CROATICA • Zagreb, XLII (2018) 62: 343–364

Pregledni znanstveni rad
DOI: 10.17234/Croatica.42.22
UDK: 81'38:82
003.26:82
Primljen: 5. III. 2018.
Prihvaćen: 20. III. 2018.

KRIPTOGRAM – VRLO KRATAK UVOD

Krešimir Bagić
Filozofski fakultet Sveučilišta u Zagrebu
Odsjek za kroatistiku
ff.dubrava@gmail.com

Pojam kriptografija istodobno označava znanstvenu disciplinu koja proučava tehnike šifriranja i slanja tajnih poruka te samo umijeće šifriranja. Kriptogram je pak poruka oblikovana tajnim pismom, šifrat čitljiv jedino pošiljatelju i primatelju. Prvi dio članka sažima povijest tajnog komuniciranja prateći njegove pojavne oblike od 7. st. pr. Kr. do naših dana. Opisani su među inim: steganografija (skrivanje same poruke), transpozicijski i supstitucijski kriptogrami (koje je oblikovala klasična kriptografija) te asimetrični RSA sustav šifriranja (kojim počinje era moderne kriptografije). Drugi dio članka usredotočuje se na ulogu i pojavu kriptograma u različitim kulturnim praksama, ponajprije u enigmatici i književnosti. U tim slučajevima umjesto tajne komunikacije u prvi plan izbijaju estetsko uživanje, ludizam i privlačnost traganja. Na koncu postavlja se teza da je kriptogram u književnosti stilska figura koja eksplicitno upućuje na kriptičnost kao važno obilježje književne komunikacije.

Ključne riječi: kriptografija, kriptogram, figura, zagonetka

Uvriježeno je mišljenje da je najvažnija funkcija jezika komunikacijska te da je glavna zadaća pisma bilježiti i prenositi raznovrsna znanja i informacije kroz prostor i vrijeme. Pristaše tog mišljenja, bili lingvisti ili ne, učas će ga potkrijepiti brojnim dokazima. Kako to već biva, nije sporna branjivost uvriježenog mišljenja nego činjenica da ono gdjekad zakriva kompleksnost cjeline. Roland Barthes je ironično upozorio da smo pod teretom demokrat-

skih načela "spontano naviknuti najveću komunikaciju smatrati apsolutnim dobrom, a pismo naprednjačkom tekovinom" (2004: 34). No povijest pisma uključuje i fenomene poput cenzure, tlačenja ili zabrane pristupa. K tome pismo je često bivalo hermetično, nečitljivo, zagonetno, nerijetko mu je zadaća bila sakriti informaciju kako bi ona postala privilegij odabranih. "Kriptografija je prava vokacija pisma." – ustvrđuje Barthes. Iako je izvjesno da francuski mislilac pojam kriptografija ovdje rabi kako bi istaknuo (uvijek) neuhvatljivu prirodu pisma, njegova je tvrdnja to dragocjenija. Nakon nje rečenica poput one proučavatelja kodova Paula Lundea da se "jezik u podjednakoj mjeri koristi i za prikrivanje i za komunikaciju" (2010: 8) djeluje samorazumljivo.

NEVIDLJIVO PISMO

Načelno se razlikuju dva oblika skrivanja u pisanoj komunikaciji – steganografija i kriptografija. Steganografija (στεγανός, pokriven + γράφειν, pisati) pretpostavlja skrivanje same poruke, a kriptografija (grč. κρυπτός, skriven + γράφειν, pisati) oblikovanje tajne, šifrirane poruke koja će biti razumljiva samo pošiljatelju i primatelju.

Ljudi su na različite načine skrivali postojanje poruke. Herodot primjerice spominje priču o tiraninu Histijeju koji s perzijskog dvora poručuje Aristagori u Milet da digne ustanak.[1] Poruku je istetovirao glasniku na obrijanu glavu, pričekao da mu kosa naraste pa ga poslao na put. Kada je stigao, rekao je Aristagori da mu obrije glavu i poruka je bila isporučena. Najčešći je oblik steganografije pisanje nevidljivom (simpatetičkom) tintom. Brojni su recepti kojima se postiže da napisani tekst postane nevidljiv. Još je Plinije Stariji u 1. st. zabilježio da se nevidljiva tinta može dobiti iz mlijeka mlječike. Kroz stoljeća otkriveno je da se nevidljive poruke mogu pisati mlijekom različitih životinja, limunovim sokom, octom, štirkom, mokraćom, spermom, različitim kiselinama, mješavinama šećera i sumporne kiseline, lanenog ulja i amonijaka, olovnog oksida i negašenog vapna, spojevima u kojima su glavni sastojci kobalt, olovni oksid ili kositar.[2] Primatelj će takvu

[1] Prema Bayart 2000; Singh 2003: 16.

[2] Müller (2009) navodi više jednostavnih recepata za nevidljivu tintu te ilustrira njezinu tematizaciju u stripu i literaturi (među ostalim citira ulomak iz *Pantagruela* u kojemu Rabelaisov junak nudi svoj recept). Baveći se obavještajnim *milierom* Đuro Čukljaš (1994) kratko opisuje šezdesetak vrsta nevidljivoga pisma.

poruku moći pročitati izlažući papir suncu, zagrijavajući ga na svjetlu svijeće ili jačem plamenu, paleći ga ili kvaseći. Ovisno o postupku skrivanja pred njim će se pojaviti smeđe, zelenkasto, modro, ružičasto ili žuto pismo.

Steganografija se, osim pisanja nevidljivom tintom, bavi i kraćenjem riječi prema utvrđenom sustavu ili pak skrivanjem poruke u vidljivim tekstovima koji zbog svog sadržaja ne privlače pažnju znatiželjnika. Renesanšanin Francis Bacon (1561–1626) autor je zanimljivog steganografskog sustava – dvoslovnog alfabeta: slovima A i B šifrirao je sva 24 slova engleskoga alfabeta svoga doba:

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

Dvoslovni alfabet Francisa Bacona

Vrijedi primijetiti da se Baconov dvoslovni alfabet zasniva na istom principu kao i binarno brojčano kodiranje informacija na današnjim računalima. Zbog karaktera šifriranja šifrirani je tekst pet puta opsežniji od otvorenog teksta.

KRIPTOGRAFIJA I KRIPTOGRAM

Nazivom kriptografija ili tajnopis[3] istodobno se označavaju znanstvena disciplina koja proučava metode i tehnike šifriranja i slanja tajnih poruka te samo umijeće šifriranja. Kriptogram je prema tome poruka oblikovana tajnim pismom, šifrat čitljiv jedino pošiljatelju i primatelju. U procesu šifriranja sastavni elementi otvorenog teksta (slova, skupine slova ili slogovi) bivaju pretvoreni u dogovorene elemente kriptograma – slova, brojke, interpunkcijske, grafičke ili matematičke znakove, kemijske simbole i sl. Svrha

[3] Jezikoslovac Bulcsú László predložio je riječ *kritòpis* kao hrvatsku inačicu naziva kriptografija. Dakako i za ostale je kriptološke pojmove smislio hrvatske nazive: kriptologija je postala *kritòslôvlje*, kriptoanaliza *kritorázgloba*, a kriptogram *zakritak*. V. Škiljan 1994.

je kriptograma sigurna komunikacija preko nesigurnog komunikacijskog kanala. Klasična je situacija sljedeća: pošiljatelj i primatelj poznaju algoritam i ključ koji služe za šifriranje i dešifriranje poruke, a 'neprijatelj' nastoji presresti poruku, domoći se ključa i proniknuti u način šifriranja.

Goleme su razlike između klasične i moderne kriptografije i s obzirom na tehnike i metode šifriranja, i s obzirom na komplesnost kriptograma i s obzirom na ulogu tajnopisa u životu pojedinca i zajednice. Klasična je kriptografija od 7. st. pr. Kr. pa do druge polovice 20. st. iznjedrila brojne oblike šifriranja. Njezine su potencijale koristili vladari, ratnici, diplomati, uhode, mistici, kabalisti, alkemičari, nekromanti, policajci, ljubavnici, tragači za zakopanim blagom, znanstvenici, industrijalci, umjetnici i ljudi željni intelektualnih izazova. Ona je štitila državne, vojne, vjerske i privatne tajne.

TRANSPOZICIJSKE ŠIFRE

U klasičnoj je kriptografiji tipološki moguće lučiti dvije vrste šifri: transpozicijske i supstitucijske. U transpozicijskim šiframa slova ishodišne poruke ili otvorenog teksta mijenjaju redoslijed pojavljivanja, ali zadržavaju svoj identitet. Zapravo je riječ o tehnici anagramiranja. Što je poruka opsežnija, raste i broj potencijalnih kombinacija njezinih sastavnica. Tako primjerice rečenica od 30 slova omogućuje više od 50 milijardi kombinacija (Lunde 2010: 66). Najjednostavniji je način transpozicijskoga šifriranja tzv. izmjenična transpozicija (Singh 2003: 18) ili sustav drvene ograde (Lunde 2010: 66). Poruka se preispisuje u dva retka tako da neparna slova dospijevaju u prvi, a parna u drugi redak – kriptogram je dovršen kada se drugi redak 'zalijepi' na prvi, npr.:

otvoreni tekst: U svakom načinu jezične porabe susrećemo sve jezične funkcije.[4]
enkripcija: U V K M A I U E I N P R B S S E E O V J Z Č E U K I E
S A O N Č N J Z Č E O A E U R Ć M S E E I N F N C J
kriptogram: UVKMAIUEINPRBSSEEOVJZČEUKIESAONČNJZČEOAEUR-
ĆMSEEINFNCJ

[4] Navedena je rečenica prilagođeni citat iz članka O nekim gramatičko-leksičkim osobitostima suvremenog hrvatskog pjesništva Ive Pranjkovića. Kako bi dobila na punini značenja, navest ću mikrokontekst u kojemu se pojavljuje: "Moglo bi se čak reći da u svakom načinu jezične porabe susrećemo sve jezične funkcije. Bitan je problem u tome što su njihovi međusobni odnosi vrlo slabo istraženi. Narav svake funkcije ovisna je o hijerarhijskoj ljestvici koju čine sve jezične funkcije zajedno, a mjesto je opet ovisno o cilju komunikacije ili situaciji" (cit. prema: Pranjković 2005: 140).

Poruku je moguće i dodatno usložniti – primjerice preispisati je u tri retka ili zamijeniti mjesta susjednim slovima u već šifriranom tekstu.

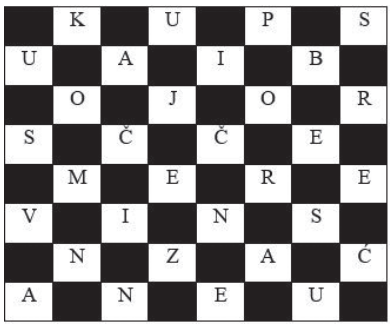
Transpozicijsko je šifriranje klica kriptografije. Naime na njezinu početku stoji skital, prvo poznato kriptografsko pomagalo. Radi se o tehnici tajne komunikacije za koju su bila potrebna dva drvena štapa jednake duljine i debljine, tj. dva skitala – jedan bi posjedovao pošiljatelj, a drugi primatelj poruke. Pošiljatelj bi oko štapa namotao vrpcu od pergamenta ili kože i na nju okomito napisao poruku. Kada bi se vrpcu odmotalo, kriptogram bi bio zgotovljen – na njoj se mogao vidjeti samo niz naizgled nepovezanih slova. Ako je vrpca bila kožna, glasnik ju je mogao okrenuti naopako i opasati se njome. Kada bi poruka došla primatelju, on bi ju namotao na svoj skital i pročitao. Komunikacijom pomoću skitala osobito su se koristili Spartanci, i to već od 5. st. prije Krista (otuda i inačica naziva – spartanski skital). Doduše, pedantni kroničari nalaze da to pomagalo još u 7. st. prije Krista spominje Arhiloh. Kasnije mit o skitalu u različitim kontekstima čuvaju i razvijaju autori poput Tukidida, Pindara, Aristofana ili Ksenofonta, a Plutarh i Aulo Gelije (Aulus Gellius) svjedoče o raširenosti upotrebe skitala kao kriptografskog sustava između 3. i 2. st. prije Krista.[5]

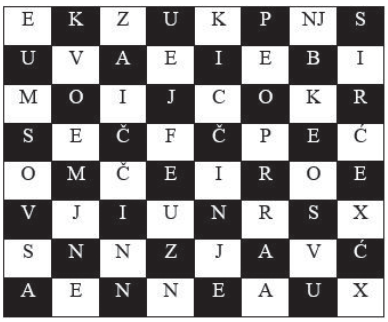
Skital (izvor: Wikipedija)

U doba renesanse sofisticiranu je transpozicijsku šifru osmislio talijanski izumitelj, matematičar i strastveni kockar Girolamo Cardano (1501–1576). Pošao je od rešetke u obliku šahovske ploče. U prvom se koraku po okomici popunjavaju 32 bijela polja. Nakon toga ploča se zakrene za 90 stupnjeva i postupak se ponavlja. Ako poruka nema dovoljno slova da bi se popunila

[5] Iscrpnu storiju o skitalu, koja uključuje njegov opis i mnoštvo citata iz djela antičkih autora, sačinila je Brigitte Collard (2004).

sva 64 polja, na njezinu se kraju dodaje neki znak po volji i ponavlja se onoliko puta koliko je praznih polja. Ako pak poruka sadrži više od 64 slova, šahovska se ploča iznova zakreće i oblikuje se kriptogram od 128 slova. Funkcioniranje Cardanove rešetke oprimjerit ću pomoću već navedene rečenice *U svakom načinu jezične porabe susrećemo sve jezične funkcije*, s tim što ću joj – zbog logike broja 64 – ovaj put dodati prezime njezina autora (*Pranjković*) i dva X.





E	K	Z	U	K	P	NJ	S
U	V	A	E	I	E	B	I
M	O	I	J	C	O	K	R
S	E	Č	F	Č	P	E	Ć
O	M	Č	E	I	R	O	E
V	J	I	U	N	R	S	X
S	N	N	Z	J	A	V	Ć
A	E	N	N	E	A	U	X

Zgotovljeni se kriptogram čita redak po redak odozgo prema dolje slijeva udesno. Pranjkovićeva rečenica, nakon prolaska kroz Cardanovu rešetku, poprima sljedeći oblik:

EKZUKPNJSUVAEIEBIMOIJCOKRSEČFČPEĆOMČEIROEVJIUNRSXSNNZJAVĆAENNEAUX[6]

SUPSTITUCIJSKE ŠIFRE

Kod supstitucijskih šifri slova otvorenoga teksta mijenjaju identitet, tj. bivaju zamijenjena drugim slovima ili znakovima, ali zadržavaju redoslijed pojavljivanja. Najstarija, a možda i najglasovitija supstitucijska šifra je ona koju je Julije Cezar rabio u Galskom ratu. Cezarovski kriptogram nastaje tako da se svako slovo otvorenog teksta zamijeni slovom koje u abecedi dolazi tri mjesta poslije njega. Moguće je dakle zamisliti postojanje otvorene i šifrirne abecede, otvorenog i šifriranog teksta. Primijenjeno na naš primjer to bi izgledalo ovako:

otvorena abeceda: a b c č ć d dž đ e f g h i j k l lj m n nj o p r s š t u v z ž

šifrirna abeceda: Č Ć D DŽ Đ E F G H I J K L LJ M N Nj O P R S Š T U V Z Ž A B C

otvoreni tekst: U svakom načinu jezične porabe susrećemo sve jezične funkcije

šifrirani tekst: ŽUAČMSOPČDŽLPŽLJHBLDŽPHŠSČĆHUŽUTHĐHOSUAHLJHBLDŽPHIŽPMDLH

Cezarova je šifra tzv. monoalfabetska šifra. Budući da se temelji na jednostavnom pomaku, kombinacija je onoliko koliko i slova abecede. To je vrlo malen broj i takvu je šifru relativno lako razbiti. Međutim monoalfabetska šifra može se oblikovati i svakovrsnim pomacima koji neće poštovati abecedni redoslijed slova, što do vrtoglavih granica uvećava broj potencijalnih kombinacija. Indijski je filozof Vātsyāyana (o. 4–6 st.) u drevnom priručniku *Kama Sutra* ženama preporučio da ljubavna iskustva razmjenjuju tajnopisom izrađenim prema nasumičnoj abecedi. Tako je izbjegnuta predvidivost cezarovskoga pomaka, ali je proces enkripcije i dekripcije znatno usložnjen.

[6] Lunde (2010: 80–81) nagađa da je mogući razlog Cardanova bavljenja kriptografijom kronični nedostatak novca zbog kojega je napisao rad o zakonima vjerojatnosti i tehnikama varanja na kocki i u kartaškim igrama. Funkcioniranje opisane rešetke, kao i nekoliko njezinih inačica, uključujući i tehniku poruke u poruci, izložio je 1545. u knjizi *Ars magna*.

Sustav je kasnije pojednostavljen uvođenjem tajnog ključa, najčešće ključne riječi ili sintagme.

Kako su se množili sustavi šifriranja, tako je bilo i sve više pokušaja njihova razbijanja. Kriptoanalizu su ustanovili arapski učenjaci potkraj prvog milenija. Ujedinivši različite discipline, ponajprije matematiku i lingvistiku, oni su ustanovili frekvencijsku analizu koja se pokazala iznimno podesnom u dešifriranju kriptograma oblikovanih supstitucijskim šiframa. Matematičar, jezikoslovac, astrolog, psiholog i meteorolog Al–Kindi (801–873) objavio je u 9. st. *Rukopis o dešifriranju kriptografskih poruka*[7] u kojemu pojašnjava da se enkriptirana poruka na poznatom jeziku razrješuje tako da se potraži neki drugi otvoreni tekst na istom jeziku dovoljno dug da se može utvrditi čestotnost pojavljivanja pojedinih slova. Kada se to učini, isti postupak valja ponoviti i sa simbolima u šifriranom tekstu.

> Tako ćemo naći slovo koje se najčešće ponavlja, pa ga sad zamijenimo »prvim« slovom uzorka, a ono koje se ponavlja odmah iza njega »drugim« slovom, a treći ćemo opet po redu među najučestalijim simbolima zamijeniti »trećim« slovom i tako dalje, dok tako ne poredamo sve simbole kriptograma koji želimo riješiti.[8]

Frekvencijska je analiza ponudila dragocjeno oruđe svima koji su nastojali proniknuti u smisao monoalfabetskih tajnih poruka. Ona se zasniva na jednostavnoj, a ispravnoj tezi da je čestotnost pojavljivanja važan element identiteta svakog slova te da nam upravo jednom utvrđeni identiteti omogućuju prepoznavanje tih slova, čak i kada su zakriveni drugim znakovima. U daljnjem razvoju frekvencijske analize – uz pomno istraživanje mogućih veza između podjednako učestalih slova i kriptografskih simbola – uspoređivale su se i relacije između podjednako učestalih dvoslova ili troslova u jeziku poruke i dvočlanih ili tročlanih dijelova kriptograma. Frekvencijska je analiza nagnala kriptografe da traže druge i drukčije, tj. sigurnije načine šifriranja.

Važan je pomak učinio Leon Battista Alberti (1404–1472), osebujni renesansni sveznadar. Biografi i povijesne knjige predstavljaju ga kao slikara, skladatelja, pjesnika i filozofa, kao projektanta prve rimske fontane Trevi i autora prve tiskane knjige o arhitekturi – *De Re Aedificatoria*, ali i kao autora prve rasprave o pitanju perspektive, rasprave o kućnoj muhi i posmrtnog govora svome psu (usp. Bayart 2000; Singh 2003: 53; Müller 2009). Alberti

---

[7] Rukopis je pronađen tek 1987. u Carigradu.

[8] Cit. prema: Singh 2003: 27.

je naime i autor prve rasprave o kriptografiji u zapadnome svijetu (*De Componendis Cyphris*, 1466/7). U njoj ističe da su poruke nastale supstitucijom na temelju jedne šifrirne abecede potencijalno lak plijen kriptoanalitičara. Stoga umjesto monoalfabetske zamjene predlaže polialfabetski sustav s dvije širfirne abecede koje će oblikovati kriptogram nedostupan frekvencijskoj analizi. Njegov se šifrirni brojčanik sastoji od dva diska – nepokretnoga vanjskog (*stabilis*) na kojemu je ispisana latinska abeceda bez slova H, K, J i Y te brojevi od 1 do 4 i pokretnoga unutrašnjeg (*mobilis*) na kojemu su ispisana slova abecede prema slučajnom rasporedu i znak &. Poruka se enkriptira čas prema jednoj čas prema drugoj abecedi, što rezultira time da isto slovo iz otvorenog teksta može biti zamijenjeno različitim slovima u kriptogramu.

Albertiev šifrirni brojčanik

Francuski diplomat Blaise de Vigenére (1523–1996) za službovanja u Italiji pomno je proučio Albertieve spise te oblikovao snažan kriptosustav koji se služi s 26 šifrirnih abeceda. O njemu je među ostalim izvijestio u svojoj *Raspravi o šiframa ili tajnopisu* (*Traité des Chiffres ou Secrètes Manières d'Escrire*, 1586).[9] Punih 300 godina vjerovalo se da je taj sustav posve siguran, toliko da je prozvan neprobojnim kodom (*le chiffre indéchiffrable*). Vigenéreov kvadrat funkcionira tako da kriptograf odredi ključnu

[9] Uz to što se novi način šifriranja vidno naslonio na Albertiev brojčanik, na više se mjesta ističe da je Blaise de Vigenère samo popularizirao kriptografski postupak koji je 1533. opisao Giovan Battista Bellaso. Dapače, nerijetko se ističe da je njemački teolog, okultist i kriptograf Johann von Tritheim sličan način šifriranja opisao 1518. u djelu *Polygraphia*. Usp. Bayart 2000; Lunde 2013: 104.

riječ (npr. JEZIK) koja će – budući petoslovna – povezati pet šifrirnih abeceda koje naizmjenično sudjeluju u enkripciji poruke. To znači da će svako slovo otvorenog teksta imati pet mogućih šifrirnih ekvivalenata. Budući da ključnu riječ čine 10, 5, 26, 9. i 11. slovo alfabeta, prvo slovo otvorenog teksta treba pomaknuti za 10, drugo za 5, treće za 26, četvrto za 9, a peto za 11 mjesta – nakon toga postupak se ponavlja.

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

Vigenéreov kvadrat (izvor: http://www.bibmath.net)

Vigenéreovu je šifru razbio ekscentrični engleski matematičar Charles Babbage (1791–1871), inače tvorac dvaju strojeva (diferencijalnog i analitičkog) koje stručnjaci tretiraju prvim računalima. Razbijanje Vigenéreove šifre (vjerojatno 1854. g.) među kriptografima se smatra najvećim kriptoanalitičkim postignućem poslije otkrića frekvencijske analize.

KRIPTOTVORCI VS. KRIPTOLOMCI

Kriptogram je u mnogim slučajevima iz komunikacijskog sredstva prerastao u moćno oružje. Priču o dvama svjetskim ratovima moguće je predočiti i kao borbu između šifrotvoraca i šifrolomaca. Presudnu važnost za trajanje i ishod Prvoga svjetskog rata imalo je dešifriranje tzv. Zimmermanova brzojava.

Radi se o brzojavu s početka 1917. godine kojim njemački ministar vanjskih poslova Arthur Zimmermann veleposlaniku u Americi poručuje da će – u slučaju da se Sjedinjene Države uključe u rat – ponuditi savezništvo Meksiku uz obećanje da će tako moći vratiti izgubljene teritorije u Americi. Poruku su presreli i dešifrirali britanski kriptoanalitičari u famoznoj Sobi 40. Kada je poruka dospjela do Bijele kuće, Amerikanci su se razbješnjeli i uključili u rat na strani Velike Britanije i Francuske što je na koncu donijelo odlučnu prevagu.

Netom po okončanju Prvoga svjetskog rata njemački je izumitelj Arthur Scherbius konstruirao šifrirni stroj Enigma koji je proglašavan neprobojnim i koji je "postao baza najvelebnijeg sustava enkripcije u povijesti" (Singh 2013: 102). Glavni dijelovi Enigme bili su tipkovnica, premetala i ploča sa žaruljicama. Kada se otvoreni tekst utipka, premetala ga enkriptiraju te se kriptogram pojavi na ploči sa žaruljicama. Primatelj, koji je poznavao dnevni ključ, trebao je samo unijeti šifriranu poruku u Enigmu i stroj bi mu ponudio otvoreni tekst. Nepoželjnima put do poruke činio se posve zatvorenim. Njemačka je vojska kupila trideset tisuća uređaja Enigma. Kako se približavao Drugi svjetski rat, u više su ga navrata poboljšavali čineći sustav šifriranja sve kompleksnijim i kompleksnijim. Od početka tridesetih godina, zahvaljujući informatoru u njemačkim redovima, Francuzi su raspolagali preciznim nacrtima Enigme i knjigama s dnevnim ključevima. Međutim njihovi su stručnjaci ubrzo svu dokumentaciju proslijedili poljskom Biurou Szyfrów. Poljaci su izgradili repliku Enigme, a kriptoanalitički tim na čelu s Marianom Rejewskim uspio je pomoću matematičkih obrazaca njemačkog jezika, statističkih podataka i poznavanja pojedinih svojstava Enigmina sustava šifriranja "broj mogućih kombinacija, koji je bio otprilike deset miljuna milijardi, smanjiti na nevjerojatnih 100 000" (v. Informatičar 2012). Dapače, Reyewski je konstruirao i tzv. bombu, uređaj za pronalaženje dnevnog ključa. Međutim kada su 1939 – neposredno prije početka rata – Nijemci uređaju dodali nova premetala, Poljaci više nisu imali snage ni novca za nastavak istraživanja te su replike Enigme i svu dokumentaciju predali saveznicima. Posao su nastavili Britanci. U londonskom Bletchley Parku osnovana je kriptoloanalitička organizacija u kojoj su surađivali matematičari, lingvisti, prirodoznanci, klasičari, šahovski velemajstori, enigmati (usp. Singh 2003: 133). Mladi je matematičar Alan Turing u golemoj količini dešifriranih poruka uočio neke stvari koje se ponavljaju – npr. da prve jutarnje poruke njemačke vojske donose vremenske izvještaje i da obično sadrže riječ *Wetter* (vrijeme). Na temelju takvih lucidnih otkrića uspoređivani su dijelovi

otvorenog i šifriranog teksta, stvarana su *kućišta*, a na temelju podataka iz kućišta izrađivane tzv. bombe koje su trebale otkriti šifrirne ključeve. Tako je tajna Enigme polako počela izlaziti na vidjelo. Britanski su šifrolomci opet nadmudrili njemačke šifrotvorce. Ne treba posebno isticati što je za saveznike značilo doznavanje njemačkih vojnih planova. Razotkrivanje Enigme simbolički je moguće motriti kao dramu epskih razmjera kojom je okončana era klasične kriptografije.

MODERNA KRIPTOGRAFIJA

Razdoblje od početka sedamdesetih godina 20. st., tj. razdoblje u kojemu glavnu ulogu preuzimaju računala, obično se uzima kao početak moderne kriptografije. Vrijeme je to u kojemu se raznovrsni oblici komunikacije množe nevjerojatnom brzinom. K tome za razliku od klasičnoga doba, kada su kriptografiji pribjegavali državnici, ratnici, uhode ili ljubavnici, tajno je pismo u naše doba postalo standardom funkcioniranja društva te nezaobilaznim dijelom svakodnevnice tzv. običnog čovjeka (bio on toga svjestan ili ne). Kriptogrami su u pozadini bankarskih transakcija, elektroničkog poslovanja i trgovine, elektroničkih identiteta, elektroničkog novca, digitalne komunikacije; rabimo ih kada kupujemo, otključavamo bicikl ili obavljamo različite radnje utipkavanjem sve brojnijih pinova i kodova. Kriptirani su podaci u digitalnom obliku, računala automatski izvode kompleksne matematičke operacije kriptiranja i dekriptiranja. Kriptografija je doslovce upala u naš svakodnevni život, ustvrđuje Bayart (2000), a mi joj i dalje slijepo vjerujemo.

Najveću je revoluciju u kriptografiji 20. stoljeća "izazvao razvoj tehnika za svladavanje problema distribucije ključa" (Singh 2003: 171). U klasičnoj kriptografiji pošiljatelj šifrira poruku i šalje ju primatelju, ali da bi ju primatelj mogao dekriptirati pošiljatelj mu mora sigurnim kanalom poslati ili mu fizički dostaviti tajni ključ. To ponekad može biti izrazito nespretno i komplicirano. Klasični su kriptosustavi simetrični sustavi – pošiljatelj i primatelj raspolažu istim znanjem s tim da ga pošiljatelj rabi pri enkripciji, a primatelj pri dekripciji poruke. Moderna je kriptografija stvorila asimetrični sustav u kojemu se pojavljuju dva ključa – javni i privatni. Njegove su temelje 1976. postavili Whitfield Diffie i Martin E. Hellman člankom Novi smjerovi u kriptografiji (New Directions in Cryptography). Godinu dana poslije u javnost je dospio sustav RSA, najpoznatiji i najrašireniji sustav asimetrične kriptografije (naziv mu je izveden prema početnim slovima

prezimena njegovih autora – Ron Rivest, Adi Shamir, Len Adleman). Trojica istraživača posebno su se usredotočili na principe modularne aritmetike koja se bavi jednosmjernim funkcijama jer su im se upravo one učinile važnim za oblikovanje sigurne asimetrične kriptografije bez razmjene ključeva. U sustavu RSA pošiljatelj kreira oba ključa, tj. posjeduje veće znanje od primatelja te je na stanovit način 'gospodar' komunikacije. Javni je ključ svima dostupan – ako ga upotrijebi neželjena osoba, moći će pomoću njega enkriptirati svoje poruke, ali ne i dešifrirati poslane. Singh ovako pojašnjava funkcioniranje asimetrične kriptografije:

> Alice svojim ključem enkriptira poruku Bobu, koji je zatim ponovno enkriptira, ali vlastitim ključem, i onda vrati. Kad Alice primi tu dvostruko enkriptiranu poruku, s nje skida vlastitu enkripciju pa je vraća Bobu, koji je zatim može dekriptirati vlastitim ključem i napokon pročitati (2003: 177).[10]

Godine 1991. američki je kriptograf i politički aktivist Philip Zimmermann izradio i na mreži objavio asimetrični sustav digitalnog šifriranja s privatnim i javnim ključem i nazvao ga PGP (*Pretty Good Privacy*) kaneći običnim građanima omogućiti najveći stupanj zaštite na internetu. Zbog tog je poteza Zimmermann dospio pred američki sud, jer kriptografske sustave "s više od 40 bitova američke carinske vlasti službeno administrativno klasificiraju kao streljivo/oružje, a PGP nikad ne koristi manje od 128 bitova" (Lunde 2013: 274). Vlast je svoj potez pojašnjavala činjenicom da se najsofisticiranijim kriptografskim tehnikama služe upravo najokorjeliji zločinci, teroristi, trgovci oružjem i narkokarteli te da obavještajne službe stoga trebaju imati relativno lak pristup tajnoj komunikaciji.

U budućnosti, i to vrlo skoroj, smatraju stručnjaci, razvit će se kvantna računala, kvantni internet i kvantna kriptografija.[11] Ideja se dakako temelji na kvantnoj fizici, tj. polazi od Einsteinove teorije, konkretnije od Heisenbergova načela neodređenosti koje tvrdi "da ništa nije moguće savršeno izmjeriti, i to zato što već i sam način mjerenja mijenja promatrano tijelo" (Singh 2003: 216), uključujući najsitnije čestice. Prevedeno na tajnopisni jezik to znači da će pošiljatelj i primatelj u slučaju neprijateljske aktivnosti primijetiti njezine

---

[10] Kako bi razigrali opise specifičnosti kriptogramskoga općenja analitičari su uobičajili pošiljatelja i primatelja zvati Alice i Bob, a 'neprijatelja', tj. prisluškivača Eva. Ta su imena postala eksplikacijski standard u modernoj kriptografiji. Usp. npr.: Brassard 1993; Müller 2009; Bayart 2000; Singh 2003; Barun – Dujella – Franušić 2008; Lunde 2010; Eschbach 2017.

[11] Priču o kvantnoj kriptografiji otvorio je IBM-ov istraživač Charles Bennett 1984. godine. O njoj, uz ostale, pišu: Singh 2003; Dujella – Maretić 2007; Lunde 2013; Gašparić – Draženović 2014.

vidljive tragove na tajnom ključu, da će "s lakoćom ustanoviti prisutnost napadača, čak i količinu informacija koje je presreo" (Gašparić – Draženović 2014). Stručnjaci nagovješćuju da će razvoj kvantne kriptografije biti završni stupanj razvoja te discipline, tj. da će njome izrađeni kriptogrami uistinu biti neodgonetljivi.

Kriptogram se – kako i sugeriraju odabrani ulomci iz njegove povijesti – pokazao izrazito pragmatičnim važnim pomagalom u različitim područjima. No on je u pojedinim trenucima bio toliko prisutan, popularan i poticajan da se na različite načine pojavljivao i u kulturnim praksama poput književnosti, likovnosti i enigmatike. U tim slučajevima pojava kriptograma izaziva ugodu, ujedinjuje estetsko uživanje, ludizam i privlačnost traganja. Izdvojit ću nekoliko epizoda u kojima se kriptogram pojavljuje kao plamen koji raspaljuje imaginaciju.

TAJNOPISNA ZAGONETKA

U jezičnim rječnicima koji imaju natuknicu kriptogram taj se fenomen obično određuje kao zagonetka. Tako Bratoljub Klaić piše da je kriptogram "vrsta zagonetke u kojoj treba najprije pronaći 'ključ', a onda primjenom njegovom i eventualnim premetanjem slova odgonetnuti značenje" (1984: 754). Anić i Goldstein doslovce ponavljaju Klaićevu definiciju.[12] Takvo pojašnjenje kriptograma najviše pogađa njegovu upotrebu u enigmatici.

Enigmatski je kriptogram "najzagonetnija zagonetka" (Šantek 2009) bliska igri riječima (Buljan 2003). Može biti slovni, crtani ili slikovni (Milovanović – Trivunac 2013: 6). Nema strogih pravila za njegovu izradu niti preciznijih uputa za njegovo rješavanje. Razlog je više nego jasan – kriptogram je uistinu poticajan samo ako je sastavljen prema originalnom ključu. Rješavač mora otkriti ključ, a na tom će mu putu dobro doći strpljivost, imaginacija, logika, iskušavanje različitih kombinacija i asocijativnost. Zagonetač rješavaču pomaže tako što iznad kriptograma navodi broj slova koji sadrži rješenje. U enigmatskoj je praksi, na temelju većeg broja primjera, ipak moguće uočiti uporišna obilježja i glavne smjerove oblikovanja tajnopisne zagonetke. Zadatak se najčešće postavlja kao vertikalno uređen niz riječi, sintagmi ili brojeva. Kada otkrije ključ, rješavač će svladati zagonetku tako

[12] Usp.: "vrsta zagonetke u kojoj treba najprije pronaći ključ rješenja, a onda njegovom primjenom i eventualnim premetanjem slova odgonetnuti značenje" (Anić – Goldstein 2000).

da izdvoji i prema intuitivno prepoznatom načelu poveže pojedine elemente postavke kriptograma. Zastanimo na trenutak kod rada Vladimira Kuterovca, objavljenog u "Vjesnikovu kvizu" 272 (1982):

Kriptogram
(4, 4)

SARAJEVO – OLIMPIJA	1:4
RIJEKA – BUDUĆNOST	1:0
CRVENA ZVEZDA – OSIJEK	2:1
VARDAR – PARTIZAN	3:2
OFK NEOGRAD – VELEŽ	0:3
DINAMO RADNIČKI	2:0
VOJVODINA – ZAGREB	0:2
HAJDUK – ŽELJEZNIČAR	2:0

Rješenje: **PRVA LIGA**

Dva broja u zagradi ispod riječi kriptogram upozoravaju da rješenje čine dvije riječi pričem svaka sadrži četiri slova. Ključ rješenja su brojevi u rezultatima utakmica nogometnih klubova. Do sintagme PRVA LIGA dolazi se tako da se zbroje golovi na svakoj utakmici, a taj zbroj upućuje na položaj slova u imenu pobjedničke momčadi. U podlozi Kuterovčeva kriptograma je dakle brojčani ključ. On, dakako, ima mnoštvo varijacija.

Osim brojčanih, ključevi enigmatskih kriptograma mogu biti pravocrtni raspored (iz svake riječi postavke uzima se po jedno slovo), frekvencijski (izdvajaju se slova ili slogovi u riječima postavke koji su češći ili rjeđi od drugih), jezični (izdvajaju se slova iza dvoslova ili dijakritika, jedini samoglasnik ili suglasnik, učahurena riječ i sl.), složeni itd.[13] Kako bih i primjerima naznačio moguće smjerove zagonetačke imaginacije, navest ću još dva kriptograma. Prvi je 1963. u *Rebusu* objavio već citirani Vladimir Kuterovac:

[13] Naveo sam samo neke od osnovnih smjerova postavljanja enigmatskog kriptograma. Pritom sam donekle slijedio klasifikaciju kriptograma koju su predložili Milovanović i Trivunac (2013). Ključevi koje oni navode su: *pravolinijski raspored*, *cifarni ključ*, *sintagme*, *učaureni pojmovi*, *gramatički ključevi* i *složeni ključ*.

Kriptogram
(8, 8)

KLATON
EUKLOD
NEWPON
HEREKLIT
RALILEJ
HERNN
AIHIMED
KRISTOTEL

Rješenje: PITAGORA – KOPERNIK

Ova Kuterovčeva tajnopisna zagonetka ima dva rješenja. Lako je uočljivo da njezinu postavku čine imena starogrčkih mislilaca (s iznimkom Galilea), s tim da se u svakom pojavljuje tipfeler ili zatipak. Prvo rješenje (PITAGORA) dobiva se kada se isprave tipfeleri, a drugo (KOPERNIK) kada se riječ formira upravo od zatipaka. Dodatnu vrijednost i eleganciju Kuterovčevu kriptogramu pribavlja činjenica da rješavačeva korektura sedmorici Grka pridružuje i osmog, a odustajanje od nje usamljenome Galileu dovodi samo stotinjak godina mlađeg kolegu.

Pavle Bogdanović je kriptogram skrio u kratkoj poruci:

Dragi ujače!
Brat Rade odlazi večeras na izlet.
Katica[14]

Čitatelj se treba upitati kamo ide Rade. Odgovor je jednostavan – ide u DUBROVNIK. Ime grada daju prva slova riječi od kojih se sastoji poruka.[15]

---

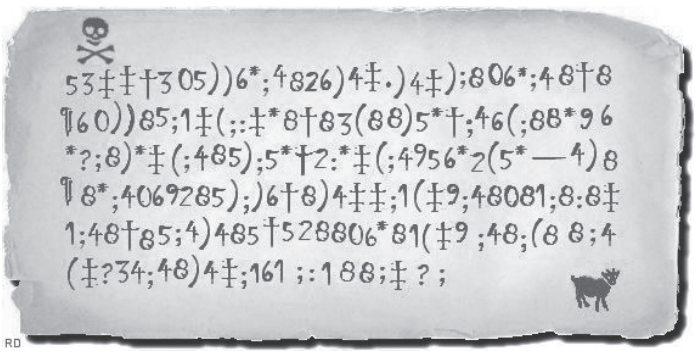
[14] Bogdanovićev kriptogram citira 1990. M. Šantek u rubrici "Kvizov tumač zagonetaka 116" ("Vjesnikov kviz" 540: 40).

[15] U enigmatici je poznata i tzv. kriptogramna križaljka ili kriptogramka. Radi se o križaljci koja koristi iskustva simetrične polialfabetske kriptografije. Polja u križaljci su obrojčena, osim onih koja pripadaju glavnome ključu. Svakom broju odgovaraju po tri slova, pri čemu su dva zadana, a treće se otkriva odgonetanjem ključne riječi. Postupak rješavanja kriptogramke, prema Nedjeljku Nediću (2016) teče ovako: "Slova glavnoga ključa nema niti u tablici. Da bi ju rješavač mogao točno odgonetnuti, kao pomoć mu se daje pomoćni ključ, obično jedan ili dva, koji otkriva(ju) više brojeva za slova glavnoga ključa i time dodatno popunjava tablicu. Nakon toga u tablici ostane najviše 5-6 nepopunjenih mjesta. Križaljka se rješava tako što

OD KRIPTOGRAMA DO KRIPTIČNOSTI

U književnosti kriptogram se pojavljuje u različitim rodovima i žanrovima. Najčešće ga se rabi kao narativni stroj na kojemu se temelji logika priče ili kao element koji na lokalnoj ili globalnoj razini estetizira, oneobičuje, ornamentalizira književni tekst. Status literarne činjenice priskrbili su mu književni velikani kakvi su Poe, Jules Verne, Conan Doyle, Tolstoj, Kipling, Eco, Tolkien ili pak pripadnici skupine Oulipo.[16] Kratko ću podsjetiti na nekoliko tekstova koji u kriptogramičnosti nalaze svoje strukturno i semantičko uporište.

Blistavu literarnu primjenu kriptograma nalazimo u priči "Zlatni skarabej" Edgara Allana Poea, objavljenu 1843. Njezin protagonist William Legrand kreće u potragu za izgubljenim blagom slijedeći tajni zapis pisan nevidljivom tintom na pergmanetu. Drugim riječima, Poe literarno aktualizira i steganografiju i kriptografiju.



Kriptogram iz Poeova Zlatnog skarabeja
(izvor: http://users.telenet.be/d.rijmenants/en/goldbug.htm)

se pod svakim brojem upisuje jedno od triju ponuđenih slova." Nedić dodaje da hrvatska povijest kriptogramne križaljke počinje u "Vjesnikovu kvizu" (22/1972) križaljkom Ivice Radovnikovića Ivre s ključnom riječju DUBROVNIK. Različite inačice kriptogramke izlaze poslije u listovima "Feniks", "Kvizorama" i "Kviskoteka".

[16] Literarni je kriptogram davno postao predmet interesa i izučavanja. Primjerice već 1858. francuski pisac Paul Lacroix pod pseudonimom Bibliophile Jacob objavljuje spis *La Cryptographie: ou l'art d'écrire en chiffres*. U njemu među ostalim izdvaja i komentira kriptograme u brojnim književnim tekstovima. Usp.: Bibliphile Jacob 2013.

U nastavku priče pokazuje se da je Poeov lik izrazito upućen u tajnopis. On pribjegava frekvencijskoj analizi, usput pojašnjavajući njezine temeljne postulate. Na kraju Legrand otkriva šifriranu poruku i pronalazi zakopano blago kapetana Kidda. Kriptogram i njegovo razotkrivanje narativni su zamašnjaci Poeova teksta.

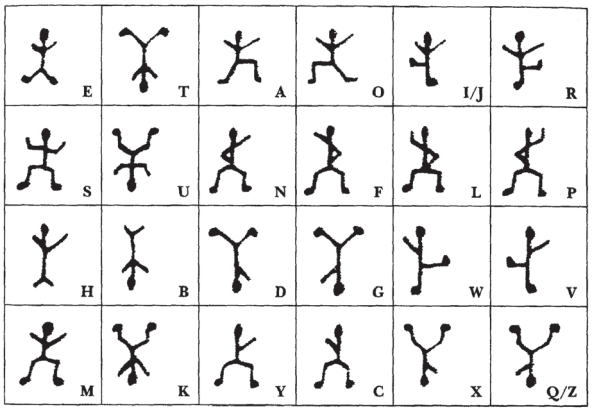
Tajno pismo ima sličnu ulogu i u priči "Likovi plesača" Arthura Conana Doylea. Najpoznatiji literarni detektiv Sherlock Holmes svome kolegi Watsonu na jednom mjestu usput spominje: "U priličnoj sam mjeri upoznat s oblicima tajnog pisanja, te sam o tome napisao i jednu beznačajnu raspravu u kojoj sam analizirao 160 raznih šifri."[17] Holmes se dakle predstavlja kao iskusni kriptoanalitičar. Ta je samopredodžba posve umjesna, jer je u konstrukciji njegova lika u čitavom pripovjednom serijalu Conan Doyle kriptologiji podario značajnu ulogu. U spomenutoj priči Sherlock Holmes rješava slučaj klijenta čija supruga dobiva čudnovate poruke u kojima se umjesto čitljivog teksta pojavljuju stilizirani plesači u različitim pozama.

Poput Poeova junaka, i Holmes pribjegava tehnici frekvencijske analize namijenjene probijanju monoalfabetske supstitucijske šifre. Nakon što je utvrdio koji lik zamjenjuje najčešće slovo engleskoga alfabeta *e*, prionuo je na posao te – uz pomoć logike, lingvistike i statistike – polako popunjavao prazna mjesta. Na koncu iza rasplesanih likova uspio je pročitati tajne poruke, otkriti njihova pošiljatelja i njegove namjere, dapače i sam napisati "plesačku" poruku[18], ali to se nažalost dogodilo prekasno da bi spriječio ubojstvo svoga klijenta.

---

[17] Usp. Doyle 1996: 117.

[18] Dapače na Wattsonovo čuđenje nad činjenicom da je do te mjere proniknuo u tajni kod da ga može i sam upotrebljavati, Holmes uzvraća aforistički: "Što jedan čovjek izmisli, drugi može otkriti" (Doyle 1996: 125).



Sherlockov plesni alfabet
(izvor: http://www.essaydocs.org/a-summary-of-the-canon.html?page=15)

Dok je u detektivskim pričama pokretač naracije, u pojedinim književnim tekstovima kriptogram je moguće razumijevati kao stilsku figuru, upravo kao figuru diskurza. U prvi plan naime izlaze njegova diskurzivna atraktivnost i retoričnost. Primjerice hrvatski pjesnik Kemal Mujičić Artnam u zbirci *Ubrzanje* (2002: 25) objavio je sljedeće:

RELeGeSiGe

DeRe, VeGeTeGe ZaReDeRe,
BiCiNiCiDŽiĆiNiZaGe Dži AHiReJeZaČiDe,
ŠaSiRe DeRe SiNi ČiDeCiGePe?

Izdaja

Ti, mala niti, prerušena u običnost, koji ti je strah?

Malo ozbiljniji pogled na dva mikroteksta na istoj stranici sugerira da je riječ o istoj lirskoj minijaturi pri čemu kriptogram prethodi otvorenom tekstu. Pjesnik se poslužio Cezarovom šifrom s pomakom 10, s tim da je radi lakšega čitanja teksta posegnuo za njegovom vokalizacijom – između suglasnika umetao je samoglasnike *a*, *e* i *i*. Nakana Mujičićeva diskurzivnog prerušavanja pjesme očito je bila njezino očuđivanje, stavljanje zvuka i melodije u prvi plan, izazivanje osjećaja stranosti teksta. Prosječnog bi govornika hrvatskoga jezika 'ozvučeni' Mujičićev tekst možda mogao podsjetiti na suglasja koja povezuje s mađarskom ili turskom intonacijom. Ukratko Mujičićev lirski kriptogram ne smjera tajnoj komunikaciji s čitateljem. Da je tako, ne bi

odmah ispod šifriranoga bio ponuđen i polazni, otvoreni tekst. Riječ je o iskušavanju same kriptogramičnosti – u podtekstu autorova postupka kao da čuči misao da kriptogram i najbezazlenijoj poruci pribavlja opažljivost. Retorički višak koji uvodi kriptogram u konačnici nas potiče da i otvorenom tekstu pristupimo pomnije.

Figurativnost pojedinih književnih, uopće artističkih, kriptograma čini se samorazumljivom. Uostalom, i opća nam tajnopisna tradicija pokazuje da je kriptogram u bliskim (gdjekad nerazmrsivim) relacijama s anagramom čiju figurativnost nije potrebno dokazivati.

Kriptogramsku intonaciju sadrže i pojedini oblici istraživanja skupine Oulipo, međunarodne skupine koja okuplja pisce, slikare, matematičare i dr. Oulipovci su, da podsjetim, tražili i iskušavali nove (potencijalno književne) tehnike i oblike, oslanjajući se pritom na matematičke obrasce i ispitujući stvaralački impuls različitih vrsta ograničenja. Kriptogramsku je inspiraciju možda najprije moguće pripisati spisateljskoj metodi S+7, koju je 1961. izmislio pjesnik Jean Lescure (1912–2005). Radi se o postupku preispisivanja postojećeg teksta koji se zasniva na zamjeni svake imenice imenicom koja se u rječniku tog jezika nalazi sedam mjesta poslije. Umjesto rječnika, mogu se koristiti i knjige poput *Biblije*, *Ustava*, *Zločina i kazne* – u tom slučaju uzima se sedma imenica iz teksta, pa četrnaesta, pa dvadeset i prva itd. Raymond Queneau je, primjenjujući metodu S+7, ludički kriptogramirao Baudelaireovu proznu minijaturu *L'Étranger* (*Stranac*) u *L'étreinte* (*Zagrljaj*), a basnu *La cigale et la fourmi* (*Cvrčak i mrav*) u *La cimaise et la fraction* (*Žljebić i prijelom*). Podvrgnemo li pak Pranjkovićevu rečenicu *U svakom načinu jezične porabe susrećemo sve jezične funkcije* logici metode S+7, i pritom se poslužimo Anićevim *Rječnikom*, dobit ćemo sljedeću rečenicu:

> U SVAKOJ NADARENOSTI JEZIČNE PORAZNOSTI SUSREĆEMO SVE JEZIČNE FURKE.

Na koncu htio bih još kazati da se imenica kriptogram, pridjev kriptogramski i prilog kriptično u rječniku književne kritike i hermeneutičkom rječniku, osim doslovno, mogu rabiti i metaforički, tj. upućivati na enigmatičnost jezika ili strukture teksta, na nerazlučivu diskurzivnu mnoštvenost i semantičku nerazrješivost teksta, upravo na njegovu hermetičnost. Čitava se književnost može zamišljati kao pokušaj da se kriptogramski dohvati arhitekst svijeta. Pritom su skrivena značenja, tamna mjesta, tajna pisma i nepoznati jezici dobrodošli saveznici, sastavni dio tog pothvata. Kriptičnost je u samom srcu književne komunikacije. Upravo nas ona potiče da iznova

čitamo već čitane tekstove, da ih iznova opisujemo proizvodeći pritom vazda nove smislove. Vjerujem da je Roland Barthes i to imao na umu kada je ustvrdio: "Kriptografija je prava vokacija pisma."

LITERATURA

Anić, Vladimir. 1998. *Rječnik hrvatskoga jezika*. Zagreb: Novi Liber.

Anić, Vladimir i Ivo Goldstein. 2000. [2]*Rječnik stranih riječi*. Zagreb: Novi Liber.

Bagić, Krešimir. 2012. *Rječnik stilskih figura*. Zagreb: Školska knjiga.

Barthes, Roland. 2004. *Užitak u tekstu / Varijacije o pismu*. Prev.: Z. Mrkonjić i V. Mikšić. Zagreb: Meandar.

Barun, Marija, Andrej Dujella i Zrinka Franušić. 2008. Kriptografija u školi. "Poučak" 33, 40–52.

Bayart, Frédéric. 2000. *La cryptographie expliquée***.** URL: http://www.bibmath.net/crypto/. [posjet 20. III. 2018]

Bazdan, Zdravko. 2016. Poslovno-obavještajne službe, industrijska i gospodarska špijunaža u međunarodnoj ekonomiji. "Zbornik Sveučilišta u Dubrovniku" 3, 49–72.

Bibliophile Jacob. 2013. *La Cryptographie ou l'art d'écrire en chiffres*. Kindle Edition. [1858. Pariz: Adolph Delahays].

Brassard, Gilles. 1993. *Cryptologie contemporaine*. Paris – Milan – Barcelone – Bonn: Masson.

Bubnjević, Slobodan. 2004. Enigme i rukopisi. "Vreme" 726. URL: http://www.vreme.com/cms/view.php?id=398176. [posjet 20. III. 2018]

Buljan, Alojz. 2003. *Kombinatorika u igrama riječi (u književnosti, enigmatici i promidžbi i matematički okviri kombiniranja)*. Novska: Ogranak Matice hrvatske.

Collard, Brigitte. 2004. La cryptographie dans l'Antiquité gréco-romaine. *Folia Electronica Classica* 7. URL: http://bcs.fltr.ucl.ac.be/FE/07/CRYPT/Crypto07-28.html. [posjet 20. III. 2018]

Čukljaš, Đuro. 1994. *Tajno komuniciranje špijuna*. Zagreb: MUP RH.

Eco, Umberto. 2008. *Ime ruže*. Prev.: L. Paić. Zagreb: Izvori.

Doyle, Arthur Conan. 1996. *Sherlock Holmes i likovi plesača*. Prev.: Lj. Hrdjok. Zagreb: Cid.

Dujella, Andrej i Marcel Maretić. 2007. *Kriptografija*. Zagreb: Element.

Eschbach, Jules. 2017. *Cryptographie. Une étude sur son évolution et ses innovations majeures*. Kindle Editions.

Gašparić, Sandra i Željka Draženović. 2014. *Kvantna kriptografija*. URL: http://security.foi.hr/wiki/index.php/Kvantna_kriptografija. [posjet 20. III. 2018]

Informatičar Starog Kova. 2012. *Nulti kompjuter*. URL: http://informaticar.eu/150-nulti-kompjuter/. [posjet 20. III. 2018]

Klaić, Bratoljub. 1984. *Rječnik stranih riječi*. Zagreb: Nakladni zavod Matice hrvatske.

Lunde, Paul (ur.). 2010. *Tajne kodova. Razumijevanje svijeta skrivenih poruka*. Prev.: D. Biličić. Zagreb: Znanje.

Milovanović, Branko i Vladeta Trivunac. 2013. *Zagonetka kriptogram*. Beograd: EK Nova zagonetka – Alma.

Mujičić, Artnam, Kemal. 2002. *Ubrzanje*. Zagreb: Naklada Breza.

Müller. Didier. 2009. *Ars cryptographica. Une étude des messages secrets de l'Antiquité à nos jours*. URL: http://www.apprendre-en-ligne.net/crypto/activites/index.html. [posjet 20. III. 2018]

Poe, Edgar Allan. 1956. *Zlatni skarabej*. Prev.: A. Temer. Zagreb: Mladost.

Pranjković, Ivo. 2005. [2]*Jezik i beletristika*. Zagreb: Disput.

Singh, Simon. 2003. *Šifre. Kratka povijest kriptografije*. Prev.: P. Raos. Zagreb: Mozaik knjiga.

Šantek, Miroslav. 1990. Kvizov tumač zagonetaka 116. "Vjesnikov kviz" 540: 40.

Šantek, Miroslav. 2009. *Kriptogram: najzagonetnija zagonetka*. Duga Resa: Pečarić & Radočaj.

Škiljan, Zdenko. 1994. *Englezko-hrvatski i hrvatsko-englezki rječnik obavjèstnîčkôga nazivlja. Prema članku prof. dr. B. Lászla "Pabirci redničnoga i obavjèstnîčnôga pojmovlja oko razumnih sustava"*. URL: http://degiorgi.math.hr/~vsego/phun/rjecnik.html. [posjet 20. III. 2018]

Vigenere Blaise de. 1586. *Traicté des chiffres, ou Secretes manieres d'escrire*. [Mrežno izdanje: 2013. Bibliothèque nationale de France. URL: http://gallica.bnf.fr/ark:/12148/bpt6k73371g: posjet 20. III. 2018]

Cryptologie dans 'Le Scarabée d'or'. URL: https://fr.wikipedia.org/wiki/Cryptologie_dans_Le_Scarab%C3%A9e_d%27or. [posjet 20. III. 2018]

Kriptografija. *Hrvatska enciklopedija*. URL: http://www.enciklopedija.hr/natuknica.aspx?ID=33988. [posjet 20. III. 2018]

SUMMARY

CRYPTOGRAM – A VERY SHORT INTRODUCTION

The term cryptography stands for a scientific discipline that studies the techniques of encrypting and dispatching secret messages as well as the artistry of encrypting itself. Cryptogram is a message which has been encrypted in a secret type of script, a code only its addresser and addressee share. The first part of the paper sums up the history of secret communication by retracing its manifestations from the 7th century BC until present day. Some of these practices include: steganography (hiding the message), transposition and substitution cryptograms (devised by classical cryptography) and the asymmetrical RSA cryptosystem (which marks the beginning of modern cryptography). The second part of the paper focuses on the roles cryptogram plays in different cultural practices, primarily in enigmatography and literature. In these cases cryptogram does not seek to establish secret communication but motivates aesthetic and ludic enjoyment as well as the appeal of a quest. Finally, the paper defines cryptogram in literature as a figure of speech (writing) which explicitly signifies crypticness as an important quality of literary communication.

Key words: cryptography, cryptogram, figure of speech, riddle