

3. Stepenasta transpozicija

Kod ove metode karaktere otvorenog teksta zapisujemo u redove manjih dužina. Dužinu reda određuje ključna reč a zadati ključ redosled čitanja kolona.

Poruka: **the alchemist by pcoelho**

Ključna reč: DREAM -> 2 5 3 1 4 (redosled karaktera po abecedi)

Transpozicija:

2	5	3	1	4
T	H	E	A	L
C	H	E	M	I
S	T	B	Y	P
C	O	E	L	H
O				

Enkriptovana poruka: *AMYL TCSCO EEBE LIPH HHTO*

Primjer 1.12: Šifrirati otvoreni tekst **KRIPTOGRAFIJA I KRIPTOANALIZA** stupčanom transpozicijom s ključem **4 3 1 2 5 7 6**.

Rješenje.

ključ	4	3	1	2	5	7	6
	K	R	I	P	T	O	G
	R	A	F	I	J	A	I
otvoreni tekst	K	R	I	P	T	O	A
	N	A	L	I	Z	A	X
šifrat	I	F	I	L	P	I	R
	A	K	R	K	N	T	J
	T	Z	G	I	A	X	O
	A	O	A				

Prepoznavanje da se radi o transpozicijskoj šifri je vrlo jednostavno jer kod nje slova imaju iste frekvencije kao u otvorenom tekstu. I

4. Odraditi enkripciju teksta DOBRODOSLI STUDENTI ako se izvrši:

a) Naizmenična transpozicija

D B O O L S U E T

O R D S I T D N I

Enkriptovana reč je: DBOOLSUET ORDSITDNI

b) stepenasta transpozicija putem ključa UTORAK:

K = UTORAK -> 6 5 3 4 1 2

6	5	3	4	1	2
D	O	B	R	O	D
O	S	L	I	S	T
U	D	E	N	T	I

Enkriptovana reč je: OST DTI BLE RIN OSD DOU

Zadaci za samostalni rad studenta

Svaki od student je dužan da za poruke koje šifruje i dešifruje uzme **ime i prezime** svih članova porodice (min 4, ukoliko ima manje uzeti **ime i prezime** najboljeg prijatelja kao četvrti primer). Tako za svaki algoritam.