Substitution Cipher

Commands

1. climb
2. read
3. enter
4. read

Analysis

We built a program named as "frequency.cpp" to perform frequency analysis. We observed the frequencies of letters in cipher text as follows : $y \approx 14\%, m \approx 11\%, a \approx 10\%, w \approx 10\%, e \approx 9\%, g \approx 5\%, s \approx 5\%, p \approx 5\%, h \approx 5\%, i \approx 3\% etc.$ In English alphabet, most frequent letters are $e(\approx 13\%), t(\approx 9\%) etc.$ It was observed that the frequencies of letters in cipher text were nearly equal to the frequencies of English alphabet letters. So, we tried to substitute $y \Rightarrow e$ and $m \Rightarrow t$. After this, we get some words with t_e, and tried to replace $e \Rightarrow h$ to get words "the" and $s \Rightarrow r$ to get "there". Then, we started guessing the letters according to the frequencies and got the replacement $a \Rightarrow s$. This helped in guessing the words like interest, password, substitution etc. which further helped in making all substitutions. It was given in code that "digits have been shifted by 8 places", which means we are having 8 as encrypted digit and we have to find a digit which is shifted by itself would give 8. That results in digit 4. So, the rest of digits were shifted backward by 4 places. Also, the cipher text was rotated with some places. So, we rotated it to get the correct plain text.

Mapping

Plaintext space and ciphertext space is the set of all strings containing English alphabets, numbers and punctuation marks.

Cipher text space is [A,M,N,P,S,a,b,d,e,f,g,h,i,j,k,m,n,o,p,r,s,t,u,v,w,x,y, 0,3,8].

The Cipher text is :
wsam ie pjo ysgtm eyipbya .P axg niphay y, mey syw ahgm ewhrg tw hmysyam wh meyiepjo ys .Ag jygtmeyk pmys ie pjo ysavw kkoyjgsy whmy sy amwh rmephmewagh y!Me yigu ynay utg smew ajya apr ywap awjfkya no a mwmnmw ghiwfeyswhve wieuwr wm aepby oyyhae wtmy uox8 fkpiya. Me y fpaavgs uwa mxSrN03u wd dvwmegnmmey dngmya. Mew awameyt

Plain text space is [A,R,S,T,U,a,b,c,d,e,f,g,h,i,l,m,n,o,p,q,r,s,t,u,v,w,y,4,6,9].

The Plain text is :
This is the first chamber of the caves .As you can see, there is nothing of interest in the chamber .Some of the later chambers will be more interesting than this one! The code used for this message is a simple substitution on cipher in which digits have been shifted by 8 places. The password is tyRgU03diqq without the quotes.

Mapping as "elements of cipher text space ⇒ elements of plain text space" : a⇒s, b⇒v, d⇒q, e⇒h, f⇒p, g⇒o, h⇒n, i⇒c, j⇒m, k⇒l, m⇒t, n⇒u, o⇒b, p⇒a, r⇒g, s⇒r, t⇒f, u⇒d, v⇒w, w⇒i, x⇒y, y⇒e , A⇒S, M⇒T, N⇒U, P⇒A, S⇒R .
For digits, 0 and 3 were shifted backward by 4 places gives 0⇒6, 3⇒9.

Password

tyRgU69diqq