CS641A Assignment-3

Sherlocked

Bholeshwar Khurana (170214) **Yaghyesh Chouhan (170813)** **Sarthak Dubey (180674)**

1 How we reached the cipher text:

1. We enter the chamber, where we see human skeletons lying on the ground. Disturbed, we start looking around and find another door on one side of the chamber. We decide to investigate, and enter with the command **enter**.
2. We find another chamber, and notice a large hole in the ground. We go into the hole with the command **enter**.
3. We enter a very loud, sticky and smelly place, with mushrooms growing out of the floor. We pluck some mushrooms with the command **pick**.
4. We go back to the previous chamber with the command **back**.
5. Stuck in the chamber with no clue what to do next, we try the command **put**, and something bites our hand. We type **back** to withdraw.
6. We finally decide to try giving the mushrooms we plucked in the hole with the command **give**. A creature takes it from our hands, and speaks:

   "Oh, thank you very much for the mushrooms! I have been hungry for so long!! I am a poor spirit trapped inside this hole by an evil man. Maybe you can help me be free ... (sigh) oh, forget it. I'll help you pass this chamber though. Note down and speak out the magic words **"thrnxxtzy"** for the hidden door to become visible. The door lies hidden in the main chamber."

7. As instructed by the voice, we retreat back to the main chamber by using the command **back** twice, and type the magic words **thrnxxtzy**. A door appears with a glass panel next to it.
8. We read the glass panel with the command **read**, and find the ciphertext:

chnbkju nc zfia xjya cvpc bb ppfcfcv zx gbc dcqfhfe gkazna ncvaafmm za wxj pxcc. hx jwchm, vhv mvau hgjh yu chnbkwzm axe cfcpm xj pah fisz zx gbc aptc luhuhn. cfx zeazna jx czu icst hhf ha mpgfhy yxgz aja. mudv csx zhiya whzx vmha pyzp zgc pjd zjd jx czu icfth. aj dyzph ksvc dhj g saiwhamj, mh pfzf cxlh mhunzh! uj zx jwnwxdj, fhkce zeh cxfjnyfv:

wsw_kmngi_ot

2 How we cracked the cipher text:

We found the index of coincidence of the cipher text which came out to be 0.057 (using *"freq_analysis.cpp"*, which is close to substitution cipher. So, we started with substitution cipher but we found a word "bb" in the cipher text. There are no double-lettered words in the English language, so the text can't be entirely substitution cipher. So it could be a Substitution-Permutation network.

The length of the cipher text is 270, so the segment length could be 2, 3, 5 or 10. The second paragraph (which is most likely the password) has a length of 10, so the segment length would be either 2, 5 or 10. We checked for segment length 2 but the new cipher text too didn't make much sense. So we assumed the segment length to be 5.

1. We observe the cipher text. The second paragraph would most probably be the password for this level. The last 3 words of the first paragraph "fhkce zeh cxfjnyfv" seem most likely to be "enter/speak the password" as evident from the last levels. We divided them in blocks of 5:

   wxdjf hkcez ehcxf jnyfv
   * ****t hepas sword

2. The last 2 blocks have a common letter "f" in the cipher text and "s" in the corresponding plain text. This gives us the mapping **s to f** and the permutation for **Encryption** $\rightarrow$ **Decryption** to be $(1, 2, 3, 4, 5) \rightarrow (*, *, *, 1, 5)$

3. The above permutation gives us the mapping **h to x**.

4. Since s is mapped to f and 5 is permuted to 5, the block "wxdjf" decrypts to "****s" which means that the third last word is "speak" and not "enter". This gives us:

   wxdjf hkcez ehcxf jnyfv
   s peakt hepas sword

5. Since 4 is permuted to 1, the second block gives us the mapping **p to e**. This mapping gives us the permutation **1 to 3** from the third block.

6. Since 1 is permuted to 3, the second block gives us the mapping **a to h**. This mapping gives us the permutation **2 to 4** from the third block. Hence we get the permutation **Encryption** $\rightarrow$ **Decryption** to be $(1, 2, 3, 4, 5) \rightarrow (3, 4, 2, 1, 5)$, i.e. if we apply this permutation to the cipher text, we will get the cipher text with only monoalphabetic substitution.

7. This permutation gives us the mapping **d to v, o to j, w to y, r to n, e to c, k to k, t to z** from the already known words "speak the password". This mapping is also compatible with the frequency analysis.

8. We did the Encryption to Decryption permutation (using the code *"permute.cpp"*) to obtain the following cipher text which has only monoalphabetic substitution:

   bnchkcn ju zxaf ijvc yapp bc bpcffcv bg zxc fqdchkg feanaz ncfavamw am zxc xjpc. wj hxchv, hmv uamv hyhg ju bnchkamw zxc fecpp jm xas ihfz bg zxc ctap lhuuhn. zxc feanaz ju zxc ihtc shm af hpyhgf yazx gjd. uamv zxc shwai yhmv zxhz yapp pcz gjd jdz ju zxc ihtcf. az yjdpv shkc gjd h shwaiahm, mj pcff zxhm lhuuhn! zj wj zxnjdwx, fechk zxc ehffyjnv:

   kww_smoin_gt

9. We already know the mapping of 11 letters. Using the same method to solve substitution cipher as we did in level-1, we cracked the cipher text and got a meaningful text, proving that our assumed permutation was correct. We obtained the following mapping:

   a b c d e f g h i j k l m n o p q r s t u v w x y z
   h b i v c u w x a l k p s m j e q n f z d t y * g *

10. We got the following plain text after decryption:

    breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead, and find away of breaking the spell on him cast by the evil jaffar. the spirit of the cave man is always with you. find the magic wand that will let you out of the caves. it would make you a magician, no less than jaffar! to go through, speak the password:

    kgg_mnzcr_yv

11. We used the password **kgg_mnzcr_yv**, and proceeded to the next level.