Транспозицијске шифре

***Бернадин Ибрахимпашић, Адмир Карабеговић*, Бихаћ**

1. Увод

Криптографија се појавила кад је човек покушао да сакрије своје намере. Забележени знак на камену као путоказ пријатељу један је од облика тајног споразумевања. Развој друштва које се почело делити на класе и сукобљавање интереса тих класа узроковали су појаву неповерења и неминовно су довели до потребе сакривања намера. Стварање држава, а самим тим и сукоба, још је више допринело тој појави. Тако се појавила шифра, као средство заштите тајности. Она је унапред договорени поступак којим се нека информација трансформише у неразумљив облик за свакога ко не познаје тај поступак.

Уколико посматрамо системе за шифровање, онда приликом њихове поделе према типу операција које се користе при шифровању имамо поделу на основна два типа шифри, и то *супституцијске шифре* и *транспозицијске шифре*.

Супституцијске шифре (погледати [3]) су шифре у којима се сви елементи отвореног текста, према унапред утврђеној трансформацији (или трансформацијама), замењују неким другим елементима који могу бити слова, бројеви или било какви унапред одређени знакови.

Транспозицијске шифре су шифре којима се елементи отвореног текста пермутују и на тај начин се добија шифрат. Кључ представља пермутација по којој се елементи пермутују.

Неке од најпознатијих транспозицијских шифри су: пермутацијска шифра; цик–цак шифра; ступчана транспозиција; нихилистичка транспозиција; Карданова решетка; Карданова ротирајућа решетка; таблица са спољашњом фигуром; таблица с унутрашњом фигуром.

Ми ћемо овде описати неке од њих и на прикладно одабраним примерима покушати да их приближимо свима које ова област математике интересује.

2. Rail fence (цик–цак) шифра

Цик–цак шифра, која је добила име по начину на који се врши шифрирање и дешифрирање, представља једну варијанту транспозицијске шифре која се користила у америчком грађанском рату.

Кључ $K = n$ у овој шифри представља природан број (обично већи од 1).

Приликом шифрирања текст се уписује у табелу димензија $n \times m$, где m представља дужину отвореног текста. То чинимо на следећи начин.

- Прво слово уписујемо у прво поље првог реда.
- Следеће слово уписујемо у следећи ред, померајући се дијагонално удесно. Тако идемо до последњег реда.
- Од последњег реда слова уписујемо редом дијагонално удесно али према горе.
- Након повратка у први ред, поступак се наставља даље на исти начин.
- Шифрат се добија читајући слова по речима.

Пример 1. Шифрирати отворени текст TRANSPOZICIJSKE ŠIFRE rail fence шифром где је $K_1 = 3$ и $K_2 = 4$.

Решење. а) $K_1 = 3$

T	·	·	·	S	·	·	·	I	·	·	·	S	·	·	·	I	·	·	·
·	R	·	N	·	P	·	Z	·	C	·	J	·	K	·	S	·	F	·	E
·	·	A	·	·	·	O	·	·	·	I	·	·	·	E	·	·	·	R	·

Добијамо да је шифрат TSISI RNPZC JKSFE AOIER.

б) $K_2 = 4$

T	·	·	·	·	·	O	·	·	·	·	·	S	·	·	·	·	·	R	·
·	R	·	·	·	P	·	Z	·	·	·	J	·	K	·	·	·	F	·	E
·	·	A	·	S	·	·	·	I	·	I	·	·	·	E	·	I	·	·	·
·	·	·	N	·	·	·	·	·	C	·	·	·	·	·	S	·	·	·	·

Добијамо да је шифрат TOSRR PZJKF EASII EINCS. ◇

Уколико желимо дешифрирати шифрат дужине m, добијен цик–цак шифром, онда је један од најједноставнијих начина да се то учини метод грубе силе. Шифрат ћемо уписивати у табелу која има m колона, а број редова n, који представља кључ $K = n$, ћемо повећавати за један. За $K = 1$ дешифрирање је тривијално, јер је у том случају шифрат уједно и отворени текст, па је општа претпоставка да је $K = n > 1$. Због тога се почиње с претпоставком да је $K = n \geqslant 2$. Поступак дешифрирања, који ћемо описати, понавља се све док не добијемо смислен отворени текст. Један од проблема који се појављује јесте када отворени текст нема смисла. Тада је дешифрирање, без познавања кључа K, скоро па немогуће.

Поступак одређивања кључа K и дешифрирање се спроводи на следећи начин.

1. Претпоставимо да је $K = n$. Обично се почиње с $n = 2$.
2. Нацртамо табелу с n редова и m колона.
3. Уписивање шифрата вршимо слово по слово на следећи начин.
   - Прво слово се уписује на прво место у првом реду. Након тога остављамо $2n - 3$ празних мјеста па уписујемо следеће слово, и тако редом док не дођемо до краја реда. Након тога настављамо писати у другом реду.
   - У i–том реду, прво слово уписујемо у i–ту колону. Након тога остављамо $2(n - i) - 1$ празних мјеста, затим уписујемо сљедеће слово, па остављамо $2i - 3$ празних места и понављамо поступак (слово, $2(n - i) - 1$ празних места, слово, $2i - 3$ празних места) док не дођемо до краја реда. Након тога настављамо писати у следећем реду. Тако пишемо док не пређемо у последњи ред.
   - У последњем (n–том) реду с писањем почињемо у n–тој колони. Након тога, као у првом реду, иде $2n - 3$ празних места, па следеће слово, и тако редом док не дођемо до краја отвореног текста.
4. Отворени текст ишчитавамо дијагонално цик–цак.
5. Уколико смо добили смислен отворени текст, онда је $K = n$ и добили смо отворени текст. Уколико то није случај, онда кључ повећавамо за 1 и враћамо се на 1. корак.

Пример 2. Дешифрирати шифрат SNSIC IOIMI KTSIE RRPTM TIE добијен rail fence шифром с кључем $K = 5$.

РЕШЕЊЕ. Како је $m = 23$ и $n = 5$, то нацртамо табелу која има 5 редова и 23 колоне. У првом реду уписујемо прво слово S у прво поље, а након тога остављамо $2n - 3 = 2 \cdot 5 - 3 = 7$ празних места до следећег слова. Тако идемо до краја реда.

S	·	·	·	·	·	·	·	N	·	·	·	·	·	·	·	S	·	·	·	·	·	·

Сада прелазимо у други ред. Почињемо писање од другог места у реду, а број празних места између суседних слова је редом $2(n - i) - 1 = 2 \cdot (5 - 2) - 1 = 5$ и $2i - 3 = 2 \cdot 2 - 3 = 1$ (слово, 5 празних места, слово, 1 празно место, слово, 5 празних места, итд.).

·	I	·	·	·	·	·	C	·	I	·	·	·	·	·	O	·	I	·	·	·	·	·

У трећем реду почињемо писање од трећег места у реду, а број празних места између суседних слова је редом $2(n - i) - 1 = 2 \cdot (5 - 3) - 1 = 3$ и $2i - 3 = 2 \cdot 3 - 3 = 3$.

·	·	M	·	·	·	I	·	·	·	K	·	·	·	T	·	·	·	S	·	·	·	I

Погледајмо како то изгледа у табели.

S	·	·	·	·	·	·	·	N	·	·	·	·	·	·	·	S	·	·	·	·	·	·
·	I	·	·	·	·	·	C	·	I	·	·	·	·	·	O	·	I	·	·	·	·	·
·	·	M	·	·	·	I	·	·	·	K	·	·	·	T	·	·	·	S	·	·	·	I

У четвртом реду почињемо писање од четвртог места у реду, а број празних места између суседних слова је редом $2(n - i) - 1 = 2 \cdot (5 - 4) - 1 = 1$ и $2i - 3 = 2 \cdot 4 - 3 = 5$, док у петом (последњем) реду почињемо писање од петог места у реду, а број празних места је, као и у првом реду, једнак $2n - 3 = 2 \cdot 5 - 3 = 7$.

S	·	·	·	·	·	·	·	N	·	·	·	·	·	·	·	S	·	·	·	·	·	·
·	I	·	·	·	·	·	C	·	I	·	·	·	·	·	O	·	I	·	·	·	·	·
·	·	M	·	·	·	I	·	·	·	K	·	·	·	T	·	·	·	S	·	·	·	I
·	·	·	E	·	R	·	·	·	·	·	R	·	P	·	·	·	·	·	T	·	M	·
·	·	·	·	T	·	·	·	·	·	·	·	I	·	·	·	·	·	·	·	E	·	·

Добили смо да је отворени текст SIMETRIČNI KRIPTOSISTEMI. ◊

Пример 3. Дешифрирати шифрат KGARO RJITA IPF добијен rail fence шифром.

РЕШЕЊЕ. Да бисмо одредили отворени текст употребимо методу грубе силе, тј. испитајмо све могуће кључеве $K = n \geqslant 2$, док не добијемо отворени текст који има смисла.

K=2:

K	·	G	·	A	·	R	·	O	·	R	·	J
·	I	·	T	·	A	·	I	·	P	·	F	·

Добили смо да отворени текст KIGTAARIOPRFJ нема смисла, па кључ повећавамо за 1.

K=3:

K	·	·	·	G	·	·	·	A	·	·	·	R
·	O	·	R	·	J	·	I	·	T	·	A	·
·	·	I	·	·	·	P	·	·	·	F	·	·

И овде смо добили отворени текст KOIRGJPIATFAR који нема смисла, па настављамо даље.

K=4:

K	·	·	·	·	·	G	·	·	·	·	·	A
·	R	·	·	·	O	·	R	·	·	·	J	·
·	·	I	·	T	·	·	·	A	·	I	·	·
·	·	·	P	·	·	·	·	·	F	·	·	·

Добили смо отворени текст KRIPTOGRAFIJA који има смисла, па закључујемо и да је кључ $K = 4$. ◇

3. Ступчана транспозиција

Ступчана транспозиција је транспозицијска шифра која се најчешће користила у пракси. Постоје две врсте ове шифре које се разликују према броју кључева који се користе при шифрирању отвореног текста. Тако разликујемо ступчану транспозицију с једним кључем која се користила до 1950. године и ступчану транспозицију с два кључа, која је настала увиђањем недостатака ступчане транспозиције с једним кључем.

Код ове шифре се отворени текст уписује у табелу по редовима, а шифрирани текст се чита по колонама, али с промењеним поретком колона. Ако се последњи ред не испуни до краја, онда се празна места попуне произвољним словима која не мењају садржај текста.

Напоменимо да се из табеле која је одређена кључем за шифрирање, врло једноставно, њеним преслагивањем по другом реду, добија кључ за дешифрирање.

Пример 4. Шифрирати отворени текст TANGENTA KRAGUJEVAC ступчаном транспозицијом где је $K = (3, 5, 2, 4, 1)$.

Решење. Како је $m = 5$ то отворени текст уписујемо у табелу с 5 колона.

3	5	2	4	1
T	A	N	G	E
N	T	A	K	R
A	G	U	J	E
V	A	C	L	I

Како се шифрирани текст чита по колонама, полазимо од колоне која је означена бројем 1, затим она означена бројем 2 и тако редом. На тај начин добијамо да је шифрат *EREIN AUCTN AVGKJ LATGA*. ◇

Пример 5. Дешифрирати шифрат

NESMR SGCZA ATAJI EIRTA PTUAE AATCV TOAKN ANSMI UO

ако знамо да је добијен ступчаном транспозицијом с кључем $K = (4, 3, 1, 2, 5, 7, 6)$.

РЕШЕЊЕ. Имамо да је дужина кључа $m = 7$, па како је шифрат дужине 42, то ће табела имати 7 колона и 6 редова.

Прво треба одредити кључ за дешифрирање. Запишимо кључ за шифрирање у табелу.

1	2	3	4	5	6	7
4	3	1	2	5	7	6

Сложимо табелу по другом реду.

3	4	2	1	5	7	6
1	2	3	4	5	6	7

У првом реду добијамо кључ за дешифрирање који гласи $(3, 4, 2, 1, 5, 7, 6)$. Будући да познајемо кључ за дешифрирање, шифрат записујемо у табелу по колонама.

3	4	2	1	5	7	6
N	G	A	T	E	T	N
E	C	J	A	A	O	S
S	Z	I	P	A	A	M
M	A	E	T	T	K	I
R	A	I	U	C	N	U
S	T	R	A	V	A	O

Сада табелу пресложимо по кључу који је исписан изнад. Прво иде колона означена бројем 1, затим она означена бројем 2, итд.

1	2	3	4	5	6	7
T	A	N	G	E	N	T
A	J	E	C	A	S	O
P	I	S	Z	A	M	A
T	E	M	A	T	I	K
U	I	R	A	C	U	N
A	R	S	T	V	O	A

Читањем по редовима из табеле добијамо

TANGENTAJECASOPISZAMATEMATIKUIRACUNARSTVOA.

Одбацимо ли задње слово, које је додато да би се попунила табела, добијамо отворени текст

TANGENTA JE ČASOPIS ZA MATEMATIKU I RAČUNARSTVO. ◇

Пример 6. Шифрирати отворени текст STEGANOGRAFIJA ступчаном транспозицијом с два кључа где је $K_1 = (2, 4, 1, 3)$ и $K_2 = (4, 2, 1, 3)$.

РЕШЕЊЕ. Поступак шифрирања је идентичан поступку описаном код ступчане шифре с једним кључем само се два пута понови. Како је $m = 4$, отворени текст треба уписати по редовима у табелу која има 4 колоне помоћу првог кључа.

2	4	1	3
S	T	E	G
A	N	O	G
R	A	F	I
J	A	K	D

Читајући текст по колонама, у распореду који је одређен кључем, добијамо шифрат *EOFKS ARJGG IDTNA A*, који је заправо отворени текст за други кључ. Сада се над тим текстом врши шифрирање помоћу другог кључа. Како је и овде $m = 4$, отворени текст треба уписати по редовима у табелу која има 4 колоне.

4	2	1	3
E	O	F	K
S	A	R	J
G	G	I	D
T	N	A	A

Коначно добијамо шифрат *FRIAO AGNKJ DAESG T.* ◊

4. Криптоанализа ступчане транспозиције

Криптоанализу ступчане транспозиције, тј. дешифрирање шифрата добијеног ступчаном транспозицијом уколико нам није познат кључ за шифрирање, па самим тим ни кључ за дешифрирање, описаћемо детаљно на следећем примеру.

Пример 7. Дешифрирати шифрат

KFIEU JTRIE IARTF OSISE IIKAA KSZNR
SRSTM NAIAF LROAA KIREJ AOLEC JOIIA
IGGMK ARFDN RTAJI IKSER FPIMT CEAJI

добијен ступчаном транспозицијом, ако је познато да је отворени текст на српском језику.

Решење. Приликом дешифрирања шифрата који је добијен ступчаном транспозицијом прво је потребно одредити димензију правоугаоника. То чинимо тако да број слова у шифрату факторишемо, а онда испитујемо добијене могућности. Слова шифрата пишемо по колонама у правоугаоник претпостављених димензија, а затим у сваком реду посматрамо однос броја самогласника и сугласника. Ако је претпоставка о димензији правоугаоника тачна, онда тај однос, углавном, не одступа од тог односа који вреди у језику отвореног текста. За српски језик је однос самогласника и сугласника једнак 44 : 56 ([3]).

Како у шифрату имамо 90 слова, могуће димензије су: 2×45, 3×30, 6×15, 9×10, 10×9, 15×6, 30×3 и 45×2. На самом почетку можемо одбацити неке претпоставке димензија, јер се њихово решавање обавља тривијално. Тако, нпр. можемо одбацити димензије 2×45, јер би те димензије значиле да је кључ дужине 2, што се чини прекратким. Аналогно томе одбацимо и 3×30, те због превелике дужине кључа одбацујемо димензије 30×3 и 45×2.

Уколико сада испитамо преостале могућности, добијамо да се, према односу самогласника и сугласника, као кандидати за димензије правоугаоника појављују 10×9 и 15×6. Напоменимо да су ово само претпоставке и да оне не морају бити тачне. Криптоанализа је пуна поступака који нису унапред дефинисани, него се морамо ослањати на интуицију и искуство, а понекад и на срећу.

Анализирајмо случај за табелу која има 10 редова и 9 колона. У ту сврху упишимо шифрат по колонама у правоугаоник тих димензија.

1	2	3	4	5	6	7	8	9	(SA : SU)
K	I	I	S	L	A	I	R	F	4:5
F	A	I	R	R	O	G	T	P	3:6
I	R	K	S	O	L	G	A	I	4:5
E	T	A	T	A	E	M	J	M	4:5
U	F	A	M	A	C	K	I	T	4:5
J	O	K	N	K	J	A	I	C	3:6
T	S	S	A	I	O	R	K	E	4:5
R	I	Z	I	R	I	F	S	A	4:5
I	S	N	A	E	I	D	E	J	4:5
E	E	R	F	J	A	N	R	I	3:6

Да бисмо одредили отворени текст (а самим тим и кључ) треба колоне сложити у правом поретку. У ту сврху анализирамо фреквенције биграма. Најфреквентнији биграми у српском језику који имају фреквенцију већу од 0,8 по абецедном реду су:

AK, AN, AS, AT, AV, CI, DA, ED, EN, IC, IJ, IN
IS, JA, JE, KA, KO, LI, NA, NE, NI, NO, OD, OJ
OS, OV, PO, PR, RA, RE, RI, ST, TA, TI, VA, ZA.

Сада за сваки уређени пар колона пребројимо колико се од 10 добијених биграма налази међу најфреквентнијим. Уколико гледамо уређени пар $(1, 2)$ онда видимо да се ту налазе 2 који су међу најфреквентнијим и то RI и IS, а ако посматрамо уређени пар $(2, 1)$ онда имамо 3 биграма и то: RI, OJ и ST. То учинимо са свим могућим уређеним паровима и резултате прикажемо табелом.

	1	2	3	4	5	6	7	8	9
1		2	1	3	1	2	1	0	2
2	3		1	1	1	0	1	3	1
3	2	3		3	2	2	2	2	3
4	1	4	4		1	0	1	3	0
5	0	5	4	3		2	3	0	2
6	2	2	2	1	0		2	2	2
7	0	1	2	4	3	1		0	2
8	2	3	5	3	1	6	2		2
9	0	0	1	2	3	1	1	3	

Према добијеним резултатима, највероватније после колоне 8 долази колона 6 (6 биграма у 8. реду), а да после колоне 5 долази колона 2 (5 биграма у 5. реду).

Погледамо ли 2. ред имамо да би после 2. колоне могле доћи или 1. или 8. колона, међутим ако погледамо 1. колону видимо да пре 1. колоне највероватније долази 2. колона (3 биграма). На тај начин већ имамо формирану једну трочлану групу 521 и једну двочлану 86. У 4. реду видимо да после 4. колоне долази или 2. или 3. колона (3 биграма), али како већ имамо да 2. долази после 5. закључујемо да је поредак 43. Погледамо ли 8. колону у табели видимо да 8. колона долази највероватније иза једне од колона 2, 4 или 9 (3 биграма). Како су 2. и 4. „заузете", највероватније је да 8. колона дође после 9. па добијамо групу 986. Анализирајући 9. колону у табели видимо да она највероватније дође после 3. колоне (3 биграма), па имамо групу 43986. Како после 7. колоне долазе или 4. или 5. колона, а како после 6. колоне не долази 5. колона, то имамо следеће могућности: (43986)7(521), 7(521)(43986) и (521)7(43986). Сада је лако проверити да једино први избор (439867521) даје смислен тескт. Сложимо сада колоне по добијеном поретку, тако да прво запишемо колону с бројем 4, затим с бројем 3, итд.

4	3	9	8	6	7	5	2	1
S	I	F	R	A	I	L	I	K
R	I	P	T	O	G	R	A	F
S	K	I	A	L	G	O	R	I
T	A	M	J	E	M	A	T	E
M	A	T	I	C	K	A	F	U
N	K	C	I	J	A	K	O	J
A	S	E	K	O	R	I	S	T
I	Z	A	S	I	F	R	I	R
A	N	J	E	I	D	E	S	I
F	R	I	R	A	N	J	E	E

Читајући текст по редовима и одбацујући последње слово E, које је служило само као надопуна до пуног реда, добијамо отворени текст

ŠIFRA ILI KRIPTOGRAFSKI ALGORITAM JE MATEMATIČKA FUNKCIJA KOJA SE KORISTI ZA ŠIFRIRANJE I DEŠIFRIRANJE. ◇

5. Нихилистичка транспозиција

Нихилистичка транспозиција је развијена од стране руских затвореника. Како им је било забрањено да међусобно разговарају, долазе до идеје како да пронађу пут до комуникације коју чувари не би могли разумети. У ту сврху употребљаван је систем „куцања", који је био веома несигуран.

Да би се текст шифрирао Нихилистичком транспозицијом сва слова отвореног текста се уписују у квадратну $m \times m$ матрицу по редовима, на чијим странама се налази исти кључ дужине m. При шифрирању отвореног текста задани кључ се употребљава за пермутацију колона и редова, при чему треба водити рачуна да се прво пермутују колоне, а затим редови. Добијени шифрат се ишчитава по редовима.

Дешифрирање шифрата добијеног Нихилистичком транспозицијом слично је шифрирању, само што се кључ за дешифрирање прво примењује на редове, а затим на колоне.

Пример 8. Шифрирати отворени текст *TVOJA PORUKA JE SKRIVENA* с кључем $K = (2, 5, 4, 1, 3)$.

РЕШЕЊЕ. Како је $m = 5$, отворени текст треба уписати у матрицу димензија 5×5. Отворени текст у матрицу уписујемо по редовима. Ако задњи ред остане непопуњен, онда га допунимо словима која неће променити садржај поруке.

	1	2	3	4	5
1	T	V	O	J	A
2	P	O	R	U	K
3	A	J	E	S	K
4	R	I	V	E	N
5	A	S	L	B	E

Колоне у матрици пресложимо према задатом кључу, где кључ одређује нови поредак колона.

	2	5	4	1	3
1	V	A	J	T	O
2	O	K	U	P	R
3	J	K	S	A	E
4	I	N	E	R	V
5	S	E	S	A	L

Аналогно томе, применимо кључ и на редове.

	2	5	4	1	3
2	O	K	U	P	R
5	S	E	S	A	L
4	I	N	E	R	V
1	V	A	J	T	O
3	J	K	S	A	E

Коначно, шифрат добијамо читајући матрицу по редовима.

OKUPR SESAL INERV VAJTO JKSAE. ◊

Пример 9. Дешифрирати шифрат

EOMTA DZCOI PIFOF SOVUE SPARR KECKH RNEAJ H

добијен Нихилистичком транспозицијом с кључем $K = (3, 5, 2, 4, 1, 6)$.

РЕШЕЊЕ. Како је $m = 6$, шифрат треба уписати по редовима у матрицу која има 6 редова и 6 колона.

	1	2	3	4	5	6
1	E	O	M	T	A	D
2	Z	C	O	I	P	I
3	F	O	F	S	O	V
4	U	E	S	P	A	R
5	R	K	E	C	K	H
6	R	N	E	A	J	H

Затим треба одредити кључ за дешифрирање, а то чинимо тако што запишемо кључ за шифрирање у табелу.

1	2	3	4	5	6
3	5	2	4	1	6

Сложимо табелу по другом реду.

5	3	1	4	2	6
1	2	3	4	5	6

У првом реду добијамо кључ за дешифрирање који гласи $(5, 3, 1, 4, 2, 6)$. Применимо сада кључ за дешифрирање прво на редове, па потом на колоне.

	1	2	3	4	5	6
5	R	K	E	C	K	H
3	F	O	F	S	O	V
1	E	O	M	T	A	D
4	U	E	S	P	A	R
2	Z	C	O	I	P	I
6	R	N	E	A	J	H

	5	3	1	4	2	6
5	K	E	R	C	K	H
3	O	F	F	S	O	V
1	A	M	E	T	O	D
4	A	S	U	P	E	R
2	P	O	Z	I	C	I
6	J	E	R	A	N	H

Читајући текст по редовима добијамо

KERCKHOFFSOVAMETODASUPERPOZICIJERANH.

Ако одбацимо последња четири слова, која су додата да би се попунила матрица, добијамо отворени текст

KERCKHOFFSOVA METODA SUPERPOZICIJE. ◊

6. Карданова ротирајућа решетка

У транспозицијске шифре сврстава се и Карданова ротирајућа решетка, која је добила име по познатом италијанском математичару *Ђеролану Кардану*. Ову ротирајућу решетку користили су немачки војници у Првом светском рату. Темељи се на решетки у облику квадрата, чије су димензије у оригиналу биле 6×6. Могуће су и друге димензије, али би требало да дужина странице квадрата буде паран број. Квадрат ових димензија подели се на четири једнака квадрата димензија 3×3. Затим се у сваки од четири мања квадрата уписују бројеви од 1 до 9 на следећи начин:

1. у први квадрат (горе лево) уписују се бројеви по редовима редом од 1 до 9;
2. у други квадрат (горе десно) уписују се бројеви редоследом који се добије из првог ротацијом за 90° у смеру казаљке на сату;
3. у трећи квадрат (доле десно) уписују се бројеви редоследом који се добије из другог ротацијом за 90° у смеру казаљке на сату;
4. у четврти квадрат (доле лево) уписују се бројеви редоследом који се добије из трећег ротацијом за 90° у смеру казаљке на сату.

На тај начин добијамо следећу табелу.

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Сада се из целог квадрата изаберу бројеви од 1 до 9 тачно по једном, а управо ти изабрани бројеви ће представљати отворе за упис слова у решетку. Ако изаберемо у горњем левом квадрату 4 и 9, у горњем десном 1 и 5, у доњем десном 3 и 8, те у доњем левом 2, 6 и 7, добијамо решетку следећег облика.

1	2	3	7	4	○
○	5	6	8	○	2
7	8	○	9	6	3
3	○	9	9	○	7
○	5	8	6	5	4
1	4	○	○	2	1

У овакву Карданову ротирајућу решетку могуће је уписати укупно 36 слова отвореног текста и то по 9 слова за сваку ротацију решетке. Због нашег избора отвора, добијамо укупно 36 различитих отвора за упис слова отвореног текста. Приликом шифрирања користи се папир за писање шифрата и решетка. На папир се кроз празна поља, по редовима упише првих 9 слова отвореног текста. Затим се решетка ротира за 90° у смеру казаљке на сату и поново се кроз празна поља у решетки упише следећих 9 слова. Поново се решетка заротира за 90° и упише се следећих 9 слова. Коначно заротирамо решетку још једном за 90° и кроз отворе упишемо и преосталих 9 слова. Читајући текст редом из табеле добијамо шифрат.

Пример 10. Шифрирати отворени текст

DIFERENCIJALNA I LINEARNA KRIPTOANALIZA

помоћу горе наведене Карданове ротирајуће решетке.

РЕШЕЊЕ. Поступак шифрирања отвореног текста помоћу Карданове ротирајуће решетке заснован је на четири корака. У првом кораку кроз празна поља у решетку уписујемо први блок од 9 слова, тј. слова DIFERENCI. Након што слова упишемо и склонимо решетку, на папиру остаје следећа ситуација.

					D
I				F	
		E			
	R			E	
N					
		C	I		

Ако заротирамо решетку за 90° и поново кроз празна поља у решетку упишемо следећих 9 слова JALNAILIN, добијамо следећу ситуацију.

	J			A	D
I		L		F	
N		E	A		
I	R			E	
N		L		I	
		C	I		N

Решетка се поново заротира за 90° и на исти начин се упише следећих 9 слова EARNAKRIP.

	J	E	A	A	D
I		L		F	R
N	N	E	A	A	
I	R		K	E	
N	R	L		I	I
P		C	I		N

Поновимо исти поступак и решетку још једном заротирамо за 90° и кроз отворе упишемо и преосталих 9 слова TOANALIZA.

T	J	E	A	A	D
I	O	L	A	F	R
N	N	E	A	A	N
I	R	A	K	E	L
N	R	L	I	I	I
P	Z	C	I	A	N

Коначно, читајући редом добијамо шифрат

TJEAA DIOLA FRNNE AANIR AKELN RLIII PZCIA N. ◊

Литература

[1] A. Dujella, M. Maretić: *Kriptografija*, Element, Zagreb, 2007.

[2] D. Kahn: *The Codebreakers. The Story of Secret Writing, I–III*, Macmillan Co., New York, 1967.
(hrvatski prevod: *Šifranti protiv špijuna*, Centar za informacije i publicitet, Zagreb, 1979.)

[3] B. Ibrahimpašić: *Supstitucijske kriptografske šifre*, Tangenta **4**(2008), 1–11.

[4] B. Ibrahimpašić: *Matematičke osnove kriptografije javnog ključa*, Magistarski rad, PMF, Sarajevo, 2008.

[5] B. Ibrahimpašić: *Kriptografija kroz primjere*, Pedagoški fakultet, Bihać, 2011.

Статијата прв пат е публикувана во списанието Тангента на ДМ на Србија во 2012/13 година