Kelli Kinnikin

a.) E = M X -K -> C

* M: plain text string with letters A-Z before any encryption is applied
* K: key shift
* C: cipher text that is shifted the specific number of places depending on the value of k
* If it is a left shift, it is – the key shift
* If it is a right shift, it is + the key shift
* For this example: M - 3 -> C (key shift left of 3) to get the encrypted cipher text

D = C X K -> M (when decrypted you do the inverse of the key that you encrypted with)

* This general formula will give you the correct decoded message for this example
  + If it is a left shift, it is – the key shift
  + If it is a right shift, it is + the key shift
  + For this example: C + 3 -> M (inverse of our left (so negative) 3, we need to add 3 to get the inverse) to get the original plain text before any encryption

b.) E = M X K -> C **we want to take the mod for these because it can loop back around when it gets to the end of the key space (letter Z)**

* + M: plain text string with letters A-Z
  + K: key shift
  + C: cipher text that is then shifted “k” letters which is 13 in this case
  + For this example: M + 13 -> C

(M +13) % 26 -> C

D = C X -K ->M (when decrypted you do the inverse of the key that you encrypted with)

* M: original plain text letter
* K: key shift of -13
* C: cipher text letter that has been encrypted
* For this example: C -13 -> M (inverse of +13 is -13 to get the original letter before the message was encrypted) (C -13) %26 -> M