Aaron Hong
Prof. Poovendiran
EE 418 AU23
HW3 11/3/23

2. a. $754x + 233y = 1$, $754x = 1 \bmod 233$, $233y = 1 \bmod 754$

$754 = 3(233) + 55$
$233 = 4(55) + 13$
$55 = 4(13) + 3$
$13 = 4(3) + 1$
$3 = 3(1) + 0$

$1 = 13 - 4(3)$
$13 = 233 - 4(55)$
$1 = 233 - 4(55) - 4(3)$
$= 233 - 4(58)$
$55 = 4(4(3)+1) + 3$
$3 = 55 - 4(13)$
$1 = 13 - 4(55 - 4(13))$
$= 13 - 4(55) + 16(13)$
$= 17(13) - 4(55)$
$13 = 233 - 4(55)$
$1 = 17(233 - 4(55)) - 4(55)$
$1 = 17(233) + 68(55) - 4(55)$
$1 = 17(233) - 72(55)$
$55 = 754 - 3(233)$
$1 = 17(233) + 72(754 - 3(233))$
$= 17(233) + 216(233) + 72(754)$
$= 233(233) - 72(754)$

$x = -72, y = 233$

b. $754^{-1} \bmod 233 = -72$
$754(-72) = 1 \bmod 233$
$233^{-1} \bmod 754 = 233$
$233(233) = 1 \bmod 754$

3. a. $K_1 = \begin{matrix} 1 & 3 \\ 0 & 1 \end{matrix}$ $K_2 = \begin{matrix} 2 & 1 \\ 1 & 0 \end{matrix}$ $K_{12} = \begin{matrix} 5 & 1 \\ 1 & 0 \end{matrix}$

$K = \begin{matrix} 35 & 7 \\ 7 & 0 \end{matrix}$, $b = 2$ $\rightarrow$ $K = \begin{matrix} 2 & 7 \\ 7 & 0 \end{matrix}$

b. $K_{12} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \frac{1}{-1}\begin{pmatrix} 0 & -1 \\ -1 & 5 \end{pmatrix} = \begin{matrix} 0 & 1 \\ 1 & -5 \end{matrix}$

$-49^{-1} \bmod 11 \begin{pmatrix} 0 & -7 \\ -7 & 2 \end{pmatrix} = \begin{matrix} 0 & 0 \\ -14 & 4 \end{matrix} \begin{matrix} -14 & -3 \\ -3 & 4 \end{matrix} = \begin{matrix} 0 & 8 \\ 8 & 4 \end{matrix}$

4. a. if encrypted by shift cipher, the encoded message will also be 1 letter repeated. however, the key and letter cannot be deciphered
b. the affine cipher will have the same effect as shift in that the encoded message will always be the same letter. the key and letter cannot be deciphered.
d. the eavesdropper will only know the length of the key but they won't be able to deduce that the plaintext letter is A
c. they will be able to deduce that it is one repeated letter because the ciphertext will repeat itself every two letters. The key + letter cannot be deduced.

5. plain: 1 0 1 1 0 0 1 0 1 1 0 0 1 0 1
cph: 1 1 1 0 1 1 1 1 0 1 0 0 0 1 0
key: 0 1 0 1 1 1 0 1 1 0 0 0 1 1 1

$z_{i+5} = z_{i+4} + z_{i+3} + z_{i+2} + z_{i+1} + z_i$

8 ABCBABBAACBA → distance 7 (5 → 10)

5/12 : A, 5/12 : B, 2/12 : C

y_1 : ACABAB
y_2 BBBACA

y_1 : ABBC
y_2 BAAB
y_3 CBAA

$1/4 + 1/9 + 1/36 = 14/36 = 7/18$

$25/144 + 25/144 + 4/144 = 54/144 = 27/72 \approx 7/18$

key length probably 2, value 01
no way the ciphertext is the same as plaintext... right?