Problem-1

Aarunish Sinha

February 2021

1 Cipher Text - 1

Decrypted Plaintext:
a disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. a common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. for example, using the keyword cipher, write out the keyword followed by unused letters in normal order and match this against the plaintext letters. make reasonable assumptions about how to treat redundant letters and excess letters in the memory words and how to treat spaces and punctuation. indicate what your assumptions are. note, the message is from the sherlock holmes novel, the sign of four.

Key:

v : a, 9 : e, o : t, q : h, 5 : i, y : s, $: o, 2 : r, @ : n,
8 : d, 6 : v, 7 : g, p : f, u : l, 0 : m, 3 : p, p : f, t : c,
1 : b, s : u, 4 : q, x : y, w : k, # : w, r : x, z : z

Frequency Anaysis:

- v is the most common single letter word in the cipher text, and 'a' and 'i' are the most common single letter words in the english language.
- 9 and o are the most common and the second most common character in the cipher text and 'e' and 't' are the most common letters in the english language respectively.
- Creating a key mapped according to the frequencies of the each character in the cipher text and the english language we get a four character word TqAT therefore, there is a very high probability that this word is THAT.
- 5y is the most common two letter word in the cipher text and 'is' is the most common two letter word in the english language.
- T$ is second most common two character word and it is most likely 'TO' which implies that $->O.

- HO# is most certainly 'HOW', #->W.
- W2ITE should be 'WRITE', 2->R.
- A@8 is the most common three letter word in the cipher text and 'R' has already been assigned to 2, therefore it must 'AND'
- uETTERS is LETTERS.
- DISAD6ANTA7E is most certainly 'DISADVANTAGE'.
- From DISADVANTAGE Op THE GENERAL we may conclude that p->F.
- INDItATE is INDICATE.
- NOR0AL is NORMAL.
- MONOAL3HA1ETIC is MONOALPHABETIC.
- Further, we can guess more and more words intuitively and figure out the rest of the mapping.

2 Cipher Text - 2

Decrypted 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:

```
q : e, 4 : l, 1 : a, n : h, 9 : v, r : i, y : n, p : g, z : d,
t : r, $ : o, @ : t, v : s, 7 : b, 5 : w, # : u, 8 : p, 3 : c,
s : m, w : f, 2 : y, 6 : k, x : j, 0 : z, u : q, o : x
```

Frequency Analysis:

- q is the most common character in the cipher text so we map q to 'e'.
- We have 44 twice in the cipher text, so map it to 'LL'
- 1LL can be mapped to ALL.
- nE is the most common two character word in the cipher text so we can map it to 'HE'.

- LEA9ryp is most probably 'LEAVING'.
- zIz shoud be 'DID', z->D.
- DINNEt should be 'DINNER'.
- N$ can only be 'NO'.
- NO@ can be 'NOT'.
- HIv is the most common three character word in the cipher text, so it should most certainly be 'HIS'.
- From here we can intuitively guess the words like 7ED would be 'BED', 5ENT will be 'WENT', #NIVERSE will be 'UNIVERSE' and so on.