Air Force Institute of Technology
Department of Electrical and Computer Engineering
Cryptography and Data Security (CSCE 544)
Homework #2

April 11, 2019
Micah Hayden

[100 Points] Implement the encryption an decryption functions in Python for an Affine Cipher that takes as input the corresponding ciphertext/plaintext, and arbitrary alphabet A such that $26 \leq |A| \leq 256$. Make sure that the cipher implementation warns users about invalid inputs.

[40 Points] Consider an unfair coin where the two outcomes, heads and tails have probabilities $p(\boldsymbol{heads}) = p$ and $p(\boldsymbol{tails}) = 1 - p$

(a) If the coin is flipped two times, what are the possible outcomes along with their respective probabilities?

(b) Show that the entropy in part (a) is $-2p\log_2(p) - 2(1-p)\log_2(1-p)$. How could this have been predicted without calculating probabilites in part (a)?

[60 Points] Decipher the following ciphertext using ciphertext-only cryptanalysis. Note the alphabet used to create is this ciphertext is as following: [abcdefghijklmnopqrstuvwxyz]

[30 Points] Ciphertext #1 (Affine)

```
azwcwlugblyciuohxfoxaiallcsrrwhxobzzupubzxfuewbcxaxsxawbwpxfusbaxu
zcxoxucokoabcxollubugaucpwhuakbobzzwgucxaexfoxaialljuohxhsupoaxfob
zollukaobeuxwxfucoguxfoxaxoquxfacwjlakoxawbphuulyiaxfwsxobygubxolh
ucuhnoxawbwhrshrwcuwpunocawbobzxfoxaialliullobzpoaxfpsllyzacefohkux
fuzsxaucwpxfuwppaeuwbifaefaogojwsxxwubxuhcwfulrguk
```

[20 Points] Ciphertext #2 (Vigenère)

```
kvqkqdgepdakywcjvzclkokdnkwhrgtlcffvgxgffljwegpkvavmvaqfqxvzgmpavwfkvsvwus
iskfulcdnwpwoagkhgtwkypspvfgowulkuvzclkokdntgstltmgxcavzcffsndgykspuglqljwuso
wcffljsvayandqtgqvzggtvgjughljwrjgkkvgfvghljwwfklgvulclgkcffljwqjfwtkqxvzgghxku
gjusrhqaplgvqngjowcuegtvkfilqjgywdclkgpkcffljwwfkxqjouqvgghekdklcjabwkvaewugj
wnhowigf
```

[10 Points] Ciphertext#3 (Vigenère)

```
ujltkvbpxowvvcoqcubiubrkjofvtlpwvbuwplxtvkpytvkflnbzqxdcqgkqeqxuykbvlturvpxtw
dmcepwwjvlunrpmvtqrsflocuzcqerobkqujduarvyrvngujlomqpvkjpjxcvxtroizjvkjvlohddv
qpvkjpjjuzsqqhylujlukwjukjikmaxowvvcoujrviktvxealucqevkjpnbdrvvludxuarvuwjnonc
boqwgkqecqzvkjpjpfgcwwjhbpwzptnbvlucejvbpwpjikuhlofrvvwsawpfrtqzjvkpwwbpbdq
ddjloi
```