# SIL 765 - Network and System Security

## Assignment - 1

**Overview :**

We will be using a 'hill-climbing' algorithm to find the correct key. We need to determine how similar a piece of text is to English text for this approach. This is called rating the 'fitness' of the text. A text very similar to English will get a high score (a high fitness), while a jumble of random characters will get a low score (a low fitness). We will use a fitness measure based on quad ram statistics. This method works by first determining the statistics of English text then calculating the probability that the ciphertext comes from the same distribution. An incorrectly deciphered (i.e., using the wrong key) message will probably contain sequences, e.g., 'QKP,' which are rare in normal English. In this way, we can rank different decryption keys. The decryption key we want is the one that produces deciphered text with the highest likelihood.

**Procedure :**

The hill-climbing algorithm looks like this:

1. Generate a random key, decipher the ciphertext using this key. Rate the fitness of the deciphered text store the result.
2. Change the key slightly (swap two characters in the key at random) measure the fitness of the deciphered text using the new key.
3. If the fitness is higher with the modified key, update the old_key with the new_key
4. Go back to 2, unless no improvement in fitness occurred in the last 10000 iterations.

As this cycle proceeds, the deciphered text gets fitter and fitter, the key becomes better until either the solution appears or the solution is not found. The hill-climbing algorithm is stuck in a 'local maximum,' where no simple changes can be made to the key to improving fitness, yet it is not at the true solution. If this happens, We run the whole algorithm 100+ times to get a better key and plaintext.

**Output:**

**Ciphertext 1 :**

1981y, $pp1n1yuux oq@ 2@3s5u1n $p 1981y, 1v y n$s9o2x 19 v$soq yv1y. 1o 1v oq@ v@6@9oq uy27@vo n$s9o2x 5x y2@y, oq@ v@n$98 0$vo 3$3su$sv n$s9o2x, y98 oq@ 0$vo 3$3su$sv 8@0$n2ynx 19 oq@ #$2u8. 5$s98@8 5x oq@ 1981y9 $n@y9 $9 oq@ v$soq, oq@ y2y51y9 v@y $9 oq@ v$soq#@vo, y98 oq@ 5yx $p 5@97yu $9 oq@ v$soq@yvo, 1o vqy2@v uy98 5$28@2v #1oq 3yw1voy9 o$ oq@ #@vo; nq19y, 9@3yu, y98 5qsoy9 o$ oq@ 9$2oq; y98 5y97uy8@vq y98 0xy90y2 o$ oq@ @yvo. 19 oq@ 1981y9 $n@y9, 1981y 1v 19 oq@ 61n191ox $p v21 uy9wy y98 oq@ 0yu816@v; 1ov y98y0y9 y98 91n$5y2 1vuy98v vqy2@ y 0y21o10@ 5$28@2 #1oq oqy1uy98, 0xy90y2 y98 198$9@v1y. 7$$8, 9$# os29 p$2 oq@ v@n$98 3y2o $p oq@ 4s@vo1$9, 7$$8 usnw!

**Output Plaintext :**

india, officially the republic of india, is a country in south asia. it is the seventh largest country by area, the second most populous country, and the most populous democracy in the world. bounded by the indian ocean on the south, the arabian sea on the southwest, and the bay of bengal on the southeast, it shares land borders with pakistan to the west; china, nepal, and bhutan to the north; and bangladesh and myanmar to the east. in the indian ocean, india is in the vicinity of sri lanka and the maldives; its andaman and nicobar islands share a maritime border with thailand, myanmar and indonesia. good, now turn for the second part of the question, good luck

**Key :**

y5n8@p7q1xwu09$342vos6#xxx

**Ciphertext 2 :**

64s48u46 8y6 q480ryp nrv 6ryy43 2yu$2tn46, n4 54yu u$ o46. un8u yrpnu n4 6r6 y$u vq441 54qq, n80ryp s4043rvn 6348wv, n80ryp y$ 34vu. n4 58v 2yv234 5n4un43 n4 58v 8vq441 $3 6348wryp. t$yvtr$2v, 2yt$yvtr$2v, 8qq 58v 8 oq23. n4 34w4wo4346 t3#ryp, 5rvnryp, n$1ryp, o4ppryp, 404y q82pnryp. n4 sq$8u46 un3$2pn un4 2yr043v4, v44ryp vu83v, 1q8y4uv, v44ryp 483un, 8qq o2u nrwv4qs. 5n4y n4 q$$z46 6$5y, u3#ryp u$ v44 nrv o$6#, un434 58v y$unryp. ru 58v x2vu un8u n4 58v un434, o2u n4 t$2q6 y$u s44q 8y#unryp s$3 x2vu nrv 134v4yt4.

**Output Plaintext :**

defeated and leaving his dinner untouched, he went to bed. that night he did not sleep well, having feverish dreams, having no rest. he was unsure whether he was asleep or dreaming. conscious, unconscious, all was a blur. he remembered crying, wishing, hoping, begging, even laughing. he floated through the universe, seeing stars, planets, seeing earth, all but himself. when he looked down, trying to see his body, there was nothing. it was just that he was there, but he could not feel anything for just his presence

**Key :**

8ot64spnrxzqwy$1x3vu205x#x

## How To Run :

The code uses command-line arguments to read the file.

Execute following code in terminal

python3 <file.py> <ciphertfile.txt>