

Detyra 1 - Playfair Shifrimi

1. Përmes shifrimit të Playfair dhe rregullave të tij, enkriptoni mesazhin $P = \text{"Ju uroj sukses"}$ me çelës $k = \text{"testi"}$

Zgjidhje:

Fillimisht ndahet teksti në nga dy shkronja për enkriptim

Rregullat për playfair enkriptimin janë:

1. Nëse të dy shkronjat janë në një rresht, atëherë zhvendosja bëhet me shkronjat në të djathtë
2. Nëse të dy shkronjat janë në një kolonë, atëherë zhvendosja bëhet me shkronjat poshtë kolonës së shkronjës korrespoduese
3. Nëse formohet drejtkëndësh nga ato dy shkronja, mirën shkronjat në qoshe të drejtkëndëshit

Fillimisht krijohet matrica 5x5 (pasi që alfabeti anglez ka 26 shkronja), dhe I/J bëhet një vlerë, përmes çelësit të dhënë, dhe delikatet e shkronjave hiqen

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

Pasi krijohet matrica 5x5, fillojmë me zhvendosjet sipas rregullave.

Plaintext: JU UR OJ SU KS ES

Ciphertext: AR OU RT AQ LE SI

PlainText: "instruments"

Key: "monarchy"

Pas ndarjes në çifte: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Enriptimi:

i -> g

n -> a

s -> t

t -> l

r -> m

u -> z

m -> c

e -> l

n -> r

t -> q

s -> t

z -> x

in:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	st:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	ru:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
me:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	nt:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	sz:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												

Teksti i enkriptuar: "gatlmzclrqtx"

Pas ndarjes në çifte: 'ga' 'tl' 'mz' 'cl' 'rq' 'tx'

Teksti i dekriptuar: instrumentsz

g -> i
a -> n
t -> s
l -> t
m -> r
z -> u
c -> m
l -> e
r -> n
q -> t
t -> s
x -> z

in:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	st:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	ru:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
me:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	nt:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	sz:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												