## CSCI361

Transposition cipher

## Exams-s1-2015-csci361.pdf, Section 1 - Q6

Decrypt the following ciphertext which was generated using the subsequently defined product cipher.

VDAAPARAYGYGFTCNQJCNQTRNVYCQFCGFQKVQNFCCQJTTGNXR

- a. The plaintext was firstly processed through an array based transposition block cipher of length 24 letters, with key 435162.
- b. To the results of the first part apply a shift cipher with a key corresponding to one less than that for the classical Caesar cipher.

You should add spaces back into the message as best you can.

Exams-s1-2015-csci361.pdf

## Exams-s1-2015-csci361.pdf, Section 1 - Q6

First, arrange the ciphertext into two blocks of 24 character each, that is,

VDAAPARAYGYGFTCNQJCNQTRNVYCQFCGFQKVQNFCCQJTTGNXR into

VDAAPARAYGYGFTCNQJCNQTRN VYCQFCGFQKVQNFCCQJTTGNXR

## Exams-s1-2015-csci361.pdf, Section 1 - Q6

Next, we need to find the encryption and decryption key:

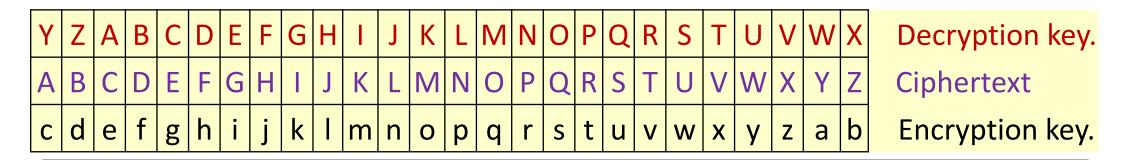
 Since the encryption was done using a key corresponding to one less than that for the classical Caesar cipher, we can establish the key as:

(Note: The key is one less than Caesar Cipher's key, that is 2 because Caesar cipher's key is 3.)

Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Decryption key.

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

C D E F G H I J K L M N O P Q R S T U V W X Y Z A B Encryption key.



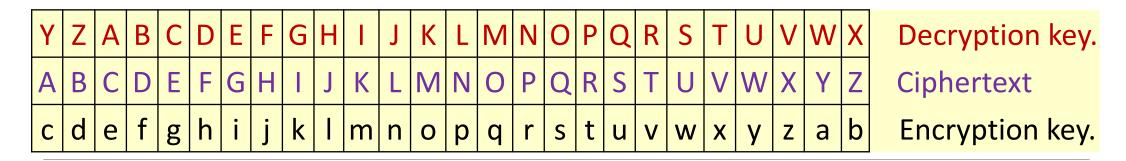
• We decrypt the ciphertext (first block) using the decryption key established, and we have:

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
V	D	Α	Α	Р	Α	R	Α	Υ	G	Υ	G	F	Т	С	N	Q	J	С	Ν	Q	Т	R	N
Т	В	Υ	Υ	Z	Υ	P	Υ	W	E	W	Е	D	R	Α	L	0	Н	A	L	0	R	Р	L

Next, we transpose the text using the key 435162 as follow: Transpose to vertical columns of four characters.



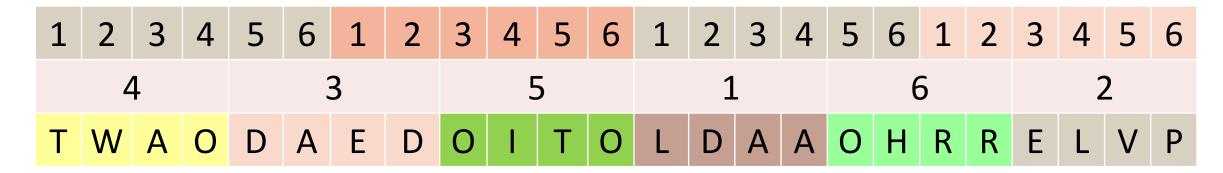
Note: There are 24 characters. Since we need to transpose using 6-digit key, we need to group the 24 characters into 6 blocks, hence, each block will have 4 ciphertext characters.



 We next decrypt the second block of ciphertext using the same decryption key, and we have:

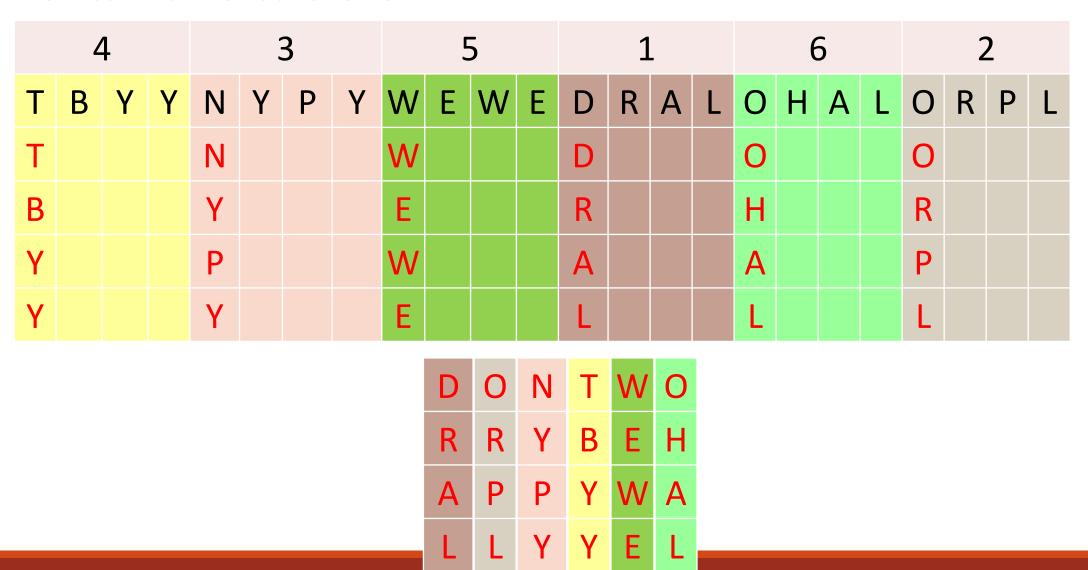
1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
V	Y	O	Q	H	C	G	F	Q	K	<b>\</b>	Q	N	F	O	O	Q	J	$\dashv$	$\dashv$	G	Z	X	R
Т	W	Α	0	D	A	E	D	0	1	Т	O	L	D	Α	Α	0	Н	R	R	Е	L	V	Р

Next, we transpose the text using the key 435162 as follow: Transpose to vertical columns of four characters.



Note: There are 24 characters. Since we need to transpose using 6-digit key, we need to group the 24 characters into 6 blocks, hence, each block will have 4 ciphertext characters.

Next, we need to arrange (transpose) the decrypted text by block in a vertical manner as follows:



Next, we need to arrange (transpose) the decrypted text by block in a vertical manner as follows:



Stack the two blocks and the plaintext (the original text) can be revealed:



Read the text row-by-row left-to-right, top-down, and we have:

DON'T WORRY BE HAPPY WALLY YELLED TOODLAW I HAVE A TRAPDOOR

