

# Assignment 1

● Graded

## Group

Bikash Saha

Valeti Lokesh

Himanshu Karnatak

 [View or edit group](#)

## Total Points

50 / 50 pts

## Question 1

### Commands

5 / 5 pts

✓ + 5 pts Specifying the correct set of commands

+ 0 pts Incorrect

Click here to replace this description.

+ 0 pts Click here to replace this description.

Click here to replace this description.

+ 0 pts Click here to replace this description.

## Question 2

### Cryptosystem

5 / 5 pts

✓ + 5 pts Correct

+ 3 pts The nature of the substitution cipher is not mentioned, Substitution cipher could be of Monoalphabetic or Polyalphabetic.

+ 0 pts Incorrect

### Question 3

#### Analysis

Resolved 25 / 25 pts

✓ + 10 pts Using frequency analysis to conclude that its substitution cipherCorrect

✓ + 5 pts Step by Step decryption from cipher to plain

✓ + 5 pts Grading comment:  
Finding the mapping in the cryptosystem used by analyzing bigrams and trigrams (or small words)

✓ + 5 pts Giving mathematical explanation for the shift in the digits (We obtained the from the plaintext after decrypting it with frequency analysis, which claims that the digits are shifted by "8" places. However, because 8 is a digit, it is obvious that 8 is also encrypted by some shifting. Assume the number that was shifted to 8 is X. Because X is the key here, we can assert that X is shifted by X places, resulting in 8. The problem is written as follows in mathematical notation:  $X+X=8 \pmod{10}$  (mod 10 because there are 10 digits only, aka 0,1,2,3,4,5,6,7,8,9). The digits satisfying the above equation is 4 and 9. Without loss of generality, let us assume that  $X=9$ . Then the method of decryption tends to find two numbers Y and Z, such that  $Y+9=0 \pmod{10}$  and  $Z+9=3 \pmod{10}$ . Therefore, leading us  $Y=1$  and  $Z=4$ . For this case the decrypted password showed incorrect. So we tried the other value of  $X=4$ . Then the method of decryption tends to find two numbers Y and Z, such that  $Y+4=0 \pmod{10}$  and  $Z+4=3 \pmod{10}$ . Therefore, leading us as  $Y=6$  and  $Z=9$ . For this case the decrypted password is showed correct.)

+ 0 pts Grading comment:  
incorrect/ Directly using online tool to decipher.

🔄 Regrade Request

Submitted on: Mar 09

Dear Sir,

1.Analysis in solution 3: We have deciphered the mapping by analyzing trigrams, bigrams, common phrases. This is clearly mentioned in our analysis.

For example:

Point-4 describes how we used 'THE' a triagram to find the mapping.

Point-5 describes how we used 'IS' a bigram that becomes part of phrase 'THIS IS'.

Point-6 describes completion of 'THEse IS' as 'THERE IS'

Point-7 mentions about identifying the word 'tIRST' as 'FIRST'

Similary other points describe phrases such as 'IhTEREST Ih' -> 'INTEREST IN' and words such as NOTHINr->NOTHING.

Yet, due 5 marks have not been awarded.

In view of above kindly regrade the assignment and award due marks.

Thank you.

Done

Reviewed on: Apr 07

#### Question 4

#### Mapping

Resolved 10 / 10 pts

✓ + 3 pts Plaintext Space and cipher text space is the set of all strings containing English alphabets, numbers, punctuation marks, and spaces. Correct

- 1 pt No mention of the existence of "digits" in the ciphertext space and plaintext space

- 1 pt No mention of the existence of "punctuation marks" in the ciphertext space and plaintext space

✓ + 7 pts The mapping used for alphabets and numbers.

- 3 pts Grading comment:  
Mistakes or missing in mapping of alphabets

- 2 pts Mistakes or missing in mapping punctuation marks

- 2 pts Mistakes or missing in mappings of numbers.

+ 0 pts Incorrect

+ 3 pts mapping only done for alphabets

🔄 Regrade Request

Submitted on: Mar 09

Mapping in Solution 4:

We have deciphered and provided mapping for all symbols (English alphabets, numbers, and punctuation symbols) used in cipher text. The mapping of numbers '8 -> 4, 0 -> 6, 3 -> 9' is clearly mentioned and the method to reach this mapping is described in point-14 in analysis as well.

Yet, 2 marks have been wrongly deducted.

In view of above kindly regrade the assignment and award due marks.

Thank You

done

Reviewed on: Apr 07

#### Question 5

#### Password

5 / 5 pts

✓ + 5 pts Correct

+ 0 pts Incorrect

#### Question 6

#### Codes

0 / 0 pts

✓ + 0 pts Correct

Question 7

Team Name

0 / 0 pts

✓ + 0 pts Correct

### Q1 Commands

5 Points

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

1  
climb  
read  
enter  
read

### Q2 Cryptosystem

5 Points

What cryptosystem was used at this level?

Mono-alphabetic Substitution Cipher

### 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.

1) Cipher text is made of some English language alphabets and a few numeral digits. Its structure seems like sentence formation structure of English language.

2) Therefore our first guess is to do frequency analysis of used English alphabets (case -insensitive) and see if the results match the standard frequency distribution of letters in English language text. We wrote a program and obtained following frequency distribution in given cipher text.

Y	36×	13.95%
M	28×	10.85%
A	27×	10.47%
W	25×	9.69%
E	22×	8.53%
G	14×	5.43%
S	13×	5.04%
P	13×	5.04%
H	12×	4.65%
I	9×	3.49%
J	7×	2.71%
O	7×	2.71%
N	7×	2.71%
T	6×	2.33%
U	6×	2.33%
R	5×	1.94%
K	5×	1.94%
V	4×	1.55%
F	4×	1.55%
X	3×	1.16%
D	3×	1.16%
B	2×	0.78%

3) Distribution of alphabets in given Ciphertext appears similar to the standard English text. This insight led to our first guess to map the most frequently used element 'y' (13%) in ciphertext to element 'e', which is found with 12%

frequency in standard English text.

4) Next key observation is the three letter word 'mey' which occurs 7 times in cipher text. On substituting 'y->e', this becomes a three letter word ending at 'e'. Letter 'm' has frequency of 10% which is close to that of 't'/'a'/'o'/'s' etc. The articles 'A', 'AN', 'THE' are some of the most common words used in English language text. With this information, we now guess substitutions 'm->t' and 'e->h' assuming that this word could be 'the'. This substitution does not create any observable inconsistency in partially deciphered text. Hence we accept this and move ahead.

5) We now see the first two words are "THwa wa" (Here decrypted letters are shown in capital case) where 'wa' is repeated cipher text and 'TH' is part of plain text. So the most probable correct guess for this two words could be "THIS IS". Hence we substitute 'w->i' and 'a->s' and check for any inconsistencies.

6) Now we see 'THEsE IS' appearing in partially decrypted cipher. (Here decrypted letters are shown in capital case). Frequency of 's' in cipher text is about 5% which correlates with 'h', 'r', 'o' etc. Here 'r' seems an appropriate choice, giving our next substitution 's->r'

7) Next we can see a word "tIRST" where first 't' is in ciphertext. We check the previous words which is "THIS IS THE tIRST". So the most probable correct guess of the word 'tIRST' seems 'FIRST'. Hence we replace 't' with 'f'. 't'->'f'

8) After replacing above we can see "IhTEREST Ih" where second 'h' was not replaced. So most probable guess can be "INTEREST IN". So we replace 'h' with 'n'.

9) With this we see words like 'NOTHINr' and 'INTERESTINr' (here 'r' is written in small case to denote it is undeciphered). This gives us probable substitution for 'r' ->'g', making the words 'NOTHING' and 'INTERESTING' respectively.

10) Letter 'p' appears alone and with 'pS' where 'S' is plain text. It is quite possible that it could be 'A'. Thus our next substitution 'p'->'a'.

11) Lot of other words now start to make sense. "iAN" looks like "can", "gF" seems like "of". So we substitute 'i' -> 'c' and 'g' -> 'o'.

SOjE'->'SOME', 'jORE'->'MORE' ; gives 'j'->'m'  
 "vHICH" -> "WHICH", gives 'v'->'w'  
 "HABe" -> "HAVE", gives 'b'->'v'  
 "oEEN"-> "BEEN", gives 'o'->'b'  
 'KATER'->'LATER', 'WIkK'->'WILL' gives 'k' ->'l'  
 "SnBSTITnTION" -> "SUBSTITUTION", gives 'n'->'u'  
 "CIfHER" -> "CIPHER", gives 'f'->'p'  
 "xOU" -> "YOU", gives 'x'->'y'  
 "COuE USEu" -> "CODE USED", gives 'u'->'d'  
 "dUOTES"->"QUOTES", gives 'd' -> 'q'

14) This gives us the key for all english alphabets used in the cipher. To decode the digit however, we need to read the message, which says 'digits have been shifted by 8 places'.

Now, the possible values of x can be

x=4	$4+4(\text{mod } 10) = 8$
or	
x=9	$9+9(\text{mod } 10) = 8$

15) On applying this, our password becomes: `tyRqU69diqq` , and this works!



## 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)

Plaintext Alphabets for plaintext space is the following set:

{'e', 'T', 't', 'h', 's', 'S', 'i', 'r', 'R', 'f', 'o', 'n', 'g', 'p', 'P', 'm', 'l', 'p', 'w', 'c', 'b', 'v', 'd', 'y', 'u', 'U', 'q', '4', '6', '9', '.', ' ', '!', ','}

Plaintext space consists of all the strings made of Plaintext Alphabets

Ciphertext Alphabets for ciphertext space is the following set:

{'y', 'M', 'm', 'e', 'a', 'A', 'w', 's', 'S', 't', 'g', 'h', 'r', 'p', 'P', 'j', 'k', 'f', 'v', 'i', 'o', 'b', 'u', 'x', 'n', 'N', 'd', '0', '3', '8', '.', ' ', '!', ','}

Ciphertext space consists of all the strings made of Ciphertext Alphabets

Mapping between elements of ciphertext space to plaintext space is as following.

(sign -> indicates "is mapped to")

{y->e, M->T, m->t, e->h, a->s, A->S, w->i, s->r, S->R, t->f, g->o, h->n, r->g, p->a, P->A, j->m, k->l

f->p, v->w, i->c, o->b, b->v, u->d, x->y, n->u, N->U, d->q, 8 -> 4, 0 -> 6, 3 -> 9, . -> ., " -> ", ! -> !, , -> , }

## 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

Enter your Team Name

mod3