Q1 Commands

5 Points

List the commands used in the game to reach the first ciphertext.

climb, read, enter, read

Q2 Cryptosystem

5 Points

What cryptosystem was used in this level?

substitution cipher

Q3 Analysis

25 Points

What tools and observations were used to figure out the cryptosystem? (Explain in less than 100 words)

The frequency analysis technique was used, wherein we find out the frequency of all the characters appearing and then compared it to the frequently occurring characters in the English language. Using this, we tried to substitute some of the characters, and then for further identification, we saw if some letters can be mapped to some specific letters and provide a meaningful context to a specific or some words. For example, after replacing the letters y->e, m->t on the basis of frequency, we notice that if we replace e->h, it will form "the" at many places, which further on helped us to identify other different possible words

too by trying out different possible combinations which can produce a meaningful context. We also observed that on shifting the last few words to the starting of the paragraph gives it a meaningful and complete context. For the digits, we tried to shift each digit by same number of places, say by x = {0...9} places, such that it justifies both the meaning of the text as well as the password. At last, we found that on shifting each digit by x=4 places gives us the required solution.

Q4 Mapping

10 Points

What is the plaintext space and ciphertext space? What is the mapping between the elements of plaintext space and the elements of ciphertext space? (Explain in less than 100 words)

The plaintext space consisted of strings composed of alphabets and digits mainly , {s,v,q,h,p,o,n,c,m,l,t,u,b,a,g,r,f,d,w,i,y,e,A,T,S,R,U,4,6,9}. The decrypted 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 cipher in which digits have been shifted by 4 places. The password is tyRgU69diqq without the quotes.

The ciphertext space consisted of strings composed of alphabets and digits mainly, {a,b,d,e,f,g,h,i,j,k,m,n,o,p,r,s,t,u,v,w,x,y,P,M,A,S,N,8,0,3}. The encrypted message was:

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

Mapping used (Ciphertext -> Plaintext) :
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, 8->4, 0->6, 3->9

Note: The mapping is case insensitive, i.e., even if the case changes, the mapping will remain same. For example, m->t and M->T.

Q5 Password

5 Points

What was the final command used to clear this level?

tyRgU69diqq

Q6 Codes

0 Points

Upload any code that you have used to solve this level.

No files uploaded

Assignment 1

GRADED

GROUP

PRADEEP KUMAR TIWARI
TANISHA RASTOGI
SHRUTI WASNIK
View or edit group

TOTAL POINTS

44 / 50 pts

QUESTION 1

Commands — **5** / 5 pts

QUESTION 2

Cryptosystem — **5** / 5 pts

QUESTION 3

Analysis — R **20** / 25 pts

QUESTION 4

Mapping — **9** / 10 pts

QUESTION 5

Password — **5** / 5 pts

QUESTION 6

Codes — **0** / 0 pts