Columnar transposition cipher: (key: 5) key: GLOBE

Plain text: PLAINTEXT IS TO BE USED FOR ENCRYPTION

$l = 5$

P	L	A	I	N
T	E	X	T	I
S	T	O	B	E
U	S	E	D	F
O	R	E	N	C
R	Y	P	T	I
O	N			

Ciphertext:

P T S U O R O L E T S R Y N

A X O E E P I T B D N T N I E F C I

Write the plain text in rows of size l each except the last row (as the number of characters in the plain text may not be divisible by ~~two~~ l, the pass key) Then write the the columns in one row (apply transpose & put in juxta position)

Decryption: Divide the total length of the ciphertext by l (the pass key) $m = q \times l + r$

There are r columns of size $q+1$ if $r > 0$ & $(l-r)$ columns of size q.
Finally concatenate rows. to get the plain tex.

In our example: $32 = 6 \times 5 + 2$

2 columns of size 7 & the remaining ones of size 6.

Columnar transposition with a password.

plain text: PLAIN TEXT IS TOBE USED FOR ENCRYPTION

PASSWORD: GLOBE (alphabetic order of the letters of GLOBE)

G	L	O	B	E
P	L	A	I	N
T	E	X	T	I
S	T	O	B	E
U	S	E	D	F
O	R	E	N	C

B	E	G	L	O
I	N	P	L	A
T	I	T	E	X
B	E	S	T	O
D	F	U	S	E
N	C	O	R	E
T	I	R	Y	P

R Y P T I | O N
O N

Ciphertext: I T B D N T N I E F C I P T S U O R O L E T S R Y N
A X O E E P

- Step 1: Arrange the plaintext below the password as rows of size equal to that of the password
- Step 2: Shuffle the columns using the alphabetic order of the letters of the password.
- Step 3: Get ciphertext by putting the transpose of the columns in juxta position.

Decryption: GLOBE

B	E	G	L	O
I	N	P	L	A
T	I	T	E	X
B	E	S	T	O
D	F	U	S	E
N	C	O	R	E
T	I	R	Y	P
		O	N	

$32 = 6 \times 5 + 2$

G L are longer columns.

G	L	O	B	E
P	L	A	I	N
T	E	X	T	I
S	T	O	B	E
U	S	E	D	F
O	R	E	N	C
R	Y	P	T	I
O	N			

PLAIN TEXT IS _____

Write the principle of decrypting the above.

"Columnar transposition with a password."

ADFGX - cipher.

Have ciphertext consists of only five characters, namely A D F G X if the plaintext has only letters of the English alphabet. If numbers are to be included with them use A D F G V X as the characters of the ciphertext.

Password: ALICE

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

plaintext: CANCEL CEASEFIRE

DDFD

Ciphertext: DGFFAX DG DDFX DG DDFF DA GG AADD

A	L	I	C	E
D	G	F	F	A
X	D	G	D	D
F	X	D	G	D
D	F	F	D	A
D	D	F	D	G
G	A	A	D	D

A	C	E	I	L
D	F	A	F	G
X	D	D	G	D
F	G	D	D	X
D	D	A	F	F
D	D	G	F	D
G	D	D	A	A

Ciphertext: DXFDDG FDG DDD ADD AGDEGD

FFAGDXFDA.

Decrypt.