

Q1 Commands**5 Points**

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

```
go
read
enter
read
```

Q2 Cryptosystem**5 Points**

What cryptosystem was used at this level?

```
"Random Substitution Cipher with fixed mapping" for the
text
"Substitution Cipher of key 4" for the digits in Password
plaintext
```

Q3 Analysis**25 Points**

What tools and observations were used to figure out the cryptosystem?

NOTE: Failing to provide proper analysis would result in zero marks for this assignment.

```
From the Assignment 1 description in hello iitk, we found
out that the command to break final stage is a plaintext
password from the cipher text.
```

```
So, we were also expecting the "password" in ciphertext, so
we tried to find which cipher word can mean "password".
```

Lot of intuition is involved in solving, no frequency analysis is involved.

By observation "fpaavgstu" matched the pattern of the word "password".

i.e. plaintext:ciphertext mapping we got from this is

p:f, a:p, s:a, w:v, o:g, r:s, d:u;

using these 7 mappings we tried to break other words in ciphertext.

(we did these breakings in rough notes, so , order may vary, like which got cracked earlier)

Plaintext : Ciphertext -> mappings found

by : ox -> b:o

you : xgn -> y:x

can : iph -> c:i

the : mey -> t:m, h:e

have : epby -> v:b

more : jgsy -> m:j

been : oyyh -> e:y

which : vewie -> i:w

places : fkpiya -> l:k

quotes : dngmya -> q:d

interest : whmysyam -> n:h

nothing : hgmewhr -> g:r

shifted : aewtmyu -> f:t

without : vwmegnm -> u:n

We checked these on the other cipher words and were able to decrypt the whole ciphertext, like

caves : ipbya, chamber : iepjoys, etc.,

and we decrypted the whole text.

In the decrypted text, it is mentioned that

"The code used for this message is a simple substitution cipher in which digits have been shifted by '8' places. The password is "mxSrN03uwdd(encrypted)".

The decrypted password from ciphertext is

"tyRgU03diqq(decrypted)", we tried to apply substitution

cipher of key 8 on the two digits "03" and entered the command but it didn't work, we even tried to apply substitution cipher of key 8 on the whole password but also didn't work,

Then we thought that '8' in ciphertext is also to be decrypted, but we didn't have any relations and mappings to find the plaintext for '8', so we tried substitution cipher of key 0 to 9 on numbers '03' with the rest of characters just decrypted by our random substitution cipher keeping as it is, we got the plaintext password that got accepted by terminal with substitution cipher shifted by 4 places.

i.e. Plaintext : Ciphertext = 4:8.

i.e. "mxSrN03uwdd" got deciphered into "tyRgU03diqq" then deciphered into "tyRgU69diqq".

So, finally we came to a conclusion that "tyRgU69diqq" is the plain text password.

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)

Let 'A' be the set of English alphabet

Plaintext space is every string that is possible from the set of characters A - {j k x z}

Ciphertext space is every string that is possible from the set of characters A - {c l q z}

Mapping:

1) Random Substitution: Plaintext -> Ciphertext

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

2)As explained earlier in question 3, substitution cipher shifted by 4 places.

Plaintext -> Ciphertext: key: 4.

0->4; 1->5; 2->6; 3->7; 4->8; 5->9; 6->0; 7->1; 8->2; 9->3.

Q5 Password

5 Points


What is 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

Q7 Team Name

0 Points

Cryptosenpai

Assignment 1

● Graded

Group

VAMSEE KRISHNA KAKUMANU

Rumit Pingleshwar Gore

Kuruma Abhinav

[✎ View or edit group](#)

Total Points

43 / 50 pts

Question 1

[Commands](#)

5 / 5 pts

Question 2

[Cryptosystem](#)

3 / 5 pts

Question 3

[Analysis](#)

R 20 / 25 pts

Question 4

[Mapping](#)

R 10 / 10 pts

Question 5

[Password](#)

5 / 5 pts

Question 6

[Codes](#)

0 / 0 pts

Question 7

[Team Name](#)

0 / 0 pts