

## Assignment 2: Answers and Comments

3. (20) Decrypt the ciphertext corresponding to your student ID from the file you decrypted in the previous problem. Determine the cipher used to encrypt the data, along with the encryption key. Submit
- 1) the name of the cipher,
  - 2) the key, and
  - 3) a description of the steps you took for recovering the key.

**Attention:** You cannot use any specialized tools or programs, unless you developed them yourself, for solving this problem. You can use generic tools, e.g., spreadsheet program.

The following is an example of good answer to the question, courtesy of student with # s12902037:

s12902037

RTHRYLYUISZZUPVNBRTOXYPSONBNVEDVEWIMZTRVOVZNTVWUTVNET  
WPUBYEXTPKXRTRVOCTTEGMFTEVZVNGTCNVMECUPMOXVDTOMEBTIY  
NRMPXRTOKMEVZBYNWHYSZWOSNTZUOSIIMBTXRMOWMOGNVBTXYBM  
FMZMQVXMYEORYSZWCTWYETVHVUHM XR VXYEBTRTNYMOPVXBYPPVE  
WRYHFMYZTEXZUMRVXTVZZXRMORYHW TOKMBVCZTVEWMGEYCZTHV  
NMOMHYSZWNVXRTNCTXYNEXYORNTWOXRVECTVKVNXYIOYCVOTVEV  
BXYMYEMXMOPUBYEFMBXMYEXRVXDMZZMEGSEWTNXRTBZYVDYIHVN  
MOEYXRMEGCSXVEVBXYIPSNWTN

He who joy fully marches to music rank and file has already earned my contempt he has been given a large brain by mistake since for him the spinal cord would surely suffice this disgrace to civilization should be done away with at once hero is mat command how violently i hate all this how despicable and ignoble war is I would rather be torn to shreds than be a part of so base an action it is my conviction that killing under the cloak of war is nothing but an act of murder

1) Monoalphabetic Cipher

2) Key :

V C B W T I G R M L D Z P E Y K A N O X S F H J U Q  
a b c d e f g h i j k l m n o p q r s t u v w x y z

3) Steps:

Step 1: Attempted all possible cases of ceaser analysis but couldn't find any possible solution.

Step 2: Frequency analysis – I wrote a C++ program to do a frequency analysis of the given encrypted string and found the following results with descending order.

ENCRYPTED		Frequency of alphabets in English												
		e	t	a	o	i	n	s	h	r	d	l	u	c
V	37	12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8
T	35	m	w	f	y	g	p	b	v	k	x	j	q	z
M	33	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.2	0.2	0.1	0.1
Y	30													
X	28													
E	27													
R	22													
O	22													
Z	20													
N	20													
B	16													
W	15													
P	11													
S	10													
C	10													
U	9													
H	9													
I	8													
G	6													
K	4													
F	4													
D	4													
Q	1													
L	1													
J	0													
A	0													

Step 3: Plug and play – I used the above table and started deciphering the given text by plugging different combinations of a,e,i,o,t (from English frequency table above) and substituted it with V,T,M,Y, X in the given code and tried the combinations which made a bit sense, eg, “is, provided me ‘s’”, “of provided me ‘f’”, “all provide me ‘l’” etc.

Step 4: After deciphering small words, I moved on to bigger words and started decrypting letter by letter till I found the whole key.

End result analysis:

	RESULT	
A		37
E		35
I		33
O		30
T		28
N		27
H		22
S		22
L		20
R		20
C		16
D		15
M		11
B		10
U		10
W		9
Y		9
F		8
G		6
K		4
P		4
V		4
J		1
Z		1
Q		0
X		0

4. (10) You are to submit a short segment of text and a hash that is derived from a combination of the quote and your student ID.

The following are an example of good answer to questions 4 & 5, courtesy of Michael Mehar Gujral:

```
QUOTE: to be or not to be that is the question to be or not to be that is the question to be
HASH: 58245095
```

Student Number	3	8	4	0	2	0	2	0
t o b e o r n o	20	15	2	5	15	18	14	15
t t o b e t h a	20	20	15	2	5	20	8	1
t i s t h e q u	20	9	19	20	8	5	17	21
e s t i o n t o	5	19	20	9	15	14	20	15
b e o r n o t t	2	5	15	18	14	15	20	20
o b e t h a t i	15	2	5	20	8	1	20	9
s t h e q u e s	19	20	8	5	17	21	5	19
t i o n t o b e	20	9	15	14	20	15	2	5
Sum	124	107	103	93	104	109	108	105
Modified Total	124+1=125	107+1=108	103+9=112	93+1=94	104+1=105	109+1=110	108+1=109	105
Modified Total	125	108	112	94	105	110	109	105
Modified Total % 10	5	8	2	4	5	0	9	5

5. (15) Collision Problem. Find a collision with the hash you computed from the previous problem #4

```
QUOTE: So be or not to be that is the question to be or not to be that is the question to be
HASH: 58245095
```

Student Number	3	8	4	0	2	0	2	0
S o b e o r n o	19	15	2	5	15	18	14	15
t t o b e t h a	20	20	15	2	5	20	8	1
t i s t h e q u	20	9	19	20	8	5	17	21
e s t i o n t o	5	19	20	9	15	14	20	15
b e o r n o t t	2	5	15	18	14	15	20	20
o b e t h a t i	15	2	5	20	8	1	20	9
T t h e q u e s	20	20	8	5	17	21	5	19
t i o n t o b e	20	9	15	14	20	15	2	5
Sum	124	107	103	93	104	109	108	105
Modified Total	124+1=125	107-1=106	103+9=112	93-1=92	104+1=105	109-1=108	108+1=109	105
Modified Total	125	106	112	92	105	108	109	105
Modified Total % 10	5	6	2	2	5	8	9	5

**Comments:**

1. Many people miscalculated the modified total for question 4 and 5. Again, the modified sum shall be calculated as follows,








**Grade distribution for assignment 2:**

Graded out of: 49.00  
Number of records: 42

Highest grade: 49.00  
Lowest grade: 0.00

Mean grade: 42.62  
Median grade: 48.00

Standard deviation: 10.72

Score Range	Frequency	
[ 0, 4.9 )	1	
[ 4.9, 9.8 )		
[ 9.8, 14.7 )	1	
[ 14.7, 19.6 )		
[ 19.6, 24.5 )		
[ 24.5, 29.4 )	2	
[ 29.4, 34.3 )	3	
[ 34.3, 39.2 )	3	
[ 39.2, 44.1 )	3	
[ 44.1, 49 )	18	
[ 49 ]	11	