CS411 Cryptography HW 1

Samuel Lee

ID: 24774

Due: 10/13/19

1. For Question number 1, the Caesar/Shift cipher is a simple encryption/decryption method where you shift all the characters of the message by a constant number. Therefore, in the English alphabet, there are only 26 possible shifts that can happen. So, in the code, I tried all the possible shifts, and if that shift led to any number greater than the number representation of the letter, I used the modulo to find its value, and appended all the possible outcomes to a list. There were only 26 possibilities, so I just used exhaustive search and found the correct decryption in the list.
   The answers are : FROG, COLD
2. In the affine cipher, there are two input values in the function that converts the message to the encryption/decryption. Because the alpha/theta values must follow the condition gcd(alpha, 26), I found the possible number values. Beta/gamma values must be any number between 0 and 26, so I create a list of numbers. Then, I used the given functions in the hwhelper.py to insert the values into the affine cipher decryption algorithm, and appended the possible values to a list, where I found the correct encryption.
   The answers are: A successful man is one who can lay a firm foundation with the bricks others have thrown at him
3. For question number 3, we were given 31 possible characters that were to be encrypted/decrypted. However, since they were bigrams, there were a total of 31*31 or 31^2 possible bigram characters. Therefore, the alpha/theta values are all possible values that meet the condition gcd(alpha, 31*31), which listed to about 930 values. Then, the beta/gamma values consist of all integers between 0 and 31*31. Because there are now over 31*31 possible bigram character sets, the modulo value was also set to 31*31. The total key space will be the number of gcd(alpha, 31*31) multiplied with 31*31 (key space= 930 * (31*31)).
   Modulus: 31*31
   Key Space: 930 * Modulus
4. The implementation of the algorithm for the affine cipher is similar to question number 2, just with different values including the alpha/theta, beta/gamma and modulo values. It was required to use brute force, and all possible texts were appended to the list. We were able to narrow it down, and find the correct encrypted message.
   Answer: THOSE WHO BELIEVE IN TELEKINETICS, RAISE MY HAND.
5. The vigenere cipher is similar to the shift cipher, yet it number shifts is dependent on the length of the key, and the values inside that key. For our example, the key was “SANITY”, which consisted of 6 letters. Therefore, I used the number representation of each letter in the key, and repeated the use of the key in a loop when we had used every letter of the key. In the actual implementation, the position values of the key was found using a simple for loop, and added to a list. Then, for the actual decryption, the implementation was similar to the shift cipher, except the number representation of the letter of encrypted text was subtracted with the position values of the key, and that key was used in repetition using a modulo function.

Answer: I REFUSE TO ANSWER THAT QUESTION ON THE GROUNDS THAT I DON’T KNOW THE ANSWER.