CS411-HW1

Ahmet Furkan Ün

October 27, 2023

Question 1

In this question, I tried to decrypt using a brute force method. I tried to subtract every number from 0 to 26 from the characters of the ciphertext. Based on my observations, if I subtract 11 from all characters of the ciphertext, the plaintext will be 'CAESAR'

Question 2

In this task, I was presented with a ciphertext encrypted using the Affine Cipher over the Z_26 alphabet, and I was given a hint that the most frequent letter in the plaintext is 'T'. First, I created a letter_count dictionary to keep track of the occurrences of each letter in the ciphertext. I analyzed the ciphertext and observed that 'a' and 'r' were the most frequently occurring letters. I speculated that these letters might correspond to 'T' in the plaintext.

To recover the encryption and decryption keys, I employed the Affine Cipher decryption function given in helper.py. But the function requires the keys to try. To find the possible α and the β values to try, I then iterated through possible values for the α from the set [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25] since the α value should be relatively prime to 26. To determine β values, I used the known plaintext-ciphertext pairs.
$\beta = (lowercase['a'] - lowercase['t'] * \alpha)$ mod 26
$\beta = (lowercase['r'] - lowercase['t'] * \alpha)$ mod 26
After finding the α and the β values, I run the decryption function to get the decrypted texts.

For 'a' to 't', I found that when α is 11 and β is 25, the decrypted text was meaningful. The result was: 'I did not fail the test. I just found three hundred eleven ways to do it wrong.'

Question 3

We are dealing with bigrams. Therefore there are $30 * 30 = 900$ combinations of bigrams. The modulus should be 900.

When it comes to the key space, we can say that the possible α values are the ones who are relatively prime to the 900. This makes the key space for a as 240 as I calculated in my python notebook. β can be any number between 0 and 899. Therefore there are 900 possible β values.

Considering the possible number of α and β values, the key space for this new affine cipher will be $240 * 900 = 216000$ which is quite large compared to conventional affine cipher.

Question 4

Despite having a larger key space, we can not say that affine cipher defined in question (3) secure against the letter frequency analysis. It is possible to perform bigram frequency analysis which is like letter frequency analysis, but applied to pairs of letters. For example, in English, some bigrams are very common, like "TH" or "IN." Attackers could use this knowledge to spot patterns in the ciphertext. If they notice certain bigrams appearing often, they might guess parts of the key.

Question 5

To decrypt the ciphertext, the first thing I did was creating a new dictionary of letters for our new 30 letter alphabet. After that I created a dictionry containing every biagram and its corresponding encrypted numerical value, also with the inverse of it. These two dictionaries acted as the dictionary of letters and their corresponding sequence numbers for regular affine cipher.

After that we know from the hints that the plaintext is a sentence that ends with a dot and the length of the plaintext is an odd number. By combining these two information, I concluded that the "SW" in ciphertext is equal to ".X" in the plaintext since the plaintext ends with dot and has odd number of characters.

Similar to the Question 2, I try to decrypt the ciphertext for every α in the list I generated in Question 3. For every α value, I calculated the β value using the known plaintext-ciphertext pair. $\beta = (bigrams['SW'] - bigrams['.X'] * \alpha) \bmod 900$

The rest of the solution is very similar to Question 2. After examining all 240 possible decryptions, I decided that the only meaningful text was "SING, GODDESS, OF THE ANGER OF ACHILLES, SON OF PELEUS." for $\alpha = 91$ and $\beta = 389$

Question 6

Consider the probability of a specific ciphertext letter β, denoted as $p\beta$. Since every letter in the plaintext is shifted randomly and independently by a uniform distribution from 0 to 28, the probability of shifting any given letter in the plaintext to a specific ciphertext letter β is the same for all β.

Therefore, $p\beta$ is independent of the values of $p\alpha$ (the probabilities of each letter in the plaintext). It's solely dependent on the fact that the shift is random and uniform. The probability of shifting any plaintext letter to β is $1/29$, as each of the 29 possible shifts is equally likely.

Question 7

At first, I put the letters of the ciphertext to a Pandas DataFrame. By doing that, I will be able to quickly shift the letters and check the number of coincidences. I checked for the shift amounts from 1 to 100. After sorting the shift amounts by their number of coincidences, I saw that all high coincidence shifts are the multiples of 5.

Shift Amount	**# of Coincidences**
60	83
85	82
10	81
30	81
35	74

At this point I was almost sure that the key length is 5 since the greatest common divisor of the shift amounts in the table is 5. After finding the key size, I split the ciphertext with grouping index mod 5, in other words, I combined all the letters having the same shift amount. To do that, again I used a DataFrame having 5 columns which are the modulo values of 5 and 216 letters in each column. Then I performed a frequency analysis on each column. I get the most frequent 2 letters from each column and expecting them to be the 'E' in plaintext to find the shift amounts and keys. Then I created a list of all possible combinations of these keys a total of 32 keys.

Then I tried to decrypt the text for each possible key. I observed that for key "MGVDB" the decrypted text is meaningful.

THE CENTRIPETAL FORCE ON OUR PLANET IS STILL FEARFULLY STRONG, ALYOSHA. I HAVE A LONGING FOR LIFE, AND I GO ON LIVING IN SPITE OF LOGIC. THOUGH I MAY NOT BELIEVE IN THE ORDER OF THE UNIVERSE, YET I LOVE THE STICKY LITTLE LEAVES AS THEY OPEN IN SPRING. I LOVE THE BLUE SKY, I LOVE SOME PEOPLE, WHOM ONE LOVES YOU KNOW SOMETIMES WITHOUT KNOWING WHY. I LOVE SOME GREAT DEEDS DONE BY MEN, THOUGH I'VE LONG CEASED PERHAPS TO HAVE FAITH IN THEM, YET FROM OLD HABIT ONE'S HEART PRIZES THEM. HERE THEY HAVE BROUGHT THE SOUP FOR YOU, EAT IT, IT WILL DO YOU GOOD. IT'S FIRST-RATE SOUP, THEY KNOW HOW TO MAKE IT HERE. I WANT TO TRAVEL IN EUROPE, ALYOSHA, I SHALL SET OFF FROM HERE. AND YET I KNOW THAT I AM ONLY GOING TO A GRAVEYARD, BUT IT'S A MOST PRECIOUS GRAVEYARD, THAT'S WHAT IT IS. PRECIOUS ARE THE DEAD THAT LIE THERE, EVERY STONE OVER THEM SPEAKS OF SUCH BURNING LIFE IN THE PAST, OF SUCH PASSIONATE FAITH IN THEIR WORK, THEIR TRUTH, THEIR STRUGGLE AND THEIR SCIENCE, THAT I KNOW I SHALL FALL ON THE GROUND AND KISS THOSE STONES AND WEEP OVER THEM; THOUGH I'M CONVINCED IN MY HEART THAT IT'S LONG BEEN NOTHING BUT A GRAVEYARD. AND I SHALL NOT WEEP FROM DESPAIR, BUT SIMPLY BECAUSE I SHALL BE HAPPY IN MY TEARS, I SHALL STEEP MY SOUL IN EMOTION. I LOVE THE STICKY LEAVES IN SPRING, THE BLUE SKY - THAT'S ALL IT IS. IT'S NOT A MATTER OF INTELLECT OR LOGIC, IT'S LOVING WITH ONE'S INSIDE, WITH ONE'S STOMACH.