Question Number 1

Capture The Flag

Demonstrate how you solved the CTF that lead you to this Assignment? If your group is among the first three teams then, you will receive bonus points. However, every group must justify how they got hold of this pdf file.

Note: *If you are unable to justify this then the rest of the solutions will not be accepted.*

Solution.

Key Points

1. We know that link will always start with "https://" which contain pattern.
2. We also know that link will always end with "sharing" which will help to stop while decrypting link.

Setps

a) Firstly we created `cipherText.txt` which contain red and blcak colored cipher text seperated by new line character.

b) Then with the help of `chipherToAscii` function from `ascii.py` file, converted all character to corresponding ascii numbers between 0 to 127

c) Then we find the pattern which match with encryption of "https://" which contain same characters at 2^{nd} and 3^{rd}. Also same pattern observed with 7^{th} and 8^{th} position. We use `getPatternIndex` from `ascii.py` file for pattern finding. This funtion will return the starting index of such pattern.

d) After Finding such pattern we find key (k_0, k_1, k_2) from message and chipher text pairs with eliminating invalid keys. We use `tryAllKey` and `getKey` function from `utils.py` file to eliminate invalid key with iteration through known message and chipher text pairs.

e) After getting a key for particular pattern, We find correspondig link using derived keys from above result and start index of pattern until we get "sharing" at the end of link. We are achieving this with help of funciton `getLink` from `utils.py` file

f) After getting link for each pattern we will figure out correct link by opening each link.

Note All the files required to get link are attached in current directory of question 1. To get links run `attack.py` file. This will dumps multiple links in your terminal with corresponding links. Correct link is one of them.