

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

Date: 9/9/2020

Directions: Please use the reference sheet, your course notes and a calculator as aids for this exam. Do NOT attempt to look up information online. Even if you use a calculator, show each step of your calculations that you would do by hand. The role of the calculator will simply be to speed up individual calculations (13 x 29, for example), not to skip whole steps, as these steps are typically awarded points in the grading criteria.

Please either type your answers or write them on paper and scan that to .pdf. The accepted file types for submission will be .doc, .docx, .txt and .pdf. I recommend that you directly type into the posted document to save time scanning, and either use the equation editor or type out the necessary math in text.

Please look at Webcourses to see when your due time and late due time are. It's recommended that you stop working at the due time and start uploading at that time. Anything turned in before the late due time will be accepted for full credit. Anything that doesn't make it in by the late due time will earn a 0. A 10 minute buffer will be provided after both due times. Please don't take advantage of these buffers as it's an unnecessary risk.

- 1) (9 pts) Encrypt the plaintext "HOWAREYOU" using the shift cipher with the key = 11.
- 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?
- 3) (5 pts) The encryption function for an Affine Cipher (in English) is $f(x) = (19x + 3) \bmod 26$. What is the corresponding decryption function, $f^{-1}(x)$? (Please make use of the reference sheet to speed up your work.)
- 4) (6 pts) Determine the greatest common divisor of 336 and 142 using the Euclidean Algorithm.