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.

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	Ciphertext
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	A	A	P	A	R	A	Y	G	Y	G	F	T	C	N	Q	J	C	N	Q	T	R	N
T	B	Y	Y	N	Y	P	Y	W	E	W	E	D	R	A	L	O	H	A	L	O	R	P	L

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

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
4				3				5				1				6				2			
T	B	Y	Y	N	Y	P	Y	W	E	W	E	D	R	A	L	O	H	A	L	O	R	P	L

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.

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	Ciphertext
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 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	C	Q	F	C	G	F	Q	K	V	Q	N	F	C	C	Q	J	T	T	G	N	X	R
T	W	A	O	D	A	E	D	O	I	T	O	L	D	A	A	O	H	R	R	E	L	V	P

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

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
4				3				5				1				6				2			
T	W	A	O	D	A	E	D	O	I	T	O	L	D	A	A	O	H	R	R	E	L	V	P

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:

4				3				5				1				6				2			
T	B	Y	Y	N	Y	P	Y	W	E	W	E	D	R	A	L	O	H	A	L	O	R	P	L
T				N				W				D				O				O			
B				Y				E				R				H				R			
Y				P				W				A				A				P			
Y				Y				E				L				L				L			

D	O	N	T	W	O
R	R	Y	B	E	H
A	P	P	Y	W	A
L	L	Y	Y	E	L

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

4				3				5				1				6				2			
T	W	A	O	D	A	E	D	O	I	T	O	L	D	A	A	O	H	R	R	E	L	V	P
T				D				O				L				O				E			
W				A				I				D				H				L			
A				E				T				A				R				V			
O				D				O				A				R				P			

L	E	D	T	O	O
D	L	A	W	I	H
A	V	E	A	T	R
A	P	D	O	O	R

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

D	O	N	T	W	O
R	R	Y	B	E	H
A	P	P	Y	W	A
L	L	Y	Y	E	L
L	E	D	T	O	O
D	L	A	W	I	H
A	V	E	A	T	R
A	P	D	O	O	R

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

☺