CS641A: Assignment 3

Rijndael
Abhishek Jain, Arham Chopra, Ayush Tulsyan

January 26, 2018

1 The Entry

We reached the cipher text by going into a few chambers. We found some mushrooms, which we gave to the spirit(squeaking voice in the hole), to get the magic word "thrnxxtzy". Using this on the main panel we got the cipher text. By looking at the cipher text it became clear that simple mono-alphabetic cipher won't work, because there were words like "jj". We also gathered from the previous cipher text that the last few words would be "enter/speak the password". Using this we still tried substitution cipher but failed to solve it using that. After that we thought it might be a SPN network. We tried to solve it for SPN network with 1 layer to start off. Since the SPN networks breaks the text in some segments of equal length and the lenght of the cipher being 270, we tried segment lengths 2,3,5. 2, 3 we skipped as the would not provide much of a security so we start with 5. Using the last few words especially the "dd" part, we gathered that this must be encrypted from the "ss" of "the password"("d" decrypts to "s"). Since our segment length was 5, we also gathered that the 1st and 5th character are permuted to themselves. Then extending this procedure to the previous words, we were able to find the substitution and permutation keys for the cipher. The following table list the decryption.

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

where ? corresponds to the charcter that could not be deciphered as it was not present in the encrypted text.
The permutation cipher that we found was
1 2 3 4 5
1 4 3 2 5

With this done the decrypted text we got was

```
breakerofthiscodewillbeblessedbythesqueakyspiritresidingintheholegoaheadandfind
awayofbreakingthespellonhimcastbytheevil?affarthespiritofthecavemanisalwayswith
youfindthemagicwandthatwillletyououtofthecavesitwouldmakeyouamagiciannolessthan
?affartogothroughspeakthepassword
```

The key we got at the end was **klr_oajsb_nu**.