**FUNDAMENTALS OF CYPTOGRAPHY ASSIGNMENT 01 (SEM 1, 2020)  
NICHOLAS KLVANA-HOOPER, 19/04/2020**

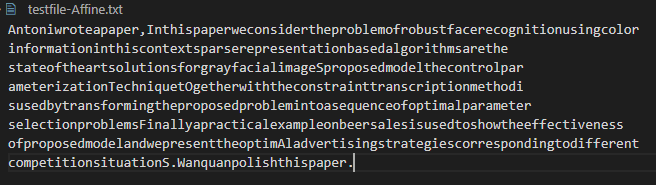
**All possible keys for Affine**

With format (a, b). Eligible keys:  
(1,0), (1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (1,7), (1,8), (1,9), (1,10), (1,11), (1,12), (1,13), (1,14), (1,15), (1,16), (1,17), (1,18), (1,19), (1,20), (1,21), (1,22), (1,23), (1,24), (1,25), (1,26)  
(2,0), (2,1), (2,2), (2,3), (2,4), (2,5), (2,6), (2,7), (2,8), (2,9), (2,10), (2,11), (2,12), (2,13), (2,14), (2,15), (2,16), (2,17), (2,18), (2,19), (2,20), (2,21), (2,22), (2,23), (2,24), (2,25), (2,26)  
(4,0), (4,1), (4,2), (4,3), (4,4), (4,5), (4,6), (4,7), (4,8), (4,9), (4,10), (4,11), (4,12), (4,13), (4,14), (4,15), (4,16), (4,17), (4,18), (4,19), (4,20), (4,21), (4,22), (4,23), (4,24), (4,25), (4,26)  
(5,0), (5,1), (5,2), (5,3), (5,4), (5,5), (5,6), (5,7), (5,8), (5,9), (5,10), (5,11), (5,12), (5,13), (5,14), (5,15), (5,16), (5,17), (5,18), (5,19), (5,20), (5,21), (5,22), (5,23), (5,24), (5,25), (5,26)  
(7,0), (7,1), (7,2), (7,3), (7,4), (7,5), (7,6), (7,7), (7,8), (7,9), (7,10), (7,11), (7,12), (7,13), (7,14), (7,15), (7,16), (7,17), (7,18), (7,19), (7,20), (7,21), (7,22), (7,23), (7,24), (7,25), (7,26)  
(8,0), (8,1), (8,2), (8,3), (8,4), (8,5), (8,6), (8,7), (8,8), (8,9), (8,10), (8,11), (8,12), (8,13), (8,14), (8,15), (8,16), (8,17), (8,18), (8,19), (8,20), (8,21), (8,22), (8,23), (8,24), (8,25), (8,26)  
(10,0), (10,1), (10,2), (10,3), (10,4), (10,5), (10,6), (10,7), (10,8), (10,9), (10,10), (10,11), (10,12), (10,13), (10,14), (10,15), (10,16), (10,17), (10,18), (10,19), (10,20), (10,21), (10,22), (10,23), (10,24), (10,25), (10,26)  
(11,0), (11,1), (11,2), (11,3), (11,4), (11,5), (11,6), (11,7), (11,8), (11,9), (11,10), (11,11), (11,12), (11,13), (11,14), (11,15), (11,16), (11,17), (11,18), (11,19), (11,20), (11,21), (11,22), (11,23), (11,24), (11,25), (11,26)  
(13,0), (13,1), (13,2), (13,3), (13,4), (13,5), (13,6), (13,7), (13,8), (13,9), (13,10), (13,11), (13,12), (13,13), (13,14), (13,15), (13,16), (13,17), (13,18), (13,19), (13,20), (13,21), (13,22), (13,23), (13,24), (13,25), (13,26)  
(14,0), (14,1), (14,2), (14,3), (14,4), (14,5), (14,6), (14,7), (14,8), (14,9), (14,10), (14,11), (14,12), (14,13), (14,14), (14,15), (14,16), (14,17), (14,18), (14,19), (14,20), (14,21), (14,22), (14,23), (14,24), (14,25), (14,26)  
(16,0), (16,1), (16,2), (16,3), (16,4), (16,5), (16,6), (16,7), (16,8), (16,9), (16,10), (16,11), (16,12), (16,13), (16,14), (16,15), (16,16), (16,17), (16,18), (16,19), (16,20), (16,21), (16,22), (16,23), (16,24), (16,25), (16,26)  
(17,0), (17,1), (17,2), (17,3), (17,4), (17,5), (17,6), (17,7), (17,8), (17,9), (17,10), (17,11), (17,12), (17,13), (17,14), (17,15), (17,16), (17,17), (17,18), (17,19), (17,20), (17,21), (17,22), (17,23), (17,24), (17,25), (17,26)  
(19,0), (19,1), (19,2), (19,3), (19,4), (19,5), (19,6), (19,7), (19,8), (19,9), (19,10), (19,11), (19,12), (19,13), (19,14), (19,15), (19,16), (19,17), (19,18), (19,19), (19,20), (19,21), (19,22), (19,23), (19,24), (19,25), (19,26)  
(20,0), (20,1), (20,2), (20,3), (20,4), (20,5), (20,6), (20,7), (20,8), (20,9), (20,10), (20,11), (20,12), (20,13), (20,14), (20,15), (20,16), (20,17), (20,18), (20,19), (20,20), (20,21), (20,22), (20,23), (20,24), (20,25), (20,26)  
(22,0), (22,1), (22,2), (22,3), (22,4), (22,5), (22,6), (22,7), (22,8), (22,9), (22,10), (22,11), (22,12), (22,13), (22,14), (22,15), (22,16), (22,17), (22,18), (22,19), (22,20), (22,21), (22,22), (22,23), (22,24), (22,25), (22,26)  
(23,0), (23,1), (23,2), (23,3), (23,4), (23,5), (23,6), (23,7), (23,8), (23,9), (23,10), (23,11), (23,12), (23,13), (23,14), (23,15), (23,16), (23,17), (23,18), (23,19), (23,20), (23,21), (23,22), (23,23), (23,24), (23,25), (23,26)  
(25,0), (25,1), (25,2), (25,3), (25,4), (25,5), (25,6), (25,7), (25,8), (25,9), (25,10), (25,11), (25,12), (25,13), (25,14), (25,15), (25,16), (25,17), (25,18), (25,19), (25,20), (25,21), (25,22), (25,23), (25,24), (25,25), (25,26)  
(26,0), (26,1), (26,2), (26,3), (26,4), (26,5), (26,6), (26,7), (26,8), (26,9), (26,10), (26,11), (26,12), (26,13), (26,14), (26,15), (26,16), (26,17), (26,18), (26,19), (26,20), (26,21), (26,22), (26,23), (26,24), (26,25), (26,26)

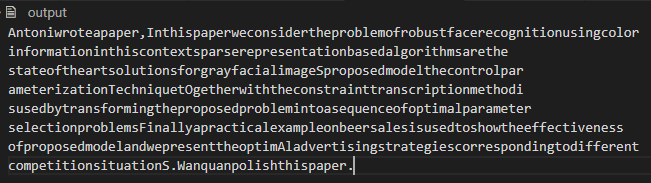
B is able to be any number between 0 and 26 inclusive as it has to be modded by 27. A can be any number between 1 and 26 inclusive that is not divisible by 3. This is because A has to be coprime with 27 and 3 is a common factor that occurs so therefore cannot be used.  
This gives us a total of 486 possible keys to use for the affine cipher.

**Showing that affine code works**

Original test file:

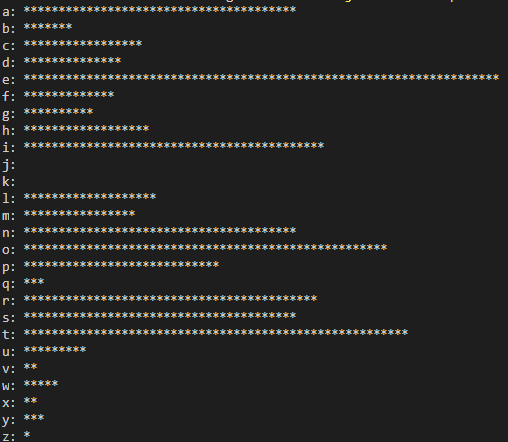
****

Encrypted then decrypted file:



Both files are exactly the same, therefore the plaintext is recovered.

**Letter distribution graph of test file**



**Skipping non-letter symbols**

To skip non-letter symbols the code has an if statement that only affects characters that have a value that represents a capital or lower-case alphabet character. In this way any other character will not be affected.

**DES Pseudocode**

**Encrypt/Decrypt Stage**

* Plain text is imported as binary
* Permutate it with the IP array
* Break it into left and right strings
* Make left equal to the previous right, and right function xor’ed with previous left becomes the new right
* Get left and right switched
* Permutate the switched block with IP\_I
* Change binary back to hex

R function Stage

* Permutate right side with E
* XOR the right side with the current key (1-16)
* Go through 8 S\_Box permutations
  + Use first and last bit to determine what row
  + Use the rest of the bits to determine what column
  + Use these row and col to find S\_BOX value to replace the part of the string
* Permutate the S\_box-replaced-phrase with P

Switch Stage

* Take in right and left substrings
* Switch it so right substring appears first

**Main issue of programming with DES**

Main difficulty with programming the code was determining whether or not the encryption was doing the right thing as its not until you try decrypting that you can see if it works.