SIL765 - NETWORK AND SYSTEM SECURITY

Assignment - 1

Anand Sharma
2024JCS2049
MTech Cyber Security

Approach

The main idea of deciphering the ciphertext is applying dictionary attack on the ciphertext. At first, we clean the ciphertext removing the punctuations (comma, semicolon, exclamation mark and full-stop characters) and create a list of cipher words. Then, we create a unique pattern for each word and match it with dictionary words. If it matches with any dictionary word patterns then mapping of the letters is done to the specific cipher letters. After mapping for each cipher word, we do intersection of it's mapping with the previous words mapping done and only take the common part. Then, we decrypt the ciphertext using the final mapping. After deciphering, check for any errors is done in the mapping comparing the words with dictionary words, if single letter difference is found in the word then necessary rectification of the mapping is done and the final deciphered plaintext and deciphered key is generated.

- **Cleaning the Ciphertext:** Non-alphabetic characters like punctuation marks (, . ; !) are removed to streamline the deciphering process.
  The cleaned ciphertext is tokenized into words for analysis.
- **Frequency Analysis**
  Letter Frequency: The occurrence of each letter in the ciphertext is calculated to help map frequently occurring letters to their counterparts in plaintext (e.g., 'e' is the most common letter in English text).
  Word Frequency: Words are grouped by their length, providing insights into potential plaintext mappings.
- **Pattern Matching**
  A unique pattern is generated for each word, representing recurring letters using indices. For example:
  Word: hello
  Pattern: 0.1.2.2.3 (distinct letters are assigned unique indices).
  Patterns from the ciphertext are matched against pre-generated patterns of English words to find potential plaintext candidates.
- **Letter Mapping**
  Possible letter mappings between ciphertext and plaintext characters are established.
  For each ciphertext letter:
  If it maps to a single plaintext letter, it's marked as "resolved."
  If it maps to multiple options, further refinement is applied using word-level analysis

- **Intersection Mapping**
  Multiple mappings are combined using intersections:
  If two mappings share common plaintext options, those are retained.
  Resolved letters are removed from other mappings to refine results iteratively.
- **Deciphering**
  Using the final resolved mappings, the ciphertext is transformed into plaintext.
  Unresolved characters are left as placeholders (_) to indicate ambiguity.
  The key mapping (plaintext-to-ciphertext) is finalized and output is printed.

Cipher Text 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!

Plain Text 1:

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, m yanmar and indonesia. good, now turn for the second part of the question, good luck!

Key 1: y5n8@p7q1xwu09$342vos6#xxx

Cipher Text 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.

Plain Text 2:

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, fishing, hoping, begging, even laughing. he floated through the universe, seeing stars, planets, seeing earth, all bet himself. then 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 2: 8ot64spnrxzqwy$1x3vu205x#x