.
Now, we must find how many values of a are possible. These are all integers from 1 to 42 that do not share any common factors with 42. We can list these out via exhaustive search and noting that 42 = 2 x 3 x 7, so we should exclude any multiples of 2, 3 and 7. The values remaining when we remove these multiples are:

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37 and 41.

There are 12 of these values.

It follows that there are a total of 42 x 12 = **504** possible keys for an Affine Cipher on an alphabet of size 42.

Grading: 1 pt for 42, 1 pt for multiplying, 3 pts for possible values of a.

3) (5 pts) The encryption function for an Affine Cipher (in English) is f(x) = (19x + 3) mod 26. What is the corresponding decryption function, $f^{-1}(x)$? (Please make use of the reference sheet to speed up your work.)

Solution
Switch x and y and solve for y:

$x \equiv (19y + 3) \bmod 26$
$(x-3) \equiv 19y \bmod 26$

Using the mod inverse chart, we find that 19^{-1} mod 26 is 11:

$11(x-3) \equiv 11(19y) \bmod 26$
$11x - 33 \equiv y \pmod{26}$
$y \equiv (11x + 19) \bmod 26$

Thus, the corresponding decryption function is **$f^{-1}(x) = (11x + 19) \bmod 26$.**

Grading: 1 pt switch x&y, 1 pt subtract 3, 1 pt mod inverse look up, 1 pt multiply out, 1 pt remap -33.

4) (6 pts) Determine the greatest common divisor of 336 and 142 using the Euclidean Algorithm.

Solution
336 = 2 x 142 + 52
142 = 2 x 52 + 38
52 = 1 x 38 + 14
38 = 2 x 14 + 10
14 = 1 x 10 + 4
10 = 2 x 4 + 2
4 = 2 x 2
Thus, GCD(336, 142) = 2.
Grading: 1 pt per step.