Transpozicijske šifre

Rošić, Kristina

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:969932

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Integrirani sveučilišni nastavnički studij matematike i informatike

Kristina Rošić

Transpozicijske šifre

Diplomski rad

Osijek, 2018.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Integrirani sveučilišni nastavnički studij matematike i informatike

Kristina Rošić

Transpozicijske šifre

Diplomski rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2018.

Sadržaj

Uvod

Prije no što kratko opišemo sadržaj ovog rada upoznati ćemo se s osnovnim pojmovima kriptografije.

Kriptologija je znanost koja se bavi proučavanjem i definiranjem metoda za zaštitu informacija (šifriranjem) i proučavanjem i pronalaženjem metoda za otkrivanje šifriranih poruka (dešifriranje). Kriptologija obuhvaća dvije znanstvene discipline kriptografiju i kriptoanalizu. Rezultate kriptologije prvenstveno koriste oružane snage i diplomatska služba, a razvojem telekomunikacija i mnoge druge službe.

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao "tajnopis". Riječ kriptografija nastala je od pridjeva *kryptos* što znači *skriven* i od riječi *graphein* što znači *pisati*. Osnovni zadatak kriptografije je omogućiti dvjema osobama (zvat ćemo ih *pošiljatelj* i *primatelj*) komuniciranje preko nesigurnog komunikacijskog kanala na način da treća osoba (njihov *protivnik*), ne može pročitati njihove poruke. Poruku koju pošiljatelj želi poslati primatelju zvat ćemo *otvoreni tekst* (engl. plaintext). Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni ključ (engl. key). Taj postupak se naziva *šifriranje*, a dobiveni rezultat *šifrat* (engl. ciphertext) ili *kriptogram*. Obrnuti proces se naziva *dešifriranje*.

Kriptoanaliza je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja pravila za šifriranje ili ključa.

Definicija 1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenog teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je konačan skup svih mogućih ključeva;*
4. $\mathcal{E}$ *je skup svih funkcija šifriranja;*
5. $\mathcal{D}$ *je skup svih funkcija dešifriranja;*
6. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(n)) = n$ *za svaki otvoreni tekst* $n \in \mathcal{P}$.

Iz svojstva $d_K(e_K(n)) = n$ slijedi kako funkcije šifriranja e_K moraju biti injekcije, u suprotnom bi moglo doći do dvosmislenosti poruka. Ako bi se dva različita slova otvorenog teksta n_1 i n_2 nekom funkcijom šifriranja šifrirala istim slovom t, odnosno

$$e_K(n_1) = e_K(n_2) = t,$$

primatelj poruke ne bi znao treba li t dešifrirati u n_1 ili n_2.

Šifre definiramo nad $\mathbb{Z}_{26}$ i budući da koristimo 26 slova engleskog alfabeta imamo sljedeću korespondenciju, koja za svako slovo alfabeta daje njegov "numerički ekivalent". U Tablici 1 vidimo korespondenciju slova alfabeta i brojeva, te s obzirom na njihove "numeričke ekvivalente" određujemo permutaciju s obzirom na ključnu riječ.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tablica 1: *Korespondencija slova engleskog alfabeta i brojeva*

Danas se kriptografija koristi za pružanje tajnosti i integriteta našim podacima te autentičnosti i anonimnosti prilikom komuniciranja. Suvremeni kriptografski algoritmi previše su složeni da bi ih izvršili ljudi, tako da se danas algoritmi izvode pomoću računala ili specijaliziranih hardverskih uređaja.

U ovom radu opisat ćemo neke od transpozicijskih šifri. Na primjerima ćemo pokazati šifriranje i dešifriranje ovih šifri. Najprije ćemo spomenuti skital, povijesnu napravu za šifriranje koju su koristili Spartanci u 5. stoljeću prije Krista. Nakon toga ćemo navesti permutacijske šifre a zatim i najupotrebljivaniju transpozicijsku šifru - stupčanu transpoziciju. Objasnit ćemo kako se ona može poboljšati korištenjem dvaju ključeva. Također ćemo spomenuti i Trellis šifru koja je korištena za vrijeme engleske kraljice Elizabete I (koristila ju je za komunikaciju sa svojim špijunima), Cardanovu rotirajuću rešetku koja je korištena u "Mathias Sandord" noveli poznatog pisca Julesa Verna, te ADFGVX šifru koju su Njemci koristili u Prvom svjetskom ratu. ADFGVX je primjer kombiniranja transpozicijske i supstitucijske šifre, gdje se koristi Polybiusov kvadrat. Tako se poboljšava sam proces šifriranja poruka. ADVGVX koristi slova koja u Morseovom kodu imaju najmanje sličnosti te se zbog toga može smanjiti broj grešaka u prijenosu poruke.

1 Transpozicijske šifre

Podjelu šifri na supstitucijske i transpozicijske uveo je u 16. stoljeću Giovanni Porta. Kod susptitucijskih šifri elementi otvorenog teksta zamjenjivani su različitim elementima šifrata. Kod transpozicijskih šifri elementi otvorenog teksta ostaju nepromijenjeni, ali se mijenja njihov međusobni položaj. Formalna definicija transpozicijske šifre prema [3] glasi:

Definicija 2. *Neka je m fiksan prirodan broj. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, te neka se $\mathcal{K}$ sastoji od svih permutacija skupa $\{1,2,\ldots,m\}$. Za $\pi \in \mathcal{K}$ definiramo*

$$e_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})$$
$$d_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)}).$$

Kardinalnost skupa $\mathcal{K}$ je $m!$. Kod vrlo kratkih poruka koje se recimo sastoje od jedne riječi, ta je metoda prilično nesigurna, zato što se malen broj slova može ispremještati na malen broj načina. Tako se tri slova mogu ispremještati na šest načina. Primjerice riječ SOL (LOS, LSO, OLS, OSL, SLO i SOL). Međutim, ako povećamo broj slova, broj mogućih kombinacija raste, zbog čega povratak na početnu poruku i nije moguć bez točnog poznavanja samog procesa miješanja. Recimo, riječ KRIPTOGRAFIJA ima 13 slova te 6 227 020 800 mogućih razmještaja slova. Da bi transpozicija imala smisla, premještanje slova mora se odvijati u skladu s nekim pravilom, koje je unaprijed dogovoreno s primateljem, a koje je nepoznato neprijatelju.

1.1 Skital

Kao i supstitucijske tako i transpozicijske šifre nisu u potpunosti sigurne, ali obje imaju bogatu povijest. Spartanci su u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje zvanu skital. To je bio drveni štap oko kojeg se namotavala vrpca od pergamenta po kojoj se okomito pisala poruka kako je prikazano na Slici 1.

Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine (vidjeti [8, str. 18]). Pretpostavimo da na štap možemo napisati četiri slova u krug i pet po dužini. Otvoreni tekst bi mogao glasiti: *Brodovi su usidreni u Mikeni.* Stoga bi ovaj tekst, namotan na skital, izgledao ovako:

SLIKA 1. *Skital*

Brodov

isuusi

dreniu

Mikeni

A šifrat bi onda bio: *BIDMR SRIOU EKDUN EOSIN VIUI*. Da bi se taj tekst dešifrirao samo bismo morali namotati tekst na štap i pročitati uzduž. Svako peto slovo bi se pojavilo u istom retku, tako bi otvoreni tekst glasio: *Brodovi su usidreni u Mikeni.* 475. godine prije Krista zabilježena je upotreba skitala. Tada je general Pausanias, htio sklopiti mir s Perzijancima, što su Spartanci smatrali izdajom. Tako su Grci ostali u povijesti zabilježeni kao prvi narod koji je koristio naprave za transpozicijsko šifriranje.

1.2 Permutacijske šifre

Vrlo često se poistovjećuje naziv permutacijske i transpozicijske šifre. Ako je ključ za šifriranje permutacija π, onda je ključ za dešifriranje njoj inverzna permutacija π^{-1}.

Definicija 3. *Svaku uređenu n-torku skupa od n elemenata zovemo permutacija.*

Broj permutacija n-članog skupa je $p_n = n!$ Primjerice, ukupan broj permutacija skupa {a,e,i,o,u} je jednak 5! odnosno 120.

Primjer 1. *Šifrirajmo otvoreni tekst*

If you can dream it there is some way to do it

koristeći permutacijsku šifru s ključem $k = \pi = (3,1,4,2,5)$.

Rješenje:

Iz ključa k nam slijedi $m = 5$. Sada otvoreni tekst pišemo po redcima u tablicu od pet stupaca.

1	2	3	4	5
I	F	Y	O	U
C	A	N	D	R
E	A	M	I	T
T	H	E	R	E
I	S	S	O	M
E	W	A	Y	T
O	D	O	I	T

Kako je $k = (3, 1, 4, 2, 5)$ šifriranje je dano s:

x	1	2	3	4	5
$\pi(x)$	3	1	4	2	5

Dakle, stupce u polaznoj tablici permutiramo prema zadanoj tablici koju određuje permutacija π . Slijedi nam:

3	1	4	2	5
Y	I	O	F	U
N	C	D	A	R
M	E	I	A	T
E	T	R	H	E
S	I	O	S	M
A	E	Y	W	T
O	O	I	D	T

Šifrat dobivamo čitanjem po redcima prethodne tablice. Šifrat glasi:

YIOFU NCDAR MEIAT ETRHE SIOSM AEYWT OOIDT.

Primjer 2. *Dešifrirajmo šifrat*

IMTMT AAELK JKARA EHSCJ IVIAI OAZTS NN

dobiven permutacijskom šifrom s ključnom riječi UMJETNIK iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Najprije svakom slovu ključne riječi pridružimo broj, koji mu odgovara s obzirom na abecedni poredak u hrvatskom jeziku.

U	M	J	E	T	N	I	K
8	5	3	1	7	6	2	4

x	1	2	3	4	5	6	7	8
$\pi(x)$	8	5	3	1	7	6	2	4

Inverzna permutacija:

y	1	2	3	4	5	6	7	8
$\pi^{-1}(y)$	4	7	3	8	2	6	5	1

Šifrat pišemo u tablicu koja ima osam stupaca (broj slova u ključnoj riječi). Šifrat pišemo po redovima.

1	2	3	4	5	6	7	8
I	M	T	M	T	A	A	E
L	K	J	K	A	R	A	E
H	S	C	J	I	V	I	A
I	O	A	Z	T	S	N	N

Sada s obzirom na inverznu permutaciju posložimo stupce u tablici. Tako dobijemo otvoreni tekst.

4	7	3	8	2	6	5	1
M	A	T	E	M	A	T	I
K	A	J	E	K	R	A	L
J	I	C	A	S	V	I	H
Z	N	A	N	O	S	T	I

Otvoreni tekst čitamo po redcima. Otvoreni tekst glasi:

Matematika je kraljica svih znanosti.

Još jedan način za dešifriranje permutacijske šifre je probati sve moguće permutacije, sve dok se ne pronađe blok koji ima smisla. Ako u ključnoj riječi postoje jednaka slova onda ih jednostavno promatramo u danom poretku. Dakle, složimo slova u abecednom poretku, pridružimo im brojeve od 1 do m i promatranjem ključne riječi formiramo odgovarajuću permutaciju. Primjerice ako je ključna riječ ABECEDA, tada je m=7.

A	A	B	C	D	E	E
1	2	3	4	5	6	7

Slijedi π=(1,3,6,4,7,5,2).

1.3 Stupčana transpozicija

Najupotrebljavanija transpozicijska šifra je stupčana transpozicija. Kod nje se otvoreni tekst upisuje u pravokutnik po redcima, a zatim se poruka čita po stupcima, ali s promijenjenim poretkom stupaca. Ako se posljednji redak ne ispuni do kraja, onda se prazna mjesta popune proizvoljnim slovima (ili nulama) koja ne mijenjaju sadržaj poruke. Kod neregularnih stupčanih transpozicijskih šifri prazna mjesta se ne ispunjavaju. Broj stupaca i stupčanih permutacija određen je ključnom riječi. Na primjer, ako bi ključna riječ bila na engleskom FLOWER koja ima šest slova, tada bi i broj stupaca bio šest, a permutacija je određena po abecednom redu slova u riječi. U našem slučaju bi to bilo: 234615.

Primjer 3. *Šifrirajmo otvoreni tekst*

She said don't let go never give up its such a wonderful life.

stupčanom transpozicijom s ključnom riječi FLOWER.

Rješenje:

Ovdje imamo tablicu gdje se u prvom redu nalazi ključ, a ispod njega je napisan otvoreni tekst.

2	3	4	6	1	5
S	H	E	S	A	I
D	D	O	N	T	L
E	T	G	O	N	E
V	E	R	G	I	V
E	U	P	I	T	S
S	U	C	H	A	W
O	N	D	E	R	F
U	L	L	I	F	E

S obzirom na naš ključ, šifrat izgleda ovako (kod transpozicijskih šifri obično se šifrat grupira u blokove od pet slova):

ATNIT ARFSD EVESO UHDTE UUNLE OGRPC DLILE VSWFE SNOGI HEI.

Pogledajmo sada prema [3], ako imamo šifrat i trebamo odrediti otvoreni tekst kako to funkcionira. Najprije moramo odrediti dimenziju pravokutnika. To se radi tako da se broj slova u šifratu faktorizira. Ako tada dobijemo više mogućnosti, onda upišemo slova šifrata po stupcima u pravokutnike pretpostavljenih dimenzija

te promatramo odnos samoglasnika i suglasnika u svakom retku. Ukoliko je pretpostavka o dimenziji točna, taj odnos ne bi smio puno odstupati od njihovog odnosa u jeziku otvorenog teksta (u hrvatskom jeziku je to 43% : 57%). Nakon što odredimo dimenzije pravokutnika, moramo još odrediti poredak stupaca. Ako je broj stupaca relativno mali, šifrat možemo dešifrirati tako da jednostavno premještamo stupce dok ne dobijemo smisleni sadržaj u redcima. Dodatnu pomoć nam mogu dati podatci o frekvencijama bigrama.

Najfrekventiniji bigrami u hrvatskom jeziku su redom:

- 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.

Primjer 4. *Dešifrirajmo šifrat*

EEBOO EKDSM NJAMR NCPOT SOAEO AULKA DOJSO EKSEA

dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

U šifratu imamo 40 slova, pa se kao najvjerojatnije dimenzije pravokutnika nameću 5×8 i 8×5 (razumno je pretpostaviti da ni broj stupaca ni broj redaka nisu jako mali - u prvom slučaju bi anagramiranje bilo trivijalno za obaviti, a u drugom duljina ključa ne bi bila bitno kraća od duljine otvorenog teksta). Ako upišemo šifrat u pravokutnike tih dimenzija, dobivamo:

E	S	C	O	J	2:3
E	M	P	A	S	2:3
B	N	O	U	O	3:2
O	J	T	L	E	2:3
O	A	S	K	K	2:3
E	M	O	A	S	3:2
K	R	A	D	E	2:3
D	N	E	O	A	3:2

E	E	N	N	S	A	D	E	4:4
E	K	J	C	O	U	O	K	3:5
B	D	A	P	A	L	J	S	2:6
O	S	M	O	E	K	S	E	4:4
O	M	R	T	O	A	O	A	5:3

S obzirom na odnos samoglasnika i suglasnika u hrvatskom jeziku možemo zaključiti da je prvi izbor dimenzija vjerojatniji. Sada ovih pet stupaca možemo pokušati "anagramirati" tako da dobijemo smisleni tekst. Na početku nam tu može pomoći već spomenuta frekvencija bigrama.

Za svaki od parova stupaca, pogledajmo koliko se od tako dobivenih pet bigrama nalazi među prethodnih 36 najfrekventnijih. Tako dobijemo sljedeću tablicu:

	1	2	3	4	5
1	-	1	2	0	1
2	0	-	3	1	5
3	2	1	-	0	1
4	2	2	1	-	3
5	2	2	0	1	-

Možemo primijetiti da je broj pet najveći od svih brojeva u tablici. Stoga možemo krenuti od pretpostavke da stupci 2 i 5 dolaze jedan do drugoga (u tom poretku). Obzirom na stupac 5 dalje možemo iz tablice pretpostaviti da je do stupca 5 stupac 1. Preostaje nam još za smjestiti stupce 3 i 4. Imamo dvije mogućnosti: 42513 i 32514. Sada lako provjerimo da prvi izbor daje rješenje šifrata. Odnosno,

Osjećam se puno bolje otkako sam se odrekao nade.

Još različitih primjera šifriranja i dešifriranja sa stupčanom transpozicijom može se vidjeti u [1].

1.3.1 Stupčana šifra s dva ključa

S obzirom na to da se stupčana transpozicija može lako razbiti, naime, ukoliko treća strana dođe u posjed šifriranog teksta, ona može lako pogoditi dimenzije pravokutnika i slagati anagrame dok se ne dobije neka smislena cjelina, tako da ona ima veliki nedostatak. Stupčana transpozicija se stoga upotrebljavala do 50-ih godina prošlog stoljeća, a onda je poboljšana sa stupčanom šifrom s dva ključa. Stupčana šifra s dva ključa jedna je od najpopularnijih šifri zbog svoje jednostavnosti i visoke razine sigurnosti. Šifriranje i dešifriranje relativno su jednostavni. Dva ključa, K_1 i K_2 moraju biti unaprijed dogovoreni i odabrani. Primjerice, želimo li šifrirati otvoreni tekst na engleskom jeziku *This is a secret text encrypted by the double transposition cipher*, koristeći ključeve K_1="KEYWORD" i K_2="SECRET". Naš otvoreni tekst ima 56 slova. Najprije napišemo ovaj otvoreni tekst u pravokutnik koji ima sedam (riječ *Keyword* ima sedam slova) stupaca i osam redova. Otvoreni

tekst pišemo u redovima, jedan ispod drugog (Tablica 2). Tada primijenimo prvu stupčanu transpoziciju, tako da promijenimo poredak stupaca prema numeričkom ekvivalentu ključa (Tablica 3). U odgovarajući pravokutnik najprije napišemo drugi ključ i njegov numerički ekvivalent, zatim uzimamo stupac po stupac i upisujemo ih u redove. (Tablica 4). Nakon toga napravimo drugu stupčanu transpoziciju, mijenjajući poredak stupaca s obzirom na numerički ekvivalent ključa (Tablica 5).

3	2	7	6	4	5	1
K	E	Y	W	O	R	D
T	H	I	S	I	S	A
S	E	C	R	E	T	T
E	X	T	E	N	C	R
Y	P	T	E	D	B	Y
T	H	E	D	O	U	B
L	E	T	R	A	N	S
P	O	S	I	T	I	O
N	C	I	P	H	E	R

Tablica 2: *Prvi korak šifriranja*

1	2	3	4	5	6	7
D	E	K	O	R	W	Y
A	H	T	I	S	S	I
T	E	S	E	T	R	C
R	X	E	N	C	E	T
Y	P	Y	D	B	E	T
B	H	T	O	U	D	E
S	E	L	A	N	R	T
O	O	P	T	I	I	S
R	C	N	H	E	P	I

Tablica 3: *Drugi korak šifriranja*

5	2	1	4	3	6
S	E	C	R	E	T
A	T	R	Y	B	S
O	R	H	E	X	P
H	E	O	C	T	S
E	Y	T	L	P	N
I	E	N	D	O	A
T	H	S	T	C	B
U	N	I	E	S	R
E	E	D	R	I	P
I	C	T	T	E	T
S	I				

Tablica 4: *Treći korak šifriranja*

1	2	3	4	5	6
C	E	E	R	S	T
R	T	B	Y	A	S
H	R	X	E	O	P
O	E	T	C	H	S
T	Y	P	L	E	N
N	E	O	D	I	A
S	H	C	T	T	B
I	N	S	E	U	R
D	E	I	R	E	P
T	C	E	T	I	T
	I			S	

Tablica 5: *Četvrti korak šifriranja*

Završni šifrat pročitamo redom po stupcima:

RHOTN SIDTT REYEH NECIB XTPOC SIEYE CLDTE RTAOH EITUE ISSPS NABRP T.

U Prvom svjetskom ratu njemačka vojska koristila je ovu vrstu šifre u manje sigurnom obliku, tako što su koristili iste ključeve. U Drugom svjetskom ratu, ovu šifru su koristile: Velika Britanija, SAD, Francuska, Njemačka, te se tada počinju koristiti različiti ključevi.

1.3.2 Myszkowski transpozicija

Myszkowski transpozicijska šifra je jedan oblik stupčane transpozicijske šifre. Predložio ju je 1902. godine Émile Victor Théodore Myszkowski bivši francuski pukovnik. Tu se koristi isti postupak kao i kod stupčane transpozicije, gdje se otvoreni tekst piše u retke ispod ključne riječi. Jedina razlika je ako ima ponavljanja slova u ključnoj riječi, sva ista slova dobiju isti broj. Za stupce koji imaju isti broj, njihova slova čitamo po redovima, a ne po stupcima.

Da bi šifrirali otvoreni tekst koristeći Myszkowski transpoziciju moramo imati ključnu riječ (ključ). Nakon toga otvoreni tekst upišemo u mrežu gdje je broj stupaca u mreži zapravo broj slova u ključnoj riječi. Nakon toga numeriramo slova u ključnoj riječi koristeći njihov abecedni poredak, ali tako da slovima koja se ponavljaju dajemo isti broj. Krenemo od broja 1 i ako se 1 samo jednom pojavljuje, isčitamo slova iz stupca isto kao i kod stupčane transpozicije. Ako se broj 1 pojavi više od jednog puta, čitamo s lijeva na desno sva prva slova u stupcima koji su ispod broja 1. Onda se prebacimo u drugi red i čitamo po redu s lijeva na desno. Kada završimo prebacimo se na broj 2 i tako do kraja.

Primjer 5. *Šifrirajmo otvoreni tekst*

Praštajući čovjek se izdiže iznad onih koji ga vrijeđaju

Myszkowski stupčanom transpozicijom s ključnom riječi BANANA.

Rješenje:

Naš otvoreni tekst ima 48 slova, a ključna riječ ima 6 slova, stoga ćemo imati 6 stupaca, a 8 redova (48:6=8). Na vrhu mreže pišemo ključnu riječ. Ispod ključne riječi pišemo brojeve, koristeći abecedni red slova u riječi, pritom pazimo da ako u ključnoj riječi ima istih slova ona se numeriraju istim brojem. Tu je razlika između Myszkowski i stupčane transpozicije. (Ovdje ćemo poistovjetiti slova Č,Ć s C, Š sa S i Đ s D.)

B	*A*	*N*	*A*	*N*	*A*
2	1	3	1	3	1

P	*R*	*A*	*S*	*T*	*A*
J	*U*	*C*	*I*	*C*	*O*
V	*J*	*E*	*K*	*S*	*E*
U	*Z*	*D*	*I*	*Z*	*E*
I	*Z*	*N*	*A*	*D*	*O*
N	*I*	*H*	*K*	*O*	*J*
I	*G*	*A*	*V*	*R*	*I*
J	*E*	*D*	*A*	*J*	*U*

Započinjemo sa stupcem ispod broja 1. Budući da imamo 3 slova A (odnosno 3 puta broj 1), šifrat započinjemo s RSA i zapisujemo slova u prvom redu ispod broja 1 s lijeva na desno. Nakon toga prelazimo u drugi red i nastavimo šifrat RSAUI O, tako nastavimo do kraja dok ne dođemo do zadnjeg slova u stupcu. Budući da se slovo *B* pojavljuje samo jednom, slova u stupcu ispod B upisujemo u šifrat. Sa slovom N postupimo isto kao i sa slovom A. Tako dobijemo šifrat

RSAUI OJKEZ IEZAO IKJGV IEAUP JVUIN IJATC CESDZ NDHOA RDJ.

Dešifriranje je slično kao kod stupčane transpozicije.

Primjer 6. *Dešifrirajmo šifrat*

IVSAO TSDAM ANIHI TSSNO PTTOU KMRRS JIVOO VKAOE VIIGT IRSLO EATLI ISUST IBIH

dobiven Myszkowski stupčanom transpozicijom s ključnom riječi OPASNOST iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Najprije napišemo ključnu riječ i s obzirom na abecedni poredak slova napišemo brojeve, ali pazeći da istim slovima pridružimo iste brojeve.

Nakon toga podijelimo broj slova u šifratu s duljinom ključne riječi (brojem slova u njoj), da znamo koliko redova će naša mreža imati. Nadalje šifrat stavimo u mrežu po stupcima. Krećemo od broja jedan pa sve do najvećeg broja. Ako se broj pojavljuje samo jednom, ispunjavamo stupac. Ako se broj pojavljuje dva ili više puta, popunjavamo redove s lijeva na desno stupaca koji imaju taj broj.

Naš šifrat ima 64 slova, a ključna riječ ima 8 slova, stoga nam treba 64:8=8, tj. 8 redova. S obzirom da broj 1 imamo samo jedan put, ispunimo stupac ispod broja 1, sa osam slova šifrata. Isto tako napravimo i ispod broja 2 (Tablica 6).

O	*P*	*A*	*S*	*N*	*O*	*S*	*T*
3	4	1	5	2	3	5	6
		I		*A*			
		V		*M*			
		S		*A*			
		A		*N*			
		O		*I*			
		T		*H*			
		S		*I*			
		D		*T*			

Tablica 6: *Ispunjavanje stupaca ispod brojeva 1 i 2*

Nakon toga prelazimo na stupac iznad kojeg je broj 3. Budući da se 3 pojavuljuje dva puta (odnosno u riječi *opasnost* slovo *o* se pojavljuje 2 puta), iduća dva slova u šifratu upisujemo u stupce ispod broja 3, tako da krenemo s lijeva na desno. Tako nastavimo sve do kraja ova dva stupca (Tablica 7).

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

Tablica 7: *Ispunjavanje stupaca ispod brojeva 1,2 i 3*

Broj 4 se pojavljuje samo jednom, stoga slova iz šifrata upisujemo u stupac ispod broja 4. Broj 5 se pojavljuje dva puta pa tu upisujemo slova iz šifrata redom u oba stupca s lijeva na desno ispod broja 5. Konačno, u stupac ispod broja 6 (budući da se samo jednom pojavljuje) upišemo ostala slova u šifratu.

O	*P*	*A*	*S*	*N*	*O*	*S*	*T*
3	4	1	5	2	3	5	6
S	*V*	*I*	*V*	*A*	*S*	*I*	*S*
N	*O*	*V*	*I*	*M*	*O*	*G*	*U*
P	*O*	*S*	*T*	*A*	*T*	*I*	*S*
T	*V*	*A*	*R*	*N*	*O*	*S*	*T*
U	*K*	*O*	*L*	*I*	*K*	*O*	*I*
M	*A*	*T*	*E*	*H*	*R*	*A*	*B*
R	*O*	*S*	*T*	*I*	*S*	*L*	*I*
J	*E*	*D*	*I*	*T*	*I*	*I*	*H*

Tablica 8: *Otvoreni tekst Primjera 6*

Koristeći Tablicu 8 prošitamo otvoreni tekst čitajući po redovima i tako dobijemo

Svi vaši snovi mogu postati stvarnost ukoliko imate hrabrosti slijediti ih.

Myszkowski stupčana transpozicija ima iste prednosti i nedostatke kao i obična stupčana transpozicija. Malo je manje podložna dešifriranju pomoću anagramiranja, jer obrazac transpozicije nije tako ponavljajući. Također, ova se šifra može više puta koristiti i to je čini sigurnijom, osobito ako koristimo različite ključeve.

1.4 Cik-cak šifra

Ova šifra dobila je ime po načinu na koji se vrši šifriranje, odnosno dešifriranje (u literaturi je poznat i engleski naziv *Rail-fence* šifra). Otvoreni tekst zapisuje se silazno na paralelne „linije", odnosno zamišljene ograde, dok se ne dođe do ruba i onda se dalje zapisuje uzlazno do vrha. Postupak se ponavlja dok se ne dođe do kraja otvorenog teksta. Nakon toga šifrirani se tekst dobije paralelnim čitanjem po redovima.

Da bi šifrirali otvoreni tekst koristeći cik-cak šifru, otvoreni tekst se treba napisati u cik-cak redove duž stranice i tada pročitati svaki red. Prvo je potrebno imati ključ, koji predstavlja broj redova koji ćemo imati. Nakon toga pišemo slova otvorenog teksta dijagonalno dolje na desno, sve dok ne dostignemo broj redova određenih ključem. Nakon toga se "vratimo" nazad gore, sve dok ne dođemo do prvog reda. Ovaj proces se nastavlja sve do kraja otvorenog teksta, (preuzeto iz [6]).

Primjer 7. *Šifrirajmo otvoreni tekst*

Dok god ima mraka bit će i svanuća

cik-cak šifrom s ključem 4.

Rješenje:

D						I						K						E						U			
	O				D		M				A		A				C		I				N		C		
		K		O				A		R				B		T				S		A				A	
			G						M						I						V						X

Tablica 9: *Rješenje Primjera 7*

Ovdje smo Ć poistovjetili sa C. Na kraju otvorenog teksta ubacili smo X. Znak X ubacuje se tako da bi otvoreni tekst stao u mrežu (tako da u prvom i zadnjem redu bude jednak broj slova). Iako nije potrebno, proces dešifriranja je jednostavniji ako otvoreni tekst ima ovaj oblik (Tablica 9). Šifrat se čita po redovima, tako da u našem slučaju imamo:

DIKEU ODMAA CINCK OARBT SAAGM IVX.

Dešifriranje cik-cak šifrom uključuje rekonstrukciju dijagonalne mreže korištene za šifriranje otvorenog teksta. Započinjemo pisati poruku ali ostavimo crticu na mjesto prostora koji nije zauzet. Napravimo mrežu s brojem redova koliko iznosi ključ te brojem stupaca koliko je slova u otvorenom tekstu. Zatim postavimo prvo slovo u gornjem lijevom kvadratu i crtu dijagonalno prema dolje gdje će biti slova. Kada se vratimo na gornji red, stavljamo sljedeće slovo u šifriranom tekstu. Ovako nastavimo preko reda i započnemo sljedeći redak kada dođemo do kraja prvog reda.

Primjer 8. *Dešifrirajmo šifrat*

SVTJE VAIOI IETSI RZVSL PIKPI UII

dobiven cik-cak šifrom s ključem 4 iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Slovo S stavimo na prvo mjesto u našoj mreži. Zatim stavimo crtice dijagonano dolje pa gore sve dok ne dođemo do prvog reda. Nakon toga stavimo drugo slovo iz šifrata (slovo V) i nastavimo popunjavati prvi red dok ne dobijemo uzorak kao u Tablici 10.

S						V						T						J						E			
	-				-		-				-		-						-				-		-		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-

Tablica 10: *Prvi korak dešifriranja*

Ovaj postupak nastavimo red po red i dobijemo traženi otvoreni tekst kako je prikazano po koracima (Tablice 11, 12 i 13).

S						V						T						J						E			
	V				A		I				O		I				I		E				T		S		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-

Tablica 11: *Drugi korak dešifriranja*

S						V						T						J						E			
	V				A		I				O		I				I		E				T		S		
		I		R				Z		V				S		L				P		I				K	
			-						-						-						-						-

Tablica 12: *Treći korak dešifriranja*

S						V						T						J						E			
	V				A		I				O		I				I		E				T		S		
		I		R				Z		V				S		L				P		I				K	
			P						I						U						I						I

Tablica 13: *Četvrti korak dešifriranja*

U četvrtom koraku možemo pročitati otvoreni tekst prateći dijagonalu kako bismo dobili:

Svi pravi životi su lijepi i teški.

Cik-cak šifra veoma je jednostavna za primjenu. Ali ona nije osobito sigurna, budući da imamo ograničen broj mogućih ključeva, osobito za kraće šifre. Da bi postojalo dovoljno "kretanja" slova, duljina poruke mora biti najmanje dvaput veća od vrijednosti ključa. Ovako kratke šifre možemo dešifrirati prilično brzo "grubom silom" a još brže računalom.

1.5 Šifra obrnutog uzorka

Ona je razrađena tehnika premještanja slova *cik-cak* šifre. Tu se koristi pravokutna mreža (u daljnjem tekstu ćemo govoriti matrica). Pogledajmo to na idućem primjeru otvorenog teksta:

Sve je lako kad si mlad.

Ova poruka ima 18 slova. Kako bismo dobili višekratnik broja 4 dodajemo dva znaka X. Za 20 slova će biti zgodno koristiti matricu 4×5. Poruka s dva X na kraju je napisana u 20 polja s lijeva na desno i od gore prema dolje (Tablica 14).

S	V	E	J	E
L	A	K	O	K
A	D	S	I	M
L	A	D	X	X

Tablica 14: *Matrica primjera: Sve je lako kad si mlad*

Idući korak je pratiti na matrici određeni put, čiji je oblik unaprijed dogovoren s onim osobama koje će koristiti taj otvoreni tekst. Nije dobro započeti put s lijeva na desno, od prvog retka prema zadnjem, zato što bi šifrat onda započeo s riječi SVE, (što je riječ u hrvatskom jeziku) a to bi moglo pružiti trag pri dešifriranju. Dobar put je *plovni put* (engl. plow path), (Tablica 15) (ime je dobio po uzorku koji nastaje prilikom obrade zemlje, kako je prikazano u [6, str.14]).

S	V	E	J	E
L	A	K	O	K
A	D	S	I	M
L	A	D	X	X

Tablica 15: *Plovni put*

Ako pratimo ovaj put tada će šifrat u blokovima od po četiri slova biti

XMKE JOIX DSKE VADA LALS.

Da bismo dešifrirali šifrat trebamo nacrtati matricu 4×5 i tu matricu ispuniti sa slovima šifrata. Prvo slovo šifrata X ide u donji desni kut, M ide u polje iznad X. Tako nastavimo dalje popunjavati matricu koristeći isti put za šifriranje. Otvoreni tekst se čita s lijeva na desno od gornjeg reda prema zadnjem. Još jedan dobar put je

spiralni put. Spirala se može započeti iz bilo kojeg vrha i onda vrtjeti prema unutra, ili u smjeru kazaljke na satu, ili obratno, ili se može započeti s jednim središnjim vrhom i spiralno ići prema vrhovima (Tablica 16).

S	V	E	J	E
L	A	K	O	K
A	D	S	I	M
L	A	D	X	X

Tablica 16: *Spirala prema unutra*

Ukoliko bismo koristili spiralni put od unutarnjeg vrha naš bi šifrat izgledao ovako

KOIS DAVE JEKM XXDA LALS.

U slučaju ako želimo otežati dešifriranje šifrata, možemo kombinirati dva različita puta. Na primjer, otvoreni tekst možemo napisati u matricu koristeći *plovni put* umjesto s lijeva na desno. Za šifriranje možemo uzeti spiralni put.

Osoba koja šalje i osoba koja prima šifrat moraju se najprije dogovoriti koju će metodu koristiti, kao i za dimenzije matrice. Putove kako ćemo čitati šifrat možemo odrediti na razne načine: možemo uzeti stupce pa ići s lijeva na desno (na primjer, počnemo svaki stupac od dolje i idemo prema gore). Također možemo koristiti i dijagonale za staze, s prekidima ili neprekidne. Možemo uzeti bilo koji oblik puta sve dok pošiljatelj i primatelj točno znaju koji put (ili putevi) su korišteni.

Primjer 9. *Šifrirajmo otvoreni tekst*

U kamenu ništa ljudsko u ljudima sve kameno

koristeći šifru obrnutog uzorka, kombinirajući dva različita puta, tako što ćemo otvoreni tekst napisati u matricu koristeći plovni put, a za šifriranje uzeti spiralni put.

Rješenje:

Najprije napišemo otvoreni tekst u matricu 6×6. Polja ispunjavamo koristeći plovni put. Slovo LJ ćemo razdvojiti na dva slova L i J, slovo Š poistovjetiti ćemo sa S (Tablica 17).

K	E	O	K	U	N
A	V	U	S	N	E
M	S	L	D	I	M
E	A	J	U	S	A
N	M	U	J	T	K
O	I	D	L	A	U

Tablica 17: *Plovni put za Primjer 9*

Šifrat dobivamo čitajući po spiralnom putu (Tablica 18).

K	E	O	K	U	N
A	V	U	S	N	E
M	S	L	D	I	M
E	A	J	U	S	A
N	M	U	J	T	K
O	I	D	L	A	U

Tablica 18: *Spiralni put za Primjer 9*

Dakle, šifrat glasi

KAMEN OIDLA UKAME NUKOE VSAMU JTSIN SULJU D.

2 Transpozicija pomoću rešetki

Još jedna poznata metoda transpozicijskih šifri temelji se na upotrebi rešetke koja je uglavnom kvadrat, podijeljen na manje kvadrate. Ti kvadrati mogu ili ne moraju biti otvori. Otvori služe za upisivanje teksta nakon što se takva rešetka položi na papir. Postoje dvije vrste rešetaka, one sa slučajno odabranim otvorima i rešetke s otvorima odabranim na primjeren način. Stoga opišimo svaku od njih.

2.1 Cardanova rotirajuća rešetka

Cardanova rotirajuća rešetka ime je dobila po talijanskom matematičaru Girolamu Cardanu, temelji se na rešetki u obliku kvadrata, čije su dimenzije u originalu bile 6×6. Kvadrat ovih dimenzija podijeli se na četiri jednaka kvadrata dimenzija 3×3. Danas se mogu koristiti i druge dimenzije, ali bi duljina stranice kvadrata trebala biti parna (vidjeti u [3, str.37]). U svaki taj kvadrat upisuju se brojevi od jedan do devet i to na sljedeći način:

- U prvi kvadrat koji se nalazi gore lijevo upisuju se brojevi po redovima redom od jedan do devet;
- U drugi kvadrat koji se nalazi gore desno upisuju se brojevi redoslijedom koji se dobije iz prvog rotacijom za 90° u smjeru kazaljke na satu;
- U treći kvadrat koji se nalazi dolje desno upisuju se brojevi redoslijedom koji se dobije iz prvog rotacijom za 180° u smjeru kazaljke na satu;
- U četvrti kvadrat koji se nalazi dolje lijevo upisuju se brojevi redoslijedom koji se dobije iz prvog rotacijom za 270° u smjeru kazaljke na satu (Tablica 19).

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

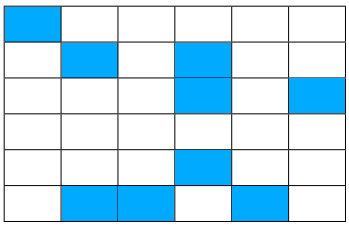
Tablica 19: *Cardanova rotirajuća rešetka*

Nakon ovog postupka iz cijelog kvadrata izabere se svaki od brojeva od jedan do devet točno jedanput. Te izabrane pozicije označavaju otvore u rešetki.

Primjer 10. *Šifrirajmo otvoreni tekst*

Napad u podne Sve jedinice nek budu spremne

s Cardanovom rotirajućom rešetkom zadanom s



Rješenje:

Prvo unosimo prvi blok od devet slova. Nakon toga rotiramo rešetku za 90°. Zatim unosimo drugi blok i rotiramo ponovo za 90°. Nakon svakog koraka se rotira rešetka i unosi novi blok slova.

- Prvi blok: NAPADUPOD
- Drugi blok: NESVEJEDI
- Treći blok: NICENEKBU
- Četvrti blok: DUSPREMNE

Pri tome pazimo na otvore u rešetci.

N					
	A		P		
			A		D
			U		
	P	O		D	

Tablica 20: *Prvi korak*

N					N
E	A		P	S	
V			A		D
	E		J	E	
D			U		
	P	O	I	D	

Tablica 21: *Drugi korak*

N	N		I	C	N
E	A	E	P	S	
V			A		D
N	E	E	J	E	
D		K	U	B	
	P	O	I	D	U

Tablica 22: *Treći korak*

N	N	D	I	C	N
E	A	E	P	S	U
V	S	P	A	R	D
N	E	E	J	E	E
D	M	K	U	B	N
E	P	O	I	D	U

Tablica 23: *Četvrti korak*

Šifrirani tekst je

NNDICN EAEPSU VSPARD NEEJEE DMKUBN EPOIDU.

Pri dešifriranju, osoba koja primi šifriranu poruku prvo crta testni kvadrat 6×6, potom piše šifrirani tekst u ćelije koristeći redove s lijeva na desno i od vrha prema dolje. Nakon toga postavlja kopiju rešetke preko kvadrata u prvoj poziciji. Idući korak je kopirati slova koristeći metodu koja je dogovorena prije slaganja slova u otvore rešetke. Nakon što je kopirano 9 slova, rešetka se okreće za pravi kut. Nakon toga rešetka se ponovo rotira za novih 90 stupnjeva u drugu poziciju, a zatim se kopira novih 9 slova. Nakon još dva okretanja rešetke, bit će zapisano 36 slova originalne poruke u pravilnom redoslijedu.

Primjer 11. *Dešifrirajmo šifrat*

LEIETA ISMTII LBWSLI SADEYU SMPOSO NTNIES

dobiven iz engleskog jezika s Cardanovom rotirajućom rešetkom zadanom s

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

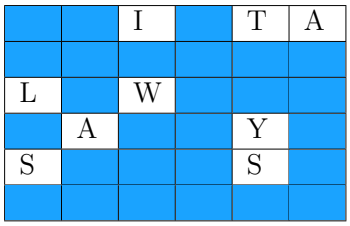
Rješenje:
Najprije u testni kvadrat upišemo šifrat (Tablica 24).

L	E	I	E	T	A
I	S	M	T	I	I
L	B	W	S	L	I
S	A	D	E	Y	U
S	M	P	O	S	O
N	T	N	I	E	S

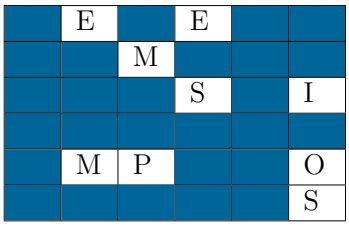
Tablica 24: *Šifrat iz Primjera 11 upisan u testni kvadrat*

Zatim postavljamo kopiju rešetke preko kvadrata u prvoj poziciji. Tako dobijemo prvih 9 slova otvorenog teksta: *ITALWAYSS* (Tablica 25). Nakon toga okrećemo rešetku za 90° u smjeru kazaljke na satu. Tako dobivamo novih 9 slova otvorenog teksta: *EEMSIMPOS* (Tablica 26). Nastavljajući tako, dobivamo otvoreni tekst:

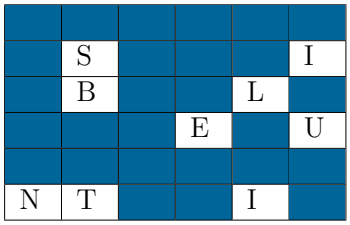
It always seems impossible until it is done.



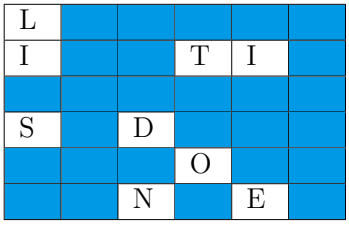
Tablica 25: *Prvi korak*



Tablica 26: *Drugi korak*



Tablica 27: *Treći korak*



Tablica 28: *Četvrti korak*

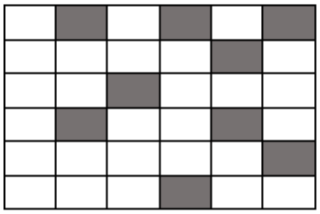
U romanu "Mathias Sandorff" (1855.), Julesa Vernea korištena je rotirajuća kvadratna rešetka za šifriranje. 1867. godine dva sitna kriminalca Sarcany i Zirone su presreli goluba pismonošu. Na njegovoj nozi pronašli su šifriranu poruku. Zajedno s korumpiranim bankarom Silasom Torontalom dešifrirali su šifru te policiji u zamjenu za bogatu nagradu izručili urotnike. Urotnici su htjeli odcijepiti Mađarsku od Austro-Ugarske. Šifrirana poruka je glasila

IHNALZ ARNURO ODXHNP AEEEIL SPESDR EEDGNC
ZAEMEN TRVREE ESTLEV ENNIOS ERSSUR TOEEDT
RUIOPN MTQSSL EEUART NOUPVG OUITSE ERTUEE.

Sarcany i Torontal pronašli su odgovarajuću rotirajuću rešetku (poznatu kao i Fleissnerovu rešetku (Slika 2.), koja je ime dobila po austrijskom kriptografu Eduardu Fleissneru von Wostrowitzu).

Rotirajući rešetku u smjeru obrnutom od kazaljke na satu dobivamo:

HAZRXEIRG NOHALEDEC NADNEPEDN ILRUOPESS
AMNETNORE VELESSUOT ETSEIRTED ZERREVNES
UONSUOVEU QLANGISRE IMERPUATE RPTSETUOT.



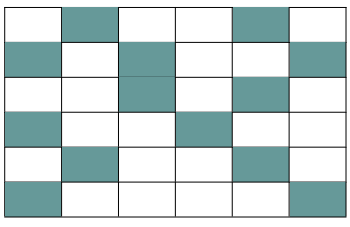
Slika 2. *Korištena Fleissnerova rešetka*

Čitajući unatrag dobivamo otvoreni tekst

Tout est prêt. Au premier signal que vous nous enverrez de Trieste, tous se lèveront en masse pour l'indépendance de la Hongrie. Xrzah. Prevedemo li to na hrvatski jezik dobivamo: *Sve je spremno. Na prvi znak koji nam pošaljete iz Trsta, sve će se podići masovno za neovisnost Mađarske. Xrzah.*, (vidjeti u [3] i [4]).

2.2 Transpozicija pomoću rešetki sa slučajno odabranim otvorima

Ova vrsta šifre zahtijeva da pošiljatelj i primatelj teksta posjeduju istu rešetku koja će se koristiti prilikom šifriranja, odnosno dešifriranja. Kod ove šifre, raspored otvora na rešetki je proizvoljan i ovisi o dogovoru između pošiljatelja i primatelja. Kad se takva rešetka položi na papir u otvore upisujemo otvoreni tekst. Nakon micanja rešetke na preostala se mjesta upisuju proizvoljna slova te se na taj način skriva poruka. Tako na primjer riječ KRIPTOGRAFIJA možemo šifrirati na sljedeći način:



A	K	S	L	R	U
I	G	P	A	D	T
N	L	O	J	G	I
R	T	E	A	Z	R
V	F	K	Z	I	H
J	C	P	F	T	A

Tablica 29: *Šifriranje pomoću rešetke sa slučajno odabranim otvorima*

2.3 Trellis šifra

Ovaj oblik slanja skrivenih poruka koristili su Englezi u 16. stoljeću. Špijun kraljice Elizabete I, sir Francis Walsingham (1530–1590), koristio je rešetke u komunikaciji sa svojim agentima. *Trellis*, odnosno rešetke, predstavljaju oblik transpozicije u obliku šahovnice koji podsjeća na Rail-fence šifru. Primjerice, otvoreni tekst *Send money with all speed to our friend Jack in Antwerp at the Golden Lion Inn x,* pomoću trellis šifre šifriramo na sljedeći način: Slova najprije upisujemo u bijela polja na šahovnici (u slučaju da se slova otvorenog teksta upisuju okomito, šifrat se čita vodoravno i obrnuto.) Nakon što se ispune 32 polja, prelazi se na crna polja (u slučaju da poruka ima manje od 64 slova, prazna polja se ispunjuju znakom X ili nulom). U slučaju ako bude više od 64 slova, potreban je još jedan papir (još jedna šahovnica) (Slika 3).

SLIKA 3. *Šifriranje pomoću Trellis šifre*

Sada iščitamo šifrat:

JMTHH DLISI YPSLU IAOWA ETIEE NWAPD ENENE LGOON NAITE EFNKE RLOON DDNTT ENRX.

Primjer 12. *Šifrirajmo otvoreni tekst*

Napadnite Francusku. Vojska neka čeka u Doveru. Brodovima otplovite u Calais.

koristeći Trellis šifru.

Rješenje:

Prva 32 slova upisujemo u bijela polja na šahovnici. Nakon toga, preostalih 32 slova upisujemo u crna polja kako je prikazano u Tablicama 30 i 31. Slovo Č ćemo poistovijetiti sa C.

	D		N		J		C
N		E		K		N	
	N		C		S		E
A		F		U		E	
	I		U		K		K
P		R		V		K	
	T		S		A		A
A		A		O		A	

Tablica 30: *Prvi korak*

U		R		O		E	
	E		V		O		L
D		O		T		U	
	R		I		V		A
O		D		P		C	
	U		M		I		I
V		O		L		A	
	B		A		T		S

Tablica 31: *Drugi korak*

Preklapanjem ove dvije tablice dobivamo traženi šifrat (Tablica 32).

U	D	R	N	O	J	E	C
N	E	E	V	K	O	N	L
D	N	O	C	T	S	U	E
A	R	F	I	U	V	E	A
O	I	D	U	P	K	C	K
P	U	R	M	V	I	K	I
V	T	O	S	L	A	A	A
A	B	A	A	O	T	A	S

Tablica 32: *Rješenje Primjera 12*

Naš šifrat glasi

UDRNO JECNE EVKON LDNOC TSUEA RFIUV EAOID UPKCK PURMV IKIVT OSLAA AABAA OTAS.

Ova transpozicijska šifra nije zadovoljavajuće sigurna te je pogodna jedino za brze i letimične poruke. Kako bi se šifra poboljšala nije loše dva puta ponoviti postupak.

3 Kombinacija transpozicije i supstitucije

Transpozicijske šifre su s kriptografskog gledišta visoko cijenjene zbog svoje jednostavnosti. One mogu imati nedostataka tako što ako se jedno slovo ispusti ili doda, proces dešifriranja može se otežati. Čista tranpozicija bez prateće supstitucijske šifre teško pruža garanciju za kriptografsku sigurnost (vidjeti u [5]). Transpozicija je učinkovita kada se koristi s frakcionalnom supstitucijom. Prema [4] *frakcionalna supstitucija* je proces u kojem se svako slovo otvorenog teksta šifrira s nekoliko simbola (najčešće slova ili brojeva). Primjerice, slova možemo napisati u mrežu, te svako slovo zamijeniti s njegovim koordinatama (najpoznatiji ovakav oblik je Polybiusov kvadrat). Polybiusov kvadrat izmislio je grčki povjesničar i znanstvenik Polybius. Izmislio je kvadrat u svrhu smanjivanja broja znakova u tekstu. U Tablici 33 možemo vidjeti osnovni oblik Polybiusovog kvadrata s engleskom abecedom. Dakle, slova engleske abecede zapisujemo u 5×5 matricu. Redovi i stupci se numeriraju od 1 do 5 tako da svako slovo predstavlja odgovarajući par retka i stupca.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Tablica 33: *Osnovni oblik Polybiusovog kvadrata*

Možemo primijetiti da slova I i J dijele istu ćeliju. Također, može se dogoditi da slova V i W dijele istu ćeliju, ovisno o kojoj se vrsti abecede radi. Primjerice riječ *Stol* zapisali bi kao 43443431. Ako imamo Polybiusov kvadrat s ključnom riječi onda najprije zapisujemo slova te ključne riječi pa nastavimo dalje abecedno popunjavati tablicu. Primjeri šifri koje koriste kombinaciju Polybiusovog kvadrata i transponiranja su: ADFGVX šifra, Bifidska šifra i Trifidska šifra.

3.1 ADFGVX šifra

Jedan od najinteresantnijih i najpraktičnijih načina u kojoj se kombiniraju supstitucija i transpozicija u jednom "sistemu" je poznat kao ADFGVX šifra.

ADFGVX šifru je koristila njemačka vojska za vrijeme Prvog svjetskog rata. Prvi put se pojavila 5. ožujka 1918. godine, a osmislio ju je njemački časnik za

veze Fritz Nebel. Prema [5], ADFGX šifra korištena je za šifriranje radio poruka na zapadnoj fronti. Slova ADFGX su izabrana zato što ona u Morseovom kodu imaju najmanje sličnosti te se zbog toga može smanjiti broj grešaka u prijenosu poruke. Nakon tri mjeseca korištenja, šifra ADFGX dobila je slovo V da bi se omogućilo slanje brojeva. Za šifriranje i dešifriranje poruka koristi se izmijenjeni Polybiusov kvadrat gdje se umjesto brojeva koriste slova. Kod šifre ADFGX on ima dimenzije 5×5, dok kod šifre ADFGVX dimenzije 6×6. Kod ADFGX šifre Polybiusov kvadrat ima 25 znakova, 25 slova abecede (u englesekom jeziku se slova I i J spajaju u jednu ćeliju, a u hrvatskom jeziku slova V i W.) Koordinate redova i stupaca su slova ADFGVX /ADFGX korištena u paru, te se kasnije koriste kao zamjena slova u tekstu. Ta se slova onda upisuju u tablice i podvrgavaju stupčanoj transpoziciji.

Primjer 13. *Šifrirajmo otvoreni tekst*

Napad na Englesku

ADFGX šifrom uz ključne riječi SUNCE i VOJNIK.

Rješenje:

Da bi šifrirali ovaj otvoreni tekst, najprije napravimo Polybiusov kvadrat s prvom ključnom riječi SUNCE. Budući da je otvoreni tekst na hrvatskom jeziku možemo poistovjetiti slova V i W (Tablica 34).

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

Tablica 34: *Polybiusov kvadrat s ključnom riječi SUNCE*

Nakon toga pronalazimo od svakog slova otvorenog teksta odgovarajući par slova (Tablica 35).

N	A	P	A	D	N	A	E	N	G	L	E	S	K	U
AF	DA	GF	DA	DF	AF	DA	AX	AF	DX	FX	AX	AA	FG	AD

Tablica 35: *Odgovarajući parovi slova za svako slovo otvorenog teksta*

Nakon toga uzimamo tekst i upisujemo ga po redovima u tablicu ispod ključne riječi VOJNIK. Također numeriramo slova ključne riječi po abecednom poretku (Tablica 36).

6	5	2	4	1	3
V	O	J	N	I	K
A	F	D	A	G	F
D	A	D	F	A	F
D	A	A	X	A	F
D	X	F	X	A	X
A	A	F	G	A	D

Tablica 36: *Stupčana transpozicija s ključnom riječi VOJNIK*

Šifrat se sada čita po stupcima, poredanim abecedno s obzirom na slova ključne riječi. Šifrat glasi

GAAAA DDAFF FFFXD AFXXG FAAXA ADDDA.

Ako želimo dešifrirati šifrat šifriran ADFGVX šifrom moramo najprije opovrgnuti stupčanu transpoziciju zapisujući šifrat u stupce u pravom redu, a nakon toga pretvoriti parove slova u odgovarajuće slovo koristeći Polybiusov kvadrat.

Primjer 14. *Dešifrirajmo šifrat*

VFAVF GGAAF VDDDV GADVD XAGA

šifriran ADFGVX šifrom uz ključne riječi OTMICA i BERLIN iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Najprije pišemo ključnu riječ za transpoziciju OTMICA i numeriramo slova abecedno. Šifrat ima 24 slova, stoga će naša tablica imati četiri reda i šest stupaca. Šifrat upisujemo po stupcima poredanim po brojevima (abecedni poredak slova ključne riječi) (Tablica 37).

A	C	I	M	O	T
1	2	3	4	5	6
V	F	A	D	A	X
F	G	F	D	D	A
A	G	V	V	V	G
V	A	D	G	D	A

O	T	M	I	C	A
5	6	4	3	2	1
A	X	D	A	F	V
D	A	D	F	G	F
V	G	V	V	G	A
D	A	G	D	A	V

Tablica 37: *Stupčana transpozicija s ključnom riječi OTMICA*

Čitajući po redovima dobivamo: AXDAFV DADFGF VGVVGA DAGDAV. Sada moramo generirati kvadrat koristeći ključnu riječ BERLIN. U drugi red kvadrata (ispod slova ADFGVX) upisujemo redom slova naše ključne riječi. Nakon što ispišemo sva slova ključne riječi, kvadrat dalje nastavljamo ispunjavati s ostalim slovima abecede, a zatim brojevima od 0 do 9 (Tablica 38).

	A	D	F	G	V	X
A	B	E	R	L	I	N
D	A	C	D	F	G	H
F	J	K	M	O	P	Q
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Tablica 38: *Polybiusov kvadrat s ključnom riječi BERLIN*

Sada za svaki par slova u šifratu pronalazimo iz kvadrata odgovarajuće slovo. (Primjerice, u gornjem kvadratu GF označava slovo U, tj. gledamo presjek reda i stupca koje čine ta dva slova) (Tablica 39).

AX	DA	FV	DA	DF	GF	VG	VV	GA	DA	GD	AV
N	**A**	**P**	**A**	**D**	**U**	**1**	**2**	**S**	**A**	**T**	**I**

Tablica 39: *Odgovarajuće slovo iz Polybiusovog kvadrata za odgovarajući par slova šifrata*

Dakle, otvoreni tekst glasi

Napad u 12 sati.

Još različitih primjera šifriranja i dešifriranja ADFGVX šifrom može se vidjeti u [7].

3.2 Bifidska šifra

Bifidska šifra je još jedna šifra koja kombinira Polybiusov kvadrat i transpoziciju. Njezin tvorac je francuski kriptograf Felix Delastele, 1895.g. Ova šifra nikada nije korištena u vojne ili vladine svrhe, jedino od strane kriptoanalitičara. Ovdje također imamo Polybiusov kvadrat te slova engleske abecede zapisujemo u 5×5 matricu. Redovi i stupci se numeriraju od 1 do 5. U procesu supstitucije svako slovo otvorenog teksta je zamijenjeno s dvije komponente (α i β koja predstavljaju stupac i red gdje je slovo otvorenog teksta), u procesu transpozicije se parovi komponenata (α, β) razdvajaju i tvore novi parovi, te ponovno proces suptitucije u kojima svaki novi par komponenata dobiva novu vrijednost slova prema izvornom bifidskom alfabetu, kako je prikazano u [5]. Pogledajmo kako to izgleda na primjeru:

Primjer 15. *Šifrirajmo otvoreni tekst*

Zavadi pa vladaj

bifidskom šifrom uz ključnu riječ RAT.

Rješenje:

Budući da je otvoreni tekst na hrvatskom jeziku u Polybiusovom kvadratu poistovjetiti ćemo slova V i W (Tablica 40).

	1	2	3	4	5
1	R	A	T	B	C
2	D	E	F	G	H
3	I	J	K	L	M
4	N	O	P	Q	S
5	U	V/W	X	Y	Z

Tablica 40: *Polybiusov kvadrat s ključnom riječi RAT*

Da bismo šifrirali otvoreni tekst, napišemo ga u tablicu, a onda za svako slovo napišemo odgovarajući red i stupac ispod svakog slova (Tablica 41).

Z	A	V	A	D	I	P	A	V	L	A	D	A	J
5	1	5	1	2	3	4	1	5	3	1	2	1	3
5	2	2	2	1	1	3	2	2	4	2	1	2	2

Tablica 41: *Odgovarajući red i stupac svakog slova otvorenog teksta*

Zatim zapišemo brojeve (čitamo po redovima) pa imamo 51 51 23 41 53 12 13 52 22 11 32 24 21 22. Onda iz Tablice 40 isčitamo slova. Šifrat glasi

UUFNX ATVER JGDE.

Kod dešifriranja koristi se obratni proces. Pogledajmo to na sljedećem primjeru.

Primjer 16. *Dešifrirajmo šifrat*

ILBDA KTRKG AIE

dobiven bifidskom šifrom uz ključnu riječ RAT iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Najprije iz Tablice 40 iščitamo koordinate svakog slova. Budući da naš šifrat ima 13 slova (svako slovo kod bifidske šifre ima dvije koordinate) imamo 26 brojeva. Prvih 13 brojeva stavimo u prvi red (označava retke u Polybiusovom kvadratu), a drugih 13 brojeva stavimo u drugi red (označava stupce u Polybiusovom kvadratu) (Tablica 42).

I	L	B	D	A	K	T	R	K	G	A	I	E
3 1	3 4	1 4	2 1	1 2	3 3	1 3	1 1	3 3	2 4	1 2	3 1	2 2

Tablica 42: *Odgovarajući red i stupac za svako slovo šifrata*

Sada po redovima i stupcima isčitamo iz Polybiusovog kvadrata slova našeg otvorenog teksta (Tablica 43). Dobivamo otvoreni tekst

Kriptografija.

3	1	3	4	1	4	2	1	1	2	3	3	1
3	1	1	3	3	2	4	1	2	3	1	2	2
K	**R**	**I**	**P**	**T**	**O**	**G**	**R**	**A**	**F**	**I**	**J**	**A**

Tablica 43: *Rješenje Primjera 16*

3.3 Trifidska šifra

Felix Delastelle je oko 1901. godine također konstruirao i Trifidsku šifru. Ona je proširena verzija bifidske šifre. Ima "tri dimenzije" tako da je svaki element frakcioniran u tri elementa umjesto u dva. Dok bifidska šifra koristi Polybiusov kvadrat da bi pretvorila svako slovo u koordinate koristeći 5×5 kvadrat, trifidska mreža ih pretvara u koordinate u 3×3×3 kocki. Kao i kod bifidske šifre i kod trifidske šifre se kombinira transpozicija kako bi se postigla difuzija, tj mješanje dviju vrsta šifriranja. Trifidska šifra koristi sustav TABLICA, RED, STUPAC (ili neku permutaciju tog skupa). U Tablici 44 vidimo prikaz kocke u trifidskoj šifri s ključnom riječi KRIPTOGRAFIJA.

	1	**2**	**3**
1	K	R	I
2	P	T	O
3	G	A	F

	1	**2**	**3**
1	J	B	C
2	D	E	H
3	L	M	N

	1	**2**	**3**
1	Q	S	U
2	V	W	X
3	Y	Z	.

Tablica 44: *Primjer kocke u trifidskoj šifri s ključnom riječi KRIPTOGRAFIJA*

Nakon toga isčitamo koordinate svakog slova. Ubuduće ćemo koristiti sustav tablica, red, stupac. Tako su na primjer, koordinate slova O 123, odnosno prva koordinata predstavlja tablicu, druga red, a treća stupac gdje se nalazi slovo. Prilikom šifriranja ispod svakog slova otvorenog teksta upisujemo tri koordinate, nakon toga isčitamo brojeve (prvi, drugi pa treći red), a zatim grupiramo trojke i ponovno iz trifidske kocke isčitamo slova šifrata.

Primjer 17. *Šifrirajmo otvoreni tekst*

Speak less than you know

trifidskom šifrom uz ključnu riječ LEAR.

Rješenje:

Najprije napravimo kocku koja je analogija Polybiusovom kvadratu s ključnom riječi LEAR (Tablica 45).

	1	**2**	**3**
1	L	E	A
2	R	B	C
3	D	F	G

	1	**2**	**3**
1	H	I	J
2	K	M	N
3	O	P	Q

	1	**2**	**3**
1	S	T	U
2	V	W	X
3	Y	Z	.

Tablica 45: *Kocka u trifidskoj šifri s ključnom riječi LEAR*

Sada iščitamo koordinate svakog slova (Tablica 46).

A 113	H 211	O 231	V 321
B 122	I 212	P 232	W 322
C 123	J 213	Q 233	X 323
D 131	K 221	R 121	Y 331
E 112	L 111	S 311	Z 332
F 132	M 222	T 312	. 333
G 133	N 223	U 313	

Tablica 46: *Koordinate svih slova*

Zatim napišemo otvoreni tekst i dolje u tri reda koordinate za svako slovo otvorenog teksta (Tablica 47).

S	P	E	A	K	L	E	S	S	T	H	A	N	Y	O	U	K	N	O	W
3	2	1	1	2	1	1	3	3	3	2	1	2	3	2	3	2	2	2	3
1	3	1	1	2	1	1	1	1	1	1	1	2	3	3	1	2	2	3	2
1	2	2	3	1	1	2	1	1	2	1	3	3	1	1	3	1	3	1	2

Tablica 47: *Koordinate za svako slovo otvorenog teksta u Primjeru 17*

Sada iz Tablice 46 iščitamo po redovima brojeve. Dobivamo: 321 121 133 321 232 322 231 311 211 111 112 331 223 212 231 121 121 331 131 312. Onda iz tablice 43 isčitamo slova šifrata. Šifrat glasi:

VRGVP WOSH LEYN IOR RYDT.

Ako želimo dešifrirati šifrat, koristimo obratni proces. Upisali bismo koordinate slova šifrata u red, ovisno o dužini tog reda podijelili bismo ga na tri reda i onda isčitali koordinate slova otvorenog teksta.

Primjer 18. *Dešifrirajmo šifrat*

VJHLE AELTB T

trifidskom šifrom uz ključnu riječ LEAR iz otvorenog teksta na engleskom jeziku.

Rješenje:

Iz Tablice 46 isčitamo koordinate svakog slova šifrata pa dobivamo redom brojeve: 321 213 211 111 112 113 112 111 312 122 312. Ovdje imamo 33 broja, stoga ćemo ih podijeliti u tri reda po 11 brojeva (Tablica 48).

3	2	1	2	1	3	2	1	1	1	1
1	1	1	2	1	1	3	1	1	2	1
1	1	3	1	2	1	2	2	3	1	2

Tablica 48: *Koordinate slova otvorenog teksta iz Primjera 18*

Sada iščitamo slova iz Tablice 45 i dobivamo otvoreni tekst

Shakespeare.

Zaključak

Informacija danas predstavlja najvrednije dobro. Komuniciranjem prenosimo određene informacije na različite načine. No, uvijek postoji mogućnost da netko neovlašteno prati našu komunikaciju i to kasnije zloupotrijebi. Zbog toga je potrebno pronaći mehanizam koji će osigurati zaštitu tajnosti informacija, integritet i autentičnost informacija. Upravo zbog toga je šifriranje i razbijanje šifri postalo najvažniji izvor tajnih obavještajnih službi na svijetu koje imaju veliku ulogu u stvaranju politike današnjih vlada. Kriptografija, kao znanost koja se bavi metodama očuvanja tajnosti informacija, pruža rješenje ovog problema. Najbitnije je da se tajni ključ u cijelom postupku komunikacije nigdje ne šalje jer ne postoji potreba da bilo tko osim njegovog vlasnika bude upoznat s njim. Što znači da možete bilo kome poslati šifriranu poruku ako znate javni ključ osobe kojoj šaljete, a samo primatelj svojim tajnim ključem može dešifrirati poruku. Od najranijih vremena ljudi su imali potrebu za šifriranjem svojih poruka. Tako su se razvile i transpozicijske šifre. U praksi najupotrebljivanija transpozicijska šifra bila je stupčana transpozicija. Sigurnost transpozicijskih šifri može se znatno povećati korištenjem više koraka transpozicije. Većina njemačkih šifri tijekom prvog svjetskog rata su bile dvostruke transpozicijske šifre. Ove šifre su vrlo sigurne, ali njihovo dešifriranje postaje relativno jednostavno ako kriptoanalitičar raspolaže s nekoliko jednako dugih šifrata šifriranih istim ključem. U današnjem svijetu svatko od nas želi zaštiti svoje podatke koji su od velike važnosti. Upravo ova znanost nam pomaže u tome. Kriptografija je neophodna ako želimo imati svoju privatnost danas kada svijet postaje globalno selo, u elektroničkoj trgovini, u privatnoj komunikaciji te u razmjeni poslovnih informacija.

Literatura

[1] R. F. Churchhouse, *Codes and ciphers*, Cambridge University Press, Cambridge, 2001.

[2] *Crypto Corner*, dostupno na
URL: `http://crypto.interactive-maths.com/`

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

[4] H. Fouche Gaines, *Cryptanalysis a study of ciphers and their solutions*, Dover publications, New York, 1956.

[5] W. Friedman, *Military cryptanalysis*, Aegean Park Press, Laguna Hills, 1980.

[6] M. Gardner, *Codes, cihers and secret writing*, Dover Publications, New York, 1972.

[7] R. Mollin, *An introduction to cryptography*, 2nd edition, Chapman Hall/CRC, Boca Raton, 2007.

[8] S. Singh, *ŠIFRE Kratka povijest kripotgrafije*, Mozaik knjiga, Zagreb, 2003.

Sažetak

Glavna tema ovog rada su transpozicijske šifre. Pomoću njih obavlja se šifriranje, odnosno dešifriranje podataka. Ideja transpozicijske šifre je da elementi otvorenog teksta ostanu nepromijenjeni, ali da se promijeni njihov međusobni položaj.

U prvome dijelu rada definirani su osnovni pojmovi kao sto su kriptologija, kriptografija i kriptoanaliza te objašnjen postupak šifriranja i dešifriranja. Nakon formalne definicije transpozicijske šifre, naveden je i primjer skitala, prve naprave za transpozicijsko šifriranje. Zatim je bilo riječi i o permutacijskim šiframa, još jednoj od vrsta transpozicijskih šifri.

U drugome dijelu rada obrađena je stupčana transpozicija, najupotrebljivanija transpozicijska šifra. Ona je jedna od najpopularnijh šifri, zbog svoje jednostavnosti i visoke razine sigurnosti. Navedena je i Myszkowski transpozicija, jedan oblik stupčane transpozicijske šifre. Za svaku šifru dani su primjeri šifiriranja i dešifriranja te odgovarajuća rješenja. Osim ovih, navedene su i cik-cak šifra, gdje se otvoreni tekst upisuje na zamišljene ograde dok se ne dođe do ruba te Šifra obrnutog uzorka, koja je zapravo razrada cik-cak šifre.

Treći dio rada bio je posvećen metodi transpozicijskih šifri koja se temelji na upotrebi rešetke koja je uglavnom kvadrat. Osim Cardanove rotirajuće rešetke, imamo još i rešetku sa slučajno odabranim otvorima te Trellis šifru. Naposljetku, spomenut je i proces frakcioniranja u kojem se svako slovo otvorenog teksta šifrira s nekoliko simbola. Tu je najpoznatiji Polybiusov kvadrat. Opisane su i šifre koje se koriste kombinacijom transpozicije i frakcioniranja, kao što su ADFGVX šifra, Bifidska i Trifidska šifra.

Ključne riječi

Kriptografija, transpozicijske šifre, stupčana transpozicija, Cardanova rešetka, ADFGVX šifra, Polybiusov kvadrat

Summary

The main topic of this work are transposition ciphers. They are used to encrypt or decrypt data. The idea of transposition cipher is to keep the elements of the plaintext unchanged, but to change their mutual position.

In the first part of the work, basic terms such as cryptology, cryptography and cryptoanalysis have been defined and the encryption and decryption process is explained. After the formal definition of the transposition cipher, an example of scytale the first transposition encryption device is also mentioned. Then we said something about permutation ciphers, one of the types of transposition ciphers.

The second part of the work deals with the columnar transposition cipher, the most usable transposition cipher. It is one of the most popular ciphers because of its simplicity and high level of security. Myszkowski transposition cipher is also mentioned, which is one form of a columnar transposition cipher. For each cipher, examples of encryption and decryption and appropriate solutions are given. In addition to these, there is also a Rail-fence cipher, where the plaintext is entered on the concealed fences until the edge of fence and the Twisted path cipher which is actually elaboration of the Rail-fence cipher.

The third part of the work was devoted to the method of transposition ciphers based on the use of a grid that is mostly square. In addition to Cardan's rotary grid, we also have grid with randomly selected openings and the Trellis cipher. Finally, there is also a fractionation process in which each letter of the plaintext is encrypted with several symbols. There is the most famous Polybius square. Ciphers used by the transposition and fractionation combination, such as the ADFGVX cipher, Bifid and Trifid cipher, are also described.

Keywords

Cryptography, transposition cipher, columnar transposition, Cardan's grille, ADFGVX cipher, Polybius square

Životopis

Zovem se Kristina Rošić. Rođena sam 11. prosinca 1993. godine u Frankfurtu u Njemačkoj. Osnovnu školu Braće Radića u Domaljevcu završila sam 2008. godine. Tijekom osnovnoškolslog obrazovanja sudjelovala sam na županijskom natjecanju iz matematike. Srednju školu Fra Martina Nedića u Orašju, smjer opća gimnazija završila sam 2012. godine. Iste godine upisala sam Preddiplomski studij matematike na Odjelu za matematiku u Osijeku. 2014. godine prebacila sam se na Sveučilišni nastavnički studij matematike i informatike.